Skysong Innovations
Advancing the Arizona State University Knowledge Enterprise

1475 N. Scottsdale Road, Suite 200
Scottsdale, AZ 85287-3538
Phone: 480 884 1996 Fax: 480 884 1984

Case ID:M19-274P
Published: 2/11/2020

Inventors

Jae-Sun Seo
Shihui Yin
Sai Kiran Cherupally

Contact

Shen Yan
shen.yan@skysonginnovations.com

Authentication and Secret Key Generation Using Electrocardiogram, Heart Rate Variability, and SRAM-Based Physical Unclonable Functions

Background

Traditional hardware designs for device authentication and secret key generation typically employ physical unclonable functions (PUFs) which generate unique random numbers based on static random-access memory (SRAM), delay, or analog circuit elements. Although silicon PUFs can be highly stable and unique, they do not represent liveliness. Biometric authentication using fingerprint or iris scanning have become standardized but are not immune to spoofing attacks. Human electrocardiogram (ECG) signals provide liveliness proof and have emerged as a new modality for authentication and secret key generation. However, ECG data manifests in an identical way on multiple devices for a unique user, which exposes a larger attack surface and cannot be revoked once leaked. Therefore, a smart security engine that integrates multiple entropy sources can advance robustness for key applications.

Invention Description

Researchers at Arizona State University have developed a smart wearable hardware security engine that combines three entropy sources—user-unique ECG features and heart rate variability (HRV), and device-unique SRAM-based PUF—to perform real-time authentication and secret key generation. Because biometric information is not used in raw form but is instead hybridized with SRAM PUFs, risk of an attack is significantly reduced. A prototype chip was fabricated which operated at 8.013μW and 0.6V for real-time authentication. Compared to ECG-only authentication schemes, the equal error rate improved by a factor of 8 for a 741-subject in-house database. Generation of random 256-bit numbers by combining ECG, HRV, and SRAM PUF was also evaluated, showing that 16 randomly selected subjects fully passed the National Institute of Standards and Technology (NIST) randomness tests.

Potential Applications

- Internet-of-Things
- Wearable electronics

Benefits and Advantages

- Low-power consumption
- Non-direct use of biometrics improves user security
- Hybridized entropy sources extend function across multiple users and devices
- Three-factor authentication allows operation even when one or two entropy sources are compromised

Homepage of Professor Jae-sun Seo