TRASNA
THE FUTURE OF IOT

Securing *PUF with Zero Knowledge Proof (ZKP)*: Future of Private Blockchain on Chip

Central idea

In the realm of IoT and blockchain, security and privacy are paramount. This article explores the fusion of Zero-Knowledge Proof & Physically Unclonable Functions (PUFs)[1] to boost the security of blockchain-enabled IoT networks.

Takeaways

After reading the article, the reader can see the limitation on PUF and how TRASNA'S innovation can offer an additional layer of security to PUF towards Blockchain's *Root of Trust* on chip.

Development

The landscape of security and privacy in IoT and PUF (*Physical Unclonable Functions)* is physical object that for a given input and conditions (challenge), provides a physically defined "digital fingerprint" output (response) that serves as a unique identifier. PUF technologies have been explored extensively, yet several gaps persist, particularly concerning their intersection.

It has been observed that proposed Physical Unclonable Functions (PUFs) can be broken by numerical modelling attacks.
Given a set of challenge-response pairs (CRPs) of a PUF, the given attacks construct a computer algorithm, which behaves indistinguishably from the original PUF on almost all CRPs. This algorithm can subsequently impersonate the PUF and can be cloned and distributed arbitrarily. This compromises the security of all applications and protocols that are based on the respective PUF.

Additionally, it potentially suffers from a lack of reliability, and becomes more sensible to modelling and physical attacks. Thus, PUF's entropy may fail to ensure a desired uniqueness on IoT devices. Hence, not all the variants of PUF are secured.

Role of Blockchain with PUF:

As edge devices become ubiquitous and interconnected in connected systems, therefore IoE (Internet of Everything)[2] networks must rely on Integrated Circuits (ICs) for data protection and privacy.

Considering this conventional protection, it always relies on well-established key generation, data confidentiality, integrity, authentication and identification. Hence, it becomes necessary for ICs to be able to provide plug-and-play protection in a cost-effective manner.

Unfortunately, the classical methodologies (e.g., digital signatures, encryption, etc.) suffer from numerous potential limitations. Seldom they are very sluggish, computationally

exhaustive, costly, and increasingly susceptible to physical and side-channel attacks. Even the scalability has also been challenged with such massive IoT systems and questions about security.

Hardware-based security paradigms such as PUF (*Physical Unclonable Functions)* provide random functions on edge modules to create security and reliability for IoT systems. PUFs can be used to retrieve hardware-based chip signatures and eruptive private keys.

Data management, security and privacy of data, devices, and individual in SCADA systems[3] are some of the key aspects in the IoE architecture that require careful consideration and resolution.

Integrating the Blockchain into the IoE environment can help solve these issues and helps in achieving a unified secure data technology. The implementation and the performance of a hybrid framework of Blockchain, based on the secret computational model of a PUF. Blockchain and PUF can complement IoE by providing a secure sharing service where information is reliable and traceable.

A Hybrid Strategy from TRASNA to secure PUF for IoT Devices :

TRASNA has initiated a next-generation strategy of Crypto-algorithm on chip, which could be a security game changer. The essential components of the innovation is to blend *Zero Knowledge Proof (ZKP)*[4] with existing PUF, resulting in a new private Blockchain foundation for IoT systems and adding an extra layer of security to the existing PUF.

What is *Zero Knowledge Proof*?

ZKP protocols as the most prominent tools to meet privacy issues for enterprise blockchain networks.

ZKP are cryptographic tools and protocols that allow parties to verify the statement without revealing any extra data regarding this statement.

ZKP methods meet the requirements for privacy while preserving the fundamental characteristics of blockchain technology: the absence of a trusted third party (TTP) and the ability to trace data.

ZKP are characterized by the following properties:

- **Completeness**: They offer an efficient means to verify whether the statement is correct.
- **Soundness**: They provide a very low probability of erroneously confirming an incorrect statement.
- **Zero-knowledge**: blockchain participants, with the exception of the data owner, do not have any additional information about private data

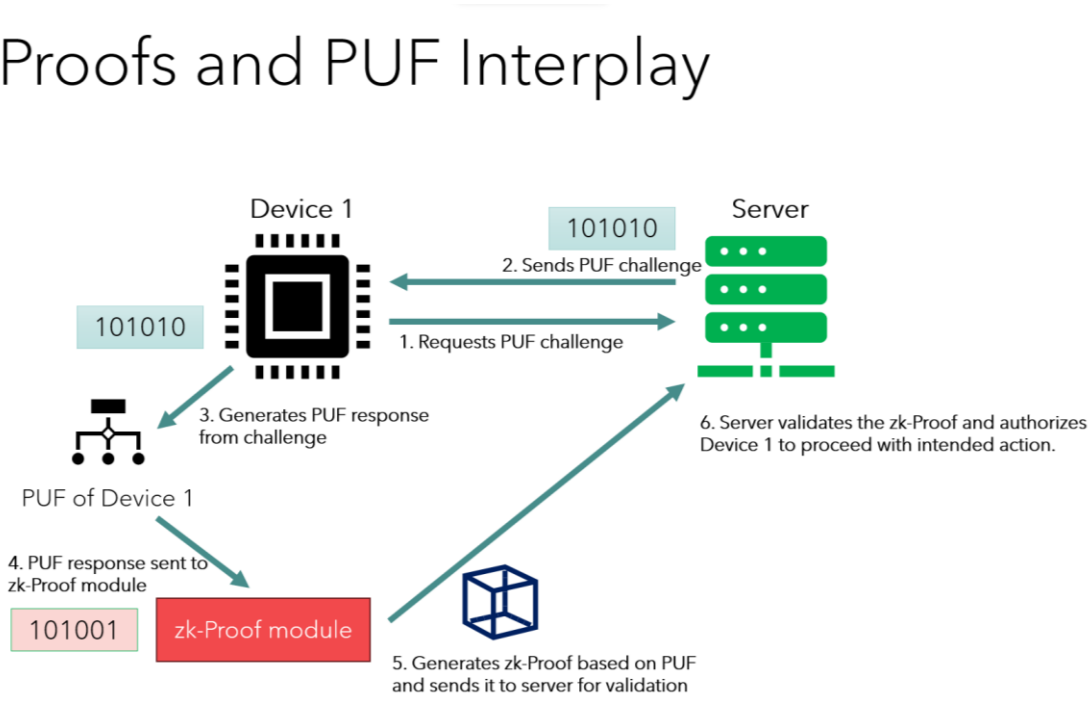

Figure 1. TRASNA Solutions Technologies Ltd.

The above high-level diagram, presented in Figure 1, illustrates how PUF is being protected with the authentication and verification scheme for any new IoT device in the PUF life cycle. The potential attack-prune components in PUF is the look-up table of challenge responses. The ZKP algorithm consolidates the security and leakage of PUF (if any) while revealing no additional information about the device.

A private blockchain is controlled by multiple organizations that allows only verified members, referred to as "trusted" devices, to become part of its network. These trusted members receive different levels of access to the blockchain. Such a network is also known as consortium blockchain as the blockchain's decisions are overlooked by a consortium rather than a single entity, thus preventing complete control of blockchain by one party.

The integration of TRASNA technology, an "hybrid" technical solution which combines Zero Knowledge Proofs (ZKP) and Physical Unclonable Function (PUF), represents a unique and innovative approach in IoT connectivity.

TRASNA's innovation Roadmap of "embedded" private Blockchain to combat various SoC challenges :

Integrating Physically Unclonable Functions (PUFs) into IoT devices along with Zero Knowledge Proofs (ZKP) offers a robust solution to prevent device cloning and protect against unauthorized access. This ensures that only legitimate devices can participate in the blockchain network, significantly reducing the risk of data breaches.

Consider the following use case to illustrate how the integration of PUF can enhance the security and protect the integrity of data across IoT devices within a Smart Cattle Farming system:

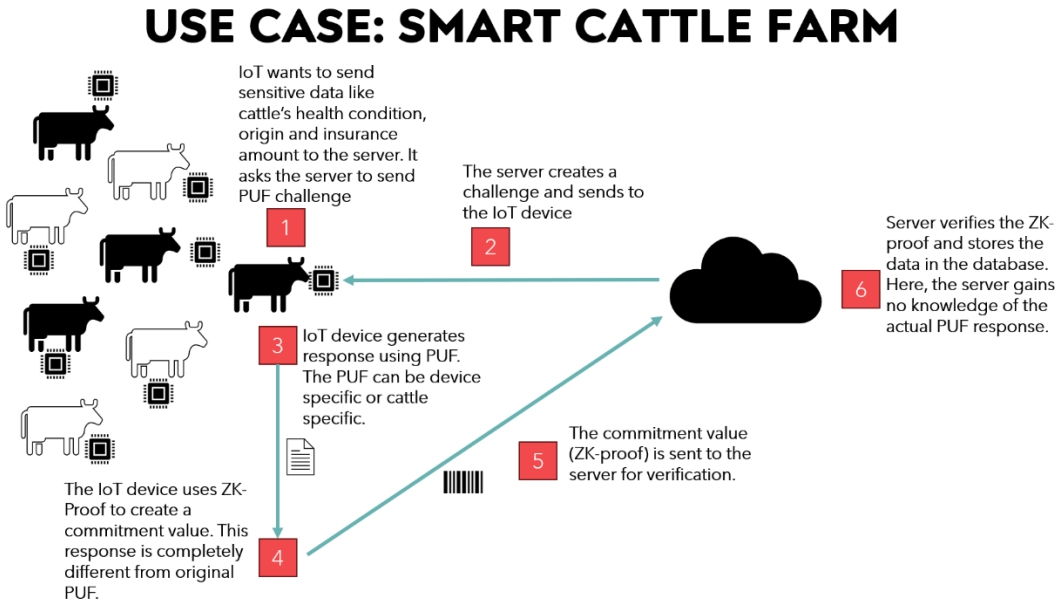

Figure 2. TRASNA Solutions Technologies Ltd.

TRASNA offers a smart and slick design for an easily scalable blockchain network that effectively accommodates the growing number of IoT devices and the associated data flow, without compromising the system efficiency, power availability and the consensus mechanism required to reconstruct missing blocks.

Hence, the entire roadmap architecture is categorized as follows :

- **Initialization of the IoT network**
- **Integration of PUF+ZKP**
- **TRASNA's proprietary algorithm of low-power Consensus Mechanism with ZKP+PUF**

Current trends in IoT networks primarily rely on centralized entities to manage data, which gives rise to a myriad of issues. These challenges include a central point of failure, leaving the system vulnerable to disruptions and potential data loss. Moreover, the centralized nature of data management opens doors to data manipulation by malicious third parties, cyber exploitation, and unauthorized access.

Another critical concern in the existing IoT ecosystem is the lack of security measures to prevent device cloning. This vulnerability allows unauthorized entities to create counterfeit devices, leading to data breaches and compromised system integrity.

In response to these challenges, TRASNA's innovative roadmap, which integrates PUF and private blockchain technology with ZKP at the chip level, will usher a design in the future of IoT.

Final Challenges

Incorporating the hybrid algorithm, which combines PUF, ZKP, and private blockchain technology, presents several key challenges. These challenges need to be addressed effectively to make this innovative approach feasible:

- **Code Size Constraint:** The prime challenge is to ensure that the hybrid algorithm and associated security features can fit within the constraints of the chip's available memory.
- **Acceleration of ZKP:** Additionally to accelerate the ZKP process (as inherently ZKP is slower in verification and crypto-calculation), TRASNA is TRASNA is exploring the deployment of low-level libraries like *Arkworks*, or using Domain-Specific Languages (DSLs) such as Cairo or Circom. These tools can compile code down to essential primitives, making ZKP processing more efficient and less resource-intensive.

Glossary:

1. **A physical unclonable function** or **PUF**, is a physical object that for a given input and conditions (challenge), provides a physically defined "digital fingerprint" output (response) that serves as a unique idetifie. PUFs are often based on unique physical variations occurring naturally during semiconductor manufacturing.

2. **Internet of Everything (IoE)** : The "Internet of Everything" (IoE) is a concept that extends the scope of the Internet of Things (IoT) to include not only physical devices and objects but also people, processes, data, and the connections between them. IoE envisions a highly interconnected digital ecosystem where everything and everyone is linked and able to communicate and share data in a seamless and intelligent manner.

3. **SCADA Systems :** SCADA, which stands for "Supervisory Control and Data Acquisition," refers to a type of control system used in various industries to monitor and manage processes, infrastructure, and facilities. SCADA systems are instrumental in collecting data in real-time from remote locations and then transmitting and displaying this data for control or monitoring purposes.

4. **Zero Knowledge Proof (ZKP) :** is a cryptographic protocol and technique that allows one party (the prover) to demonstrate to another party (the verifier) that they have certain knowledge or information without revealing any specific details about that knowledge. In other words, it enables the prover to prove the authenticity of a statement without disclosing the content of the statement itself.

References:

1. Miguel Ángel Prada-Delgado, Iluminada Baturone, Gero Dittmann, Jens Jelitto, Andreas Kind, PUF-derived IoT identities in a zero-knowledge protocol for blockchain, Internet of Things, Volume 9, 2020,100057,ISSN 2542-6605,Elsievier Publications.

2. Zero-Knowledge Proof-based Practical Federated Learning on Blockchain Z Xing, Z Zhang, M Li, J Liu, L Zhu, G Russello, MR Asghar, arXiv preprint arXiv:2304.05590, 2023•arxiv.org

ABOUT TRASNA

TRASNA is focused on Technology leadership providing semiconductors and its related software and services solutions for IoT mass deployment. TRASNA combines innovation in semiconductor design, secure Software, edge computing, AI and blockchain integration to deliver the most innovative and optimized System-On-Chip to take advantage of huge IoT opportunities facilitated by the emergence of 5G in which networks can meet the communication needs of billions of connected objects and where the NB-IoT is part of 5G specifications.

TRASNA System-on-Chip embeds RISC-V cores, i-SIM and GNSS, developed to offer the lowest Bill of Material to the market to scale up the deployment of massive IoT.

TRASNA's Telecom Business Unit, provides a unique offering with all products and services related to IoT connectivity such as eSIMs / eUICCs and expertise so its customers can build, innovate, and grow successful businesses in a constantly progressing environment. We support and guide our customers through every step of their IoT device journey.

To stay updated on the latest news about TRASNA, you can follow TRASNA on Website, Linkedin, Twitter, Facebook, Vimeo