Physical Unclonable Function based Solutions to Unification of User, Device and Data Authentication

Abstract

With the advent of the Internet of Things (IoT) and artificial intelligence (AI), security is increasingly becoming a requirement rather than an option. Further development of cutting-edge applications is challenged into seeking trust assurance of multiple credentials from user, device and data. Existing solutions rely mainly on the same underlying scheme for single factor authentication to meet this expectation with a naïve layer-by-layer multi-factor authentication. These solutions are typically realized using conventional techniques that require the safekeeping of secret binary key in the non-volatile memory or battery-backed SRAM of some device or token owned by the user, which have been proven to be vulnerable to various kinds of invasive, semi-invasive and side channel attacks. The non-repudiation assumption of these conventional techniques is being challenged by emerging artificial-intelligent assisted and malware-based attacks on independently chained weak link (factor), and their limited extension to internet of things scenarios, where the sheer number of inexpensive and often insufficiently protected endpoints prevents application of standard, secret-key based techniques. Physical Unclonable Function (PUF), a hardware-intrinsic security primitive emerged in the early 2000s, stood out as an inexpensive and yet effective way for device authentication and secret key generation. Compared to those conventional cryptographic primitives, the secret is hidden intrinsically within device structure by the uncontrollable manufacturing process variations of integrated circuits. The appealing low-cost, low-power, tamper-aware and "reply-upon-request" attributes render PUF a promising candidate for the unification of device signature with the user credential and data acquired through the device.

This research is motivated by the security threats encountered by the empowerment of smart IoT devices and AI hardware for autonomous sensing and decision making. After nearly two decades of research into various newer structures of PUF designs and quality enhancement of popular existing structures, it is time to review and explore their application gaps in conjunction with new use cases by innovative use of vision sensor and strong PUF to attest the provenance of data and ownership more than mere device authentication. A comprehensive review of PUF sheds light on new authentication schemes at the user-device and data-device nexus by leveraging on smart vision and human biometric technologies. New notions of PUF based user-device hash and data-device hash as well as event-driven PUF design are spawned as a result for end-point authentication and image forensics.

The first distinctive contribution is a new event-driven PUF, which is designed from the dynamic vision sensor (DVS). DVS is an image sensor that responds asynchronously to relative changes in intensity. Compared with the conventional active pixel sensor, DVS reduces the data redundancy and possess high dynamic range while preserving precise timing information. The DVS-based PUF is derived from the original sensing circuit of DVS, with only three transistors added per pixel (originally 14 transistors and 2 capacitors) to achieve independent but simultaneous DVS sensing and PUF operation. The responses of the PUF can be made to trigger only upon the detection of interested events. This is believed to be the only known image sensor based PUF whose response is indivisibly related to the sensing environment. This

new subfield of event-driven PUF enables proofs that a certain hardware has not been tampered with, and augments current applications of these advanced sensors, such as traffic monitoring, surveillance and remote healthcare, by endowing the camera with new security feature to generate non-repudiable proofs of exceptional events happened in an environment or surroundings. Simulations results show that the DVS sensor meets the quality criteria in PUF operation without compromising its normal imaging performance.

The second contribution is a "match-on-server" PUF-based user-device hash for endpoint authentication. A UDhashing scheme is proposed to unify the macroscopic human biometric and microscopic silicon entropy into a single identity by projecting the contactless facial biometric into a PUF-defined random space. The system achieves a bipartite authentication of both end user and end device as a whole, and mutual authentication between the endpoint and the verifier. The unified hash protects the biometric template from being compromised by spoofing, theft and tampering. In addition, the use of strong PUF enables cancellable template. The scheme is demonstrated using measured silicon data of a diode-clamped inverter-based strong PUF fabricated in 40 nm 1.1V CMOS technology, and the Olivetti Research Laboratory and extended Yale B face databases. The experimental results show that the proposed system has good authentication performance with excellent discriminability for different (challenge, user, device) tuples. Besides, the proposed system is analyzed to be resilient to several known attacks.

Finally, the design of a rotation/scaling-invariant PUF-based data-device hash is proposed for digital (more specifically, image) forensic applications. Existing digital forensics methods are capable of performing well in either forgery content detection or acquisition device identification but not both. At a time of rampant public media manipulation and ease of fake image/video fabrication, verification of benign and malicious image transformations is necessary but not sufficient for fact checking of visual artefacts presented in the court of law. The proposed scheme fills this gap by being able to detect and locate image tampering while identifying the source device that produces the images or footages with a comparatively low cost. The core idea is to create a hash tag to mate the invariant image features with the PUF-based device "fingerprint" by using random projection. The shaky security assumption of keeping a stored digital string (key) private for attestation in conventional perceptual image hash is avoided. For this use case, the proposed scheme can do away with challenge-response enrolment and hence the need for a trusted third party server to secure the database of challenge-response pairs. The proposed hash is evaluated on the modified CASIA database and the CMOS image sensor based PUF. It is able to identify the source camera with excellent accuracy while achieving a very high detection rate of content tampering against normal perceptual content invariant processing. This work opens a new horizon of sensor PUF for proactive image, video or audio provenance analysis.