

(54) Title of the invention : MIMLI: A Lightweight Block Cipher for IoT Resource Constrained Devices

(51) International classification (86) International Application No (87) International Publication No (61) Patent of Addition to Application Number (62) Divisional to Application Number	:H04L0009060000, H04W0004700000, H04L0067120000, G06F0021620000, H04L0009080000 :NA :NA :NA :NA :NA :NA	(71)Name of Applicant : 1)INSTITUTE OF ENGINEERING & MANAGEMENT Address of Applicant :INSTITUTE OF ENGINEERING & MANAGEMENT, SALT LAKE ELECTRONICS COMPLEX, SECTOR-V, SALT LAKE, KOLKATA. KOLKATA ----- Name of Applicant : NA Address of Applicant : NA (72)Name of Inventor : 1)Mihir Lal Saha Address of Applicant :INSTITUTE OF ENGINEERING & MANAGEMENT, SALT LAKE ELECTRONICS COMPLEX, SECTOR-V, SALT LAKE, KOLKATA, PIN- 700091. KOLKATA ----- 2)Dr. Malay Gangopadhyaya Address of Applicant :INSTITUTE OF ENGINEERING & MANAGEMENT, SALT LAKE ELECTRONICS COMPLEX, SECTOR-V, SALT LAKE, KOLKATA, PIN- 700091. KOLKATA ----- 3)Dr. Siddartha Roy Address of Applicant :1/2A/1A Ramkrishna Naskar Lane, Belegghata, Kolkata- 700010 KOLKATA ----- 4)Dr. Sanghamitra Poddar Address of Applicant :INSTITUTE OF ENGINEERING & MANAGEMENT, SALT LAKE ELECTRONICS COMPLEX, SECTOR-V, SALT LAKE, KOLKATA, PIN- 700091. KOLKATA ----- 5)Dr. Sayan Chatterjee Address of Applicant :Dept. of Electronics and Telecommunication Engineering, 188 Raja S. C. Mullick Road, Kolkata 700032, Jadavpur University KOLKATA --- 6)Dr. Subhabrata Banerjee Address of Applicant :INSTITUTE OF ENGINEERING & MANAGEMENT, SALT LAKE ELECTRONICS COMPLEX, SECTOR-V, SALT LAKE, KOLKATA, PIN- 700091. KOLKATA -----
--	--	---

(57) Abstract :

The proliferation of IoT devices has led to an exponential increase in the volume of data generated by these devices. This data often contains sensitive information that needs to be secured against unauthorized access, tampering, and interception. As a result, For both businesses and consumers, protecting the security of IoT devices and the data they create has become a crucial concern. However, since that most Internet of Things (IoT) devices are easily accessible, security is one of the biggest issues in the implementation of IoT, and often have constrained resources, such as physical space, power, memories, and computational capacity. In addition, The information is subject to many forms of assaults because of the extensive connection of Internet of Things (IoT) gadgets and the enormous volume of data they create. To address the security challenges of IoT, cryptographic algorithms are used to provide confidentiality and integrity to the information. However, traditional cryptographic algorithms can be too resource-intensive for IoT devices, making it necessary to develop lightweight security schemes. Lightweight cryptography algorithms are designed to be efficient and lightweight, with a small memory footprint and low computational requirements, making them well-suited for IoT devices with limited resources. Among the lightweight cryptography algorithms, lightweight block ciphers are particularly popular. These ciphers use either a Substitution Permutation type network structure or a Feistel type network structure to encrypt. In the SP network structure, the plaintext is divided into smaller blocks, and each block is substituted and permuted using a fixed set of operations. The Feistel network structure, on the other hand, divides the plaintext into two halves, and each half is processed separately using a set of round functions before being combined again. The proposed work focuses on the design of a Lightweight type Block Cipher which can be used in very low resourced devices (RFID tags, IoT devices, sensors etc.).An ultra-lightweight block cipher architecture is proposed for securing IoT devices with limited resources. The architecture utilizes a combination of the SPN and Feistel structures and achieves a balance between security and resource utilization. The proposed cipher provides robust security for IoT devices and has minimal resource utilization, making it an ideal choice for securing IoT devices with limited resources.

No. of Pages : 7 No. of Claims : 6