(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :11/05/2022

(21) Application No.202241027248 A
(43) Publication Date : 17/06/2022

(54) Title of the invention : An Embedded Prime LightWeight Block Cipher for Smart Devices

(51) International classification :H04L0029080000, H04W0004700000, H04L0029060000, H04L0009060000, H04L0009300000
(86) International Application No :PCT//
Filing Date :01/01/1900
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
1)Dr.P.Manickam
Address of Applicant :Asst. Professor, Dept. of Computer Science, Thiagarajar College, Madurai-625009, Tamil Nadu, India. ---------- ----------
2)Ms.M.Girija
3)Dr.M.Ramaswami
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr.P.Manickam
Address of Applicant :Asst. Professor, Dept. of Computer Science, Thiagarajar College, Madurai-625009, Tamil Nadu, India. ---------- ----------
2)Ms.M.Girija
Address of Applicant :Asst. Professor, Dept. of Computer Science, The American College, Madurai-625009, Tamil Nadu, India. ---------- ----------
3)Dr.M.Ramaswami
Address of Applicant :Professor Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamilnadu, India. ---------- ----------

(57) Abstract :
Lightweight cryptography (LWC) is a compact and advancing cryptography protocol. Internet of Things (IoT) is a cutting edge technology which is developed for resource constrained devices for communicating and sharing of information among fellow devices over internet. IoT smart objects are smallest tiny devices and it has limited processing and storage capacities and that often runs on small, low power, battery. IoT devices have many issues and challenges due to inherent properties of IoT and one of the major challenges is security. Success of IoT depends on how smart devices countermeasure the different security attacks. There are many cryptographic algorithms with different services are exist. Each one has some unique properties as well as limitations or constraints. After studying these cryptographic algorithms, the authors decided to propose a new lightweight block cipher, PriPresent. Also, this paper depicts the comparison results of proposed cipher with existing cipher over different metrics.

No. of Pages : 25 No. of Claims : 1