Highly secure physically unclonable cryptographic primitives based on interfacial magnetic anisotropy

November 2 2018

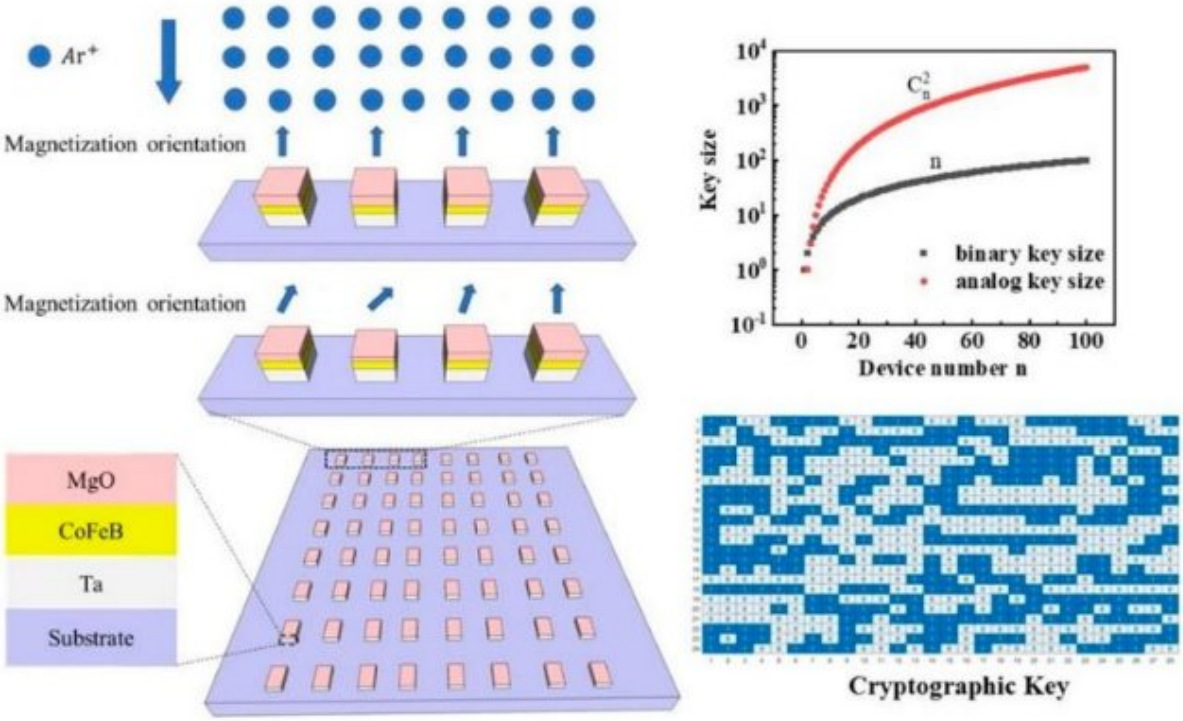

Figure. In the proposed PUF, the random distribution of magnetization orientations can be induced by the sub-nanometer variations of oxide layer through the nonuniformity of thinning process. In addition, this analogue PUF can generate larger key size than its digital counterpart. Credit: Huazhong University of Science and Technology

In a step forward for information security for the Internet of Things, a team of researchers has published a new paper in the online edition of *Nano Letters* in which they have engineered a new type of physically unclonable function (PUF) based on interfacial magnetic anisotropy energy (IAE). This PUF utilizes the random distribution of magnetization orientation of each device, which originates from the sub-nanometer variation of oxide layer produced by the thinning process.

The team is led by Long You, a professor at Huazhong University of Science and Technology and the leader of their Nanoscale Energy Efficient Devices research team, collaborating with Min Song, an assistant professor of Hubei University.

"Information security is of great importance for the approaching Internet of Things (IoT) era. PUFs are almost impossible to duplicate because of their intrinsic random physical nature and they can be considered as the intrinsic electronic fingerprint or biometric of a device," said You. "Moreover, PUFs can be used for authentication and secret key storage and have become a hot topic in the hardware security field over the last decade."

The most widely used PUFs in current integrated circuits are silicon-based semiconductor PUFs. However, silicon PUFs are vulnerable to modelling and side channel attacks. In contrast, the magnetic PUF is resistant to attack and insensitive to environmental variations.

"In all previously proposed MRAM PUFs, a procedure to set random magnetization orientations is necessary for their practical application," said Zhe Guo, a post doctor in You's team. "In our IAE-PUF, the random distribution of magnetization orientations is formed during the MgO layer thinning process, so no initialization is required." The avoidance of setting random states with an external magnetic field or writing current makes it easier to integrate and scale down with low

power consumption.

In the proposed analogue PUF, the extracted resistance values were converted to binary sequence through a comparison method.

"Compared to the digital counterpart, our analogue PUF in this work can generate larger key size with the same device number," said Huiming Chen, a coauthor in this paper. "The larger key size offers a higher security level for practical application."

More information: Huiming Chen et al. Highly Secure Physically Unclonable Cryptographic Primitives Based on Interfacial Magnetic Anisotropy, *Nano Letters* (2018). DOI: 10.1021/acs.nanolett.8b03338

Provided by Huazhong University of Science and Technology