A 2D Cryptographic Hash Function Incorporating Homomorphic Encryption for Secure Digital Signatures

A. Wali[1], H. Ravichandran[2], and S. Das[1,2,3,4, *]

[1]Electrical Engineering and Computer Science, Penn State University, University Park, PA 16802, USA

[2]Engineering Science and Mechanics, Penn State University, University Park, PA 16802, USA

[3]Materials Science and Engineering, Penn State University, University Park, PA 16802, USA

[4]Materials Research Institute, Penn State University, University Park, PA 16802, USA

Abstract:

User authentication is one of the most critical aspects within any information exchange system and encompasses the process of verifying the identity of individuals seeking access to sensitive information. Conventionally, this verification process has relied on establishing robust and secure digital signature protocols employing asymmetric encryption techniques which effectively address the vulnerabilities inherent to symmetric encryption methods that necessitate sharing and reuse of the secret key. In this article, we present a comprehensive hardware-based digital signature platform constructed using integrated circuits (ICs) with atomically thin two-dimensional (2D) monolayer molybdenum disulfide (MoS_2) memtransistors. First, we demonstrate generation of secure and robust cryptographic keys by exploiting the inherent stochasticity of carrier trapping and detrapping at the 2D/oxide interface trap sites as the source of randomness. Subsequently, we leverage the capability of manipulating the functionality of logical NOR through localized programming of MoS_2 memtransistor to create a secure one-way hash function which when homomorphically operated upon with $NAND$, XOR, OR, NOT, and AND logic circuits generate distinct and secure signatures. These signatures are subsequently decrypted to verify the authenticity of the receiver while ensuring complete preservation of data integrity and confidentiality as the underlying information is never revealed. Finally, we provide an insight on the advantages of implementing NOR based hashing techniques in comparison to the conventional XOR based encryption method. Our demonstration highlights the potential of 2D-based ICs in advancing the development of critical information security primitives.