

عنوان مقاله:

A Novel Authentication Scheme using the Advantage of DRAM and SRAM Physical Unclonable Functions

محل انتشار:

دهمین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات (سال: 1399)

تعداد صفحات اصل مقاله: 9

نویسندگان:

Fatemeh Najafi - *Department of Electrical Engineering Iran University of Science and Technology*

Masoud Kaveh - *Department of Electrical Engineering Iran University of Science and Technology*

Mohammad Reza Mosavi - *Department of Electrical Engineering Iran University of Science and Technology*

خلاصه مقاله:

Physical Unclonable Functions (PUFs) are low-cost and robust hardware primitives that address many privacy and security challenges. Stable and unique features based on variations in manufacturing processes are the basis of different PUF technologies. So far, many PUF-based constructions have been proposed, which have provided device authentication and key generation services. However, the existing mechanisms have some disadvantages that make them vulnerable to various attacks. In this paper, the new structures of memory-based PUFs and their characteristics are studied. Then, a new design is proposed, which employs both SRAM and DRAM PUFs and uses their advantages to provide a secure and robust authentication method. Furthermore, we propose a novel authentication protocol based on the proposed PUF structure. The proposed scheme not only provides proper features of PUF-based services and significantly increases the security level but also enhances the performance of the system in terms of computational cost and communication overhead.

کلمات کلیدی:

DRAM PUF, SRAM PUF, True random number generation, Efficient authentication

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1136725>

