खण्ड-10, अंक-1, वर्ष-2022, मु0प्र0 136-146
D.O.I.: https://doi.org/10.22445/avsp.v10i1.21
SJIF (2021) : 7.247

Implementing Lightweight Cryptography in Enterprises Adopting IoT for IT Transformation

Kavita Bhatia[1], Santosh Kumar Pandey[1], Vivek Kumar Singh[2], Deena Nath Gupta[3], Rajendra Kumar[3]
[1]Ministry of Electronics and IT, New Delhi-110 003, India
[2]Banaras Hindu University, Varanasi-221 005, U.P., India
[3]Jamia Millia Islamia, New Delhi-110 025, India
kbhatia@meity.gov.in, santosh.pandey@meity.gov.in, vivek@bhu.ac.in, prof.dev.cse@gmail.com, rkumar1@jmi.ac.in

Received: 26-08-2022, Accepted: 05-10-2022

Abstract- Today's technology connects different physical objects through a network by which they can transfer their data to each other as per requirement. This arrangement is commonly known as the Internet of Things (IoT). The IoT mainly consists of constrained devices. Devices not directly connected with the electric shoket Instead they work with stored energy only are known as low energy devices. Additionally, these devices manage to work with low storage power and low transmission power. It is necessary to implement lightweight algorithms in an IoT environment in order to provide the devices with a secure and seamless mode of communication. The researchers from all around the globe are currently working in this field. Lightweight cryptography consists of algorithms that work on low energy and small storage. In this paper, the authors present a study and comparison of some well known light weight cryptographic algorithms.

Key words- IT Transformation, Enterprise, IoT, Lightweight Cryptography

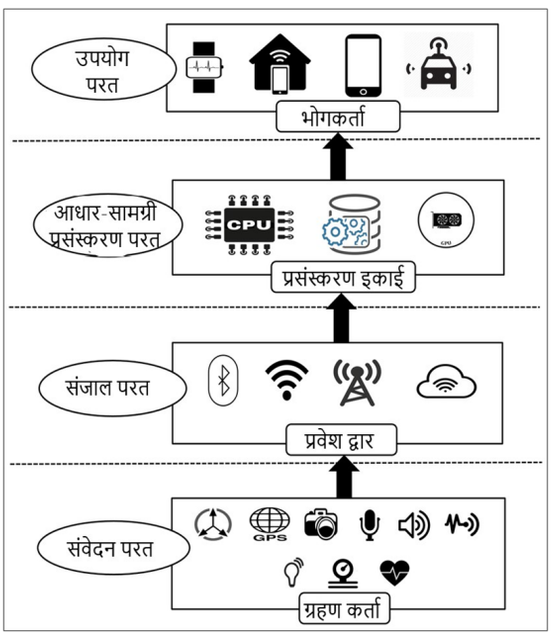
सूचना प्रौद्योगिकी परिवर्तन के लिए "वस्तुओं का अंतर्जाल" को अपनाने वाले उद्यमों में हल्के कूटलिपि विद्या को लागू करना

कविता भाटिया[1], संतोश कुमार पाण्डेय[1], विवेक कुमार सिंह[2], दीना नाथ गुप्ता[3] एवं राजेंद्र कुमार[3]
[1]इलेक्ट्रॉनिक्स और आईटी मंत्रालय, नई दिल्ली–110 003, भारत
[2]बनारस हिन्दू विश्वविद्यालय, वाराणसी–221 005, उ0प्र0, भारत
[3]जामिया मिलिया इस्लामिया, नई दिल्ली–110 025, भारत
kbhatia@meity.gov.in, santosh.pandey@meity.gov.in, vivek@bhu.ac.in, prof.dev.cse@gmail.com, rkumar1@jmi.ac.in

सार– आज की तकनीकी भौतिक जगत में विद्यमान समस्त वस्तुओं को एक–दूसरे से एक अंतर्जाल के माध्यम से जोड़ती है जिससे कि वे अपनी आधार–सामग्री को एक–दूसरे को आवश्यकतानुसार भेज सकें, इस संरचना को हम" **वस्तुओं का अंतर्जाल"** नाम से जानते हैं। **वस्तुओं का अंतर्जाल** मुख्यतः कम क्षमता की वस्तुओं का समायोजन करता है। ऐसी वस्तुएँ जो सीधा–सीधा विद्युत आपूर्ति से नही जुड़े रहते हैं अपितु संग्रहित ऊर्जा के माध्यम से चलते हैं, को हम कम ऊर्जा क्षमता की वस्तु कहते हैं। कम ऊर्जा क्षमता के साथ–साथ इन वस्तुओं में भंडारण क्षमता और तरंग संचार की क्षमता भी अत्यधिक कम होती है। **वस्तुओं का अंतर्जाल** वातावरण में निर्देशों तथा अन्य आधार–सामग्री के निर्बाध एवं सुरक्षित प्रवाह हेतु ये आवश्यक हो जाता है कि इस वातावरण में उपयोग की जाने वाली नियमावलियां एवं चरणबद्ध आचरण कम भार वहन करने वाले हों। विश्व के शोधकर्ता इस समय इसी कार्य पर लगे हुए हैं कि किस तरह से कम–भार–वहन करने वाले सुरक्षित आचरण एवं नियमावली बनाई जाए। कम–भार–वहन से तात्पर्य ऐसे आचरण और नियमावलियों से है जो कि कम विद्युत ऊर्जा में कार्य कर सकें एवं कम भंडारण का प्रयोग करें। इस शोध पत्र में लेखक कुछ बहुत ही प्रचलित कम–भार–वहन करने वाले सुरक्षित तरीकों का अध्ययन एवम तुलनात्मक विश्लेषण प्रस्तुत कर रहे हैं।

बीज शब्द–सूचना प्रौद्योगिकी परिवर्तन, उद्यम, वस्तुओं का अंतर्जाल, हल्के कूटलिपि विद्या

1. **परिचय**– ''वस्तुओं का अन्तर्जाल'' भौतिक जगत में विद्यमान लगभग सभी वस्तुओं को एक अन्तर्जाल के माध्यम से जोड़ने का कार्य करता है जिससे कि वस्तुएं अपनी आधारभूत सामग्री का आदान–प्रदान कर सकें तथा आंतरिक गणना के लिए कुछ सामग्री संग्रहित कर सकें। इन सामान्य सी दिखने वाली वस्तुओं को तीन तरह की विशेष शक्तियाँ प्रदान करता है, संग्रह करने की क्षमता, आदान–प्रदान करने की क्षमता, और आतंरिक गणना करने की क्षमता[1]। यद्यपि बहुतायत वस्तुएं आकार में छोटे होते हैं तथा प्रत्येक समय विद्युत आपूर्ति से जुड़े नहीं रह सकते हैं, यद्यपि इनके सुगम परिचालन हेतु जो नियमावलियां जिम्मेदार हों उनका भी छोटा और सुरक्षित होना आवश्यक है। सुरक्षा के दृष्टिकोण से पूर्व में भी अनेक शोधार्थियों ने अपने उच्चस्तरीय शोधकार्य प्रस्तुत किये हैं। यह तो सर्वविदित है कि किसी भी कार्यक्षेत्र की सुरक्षा तीन प्रकार से सुनिश्चित की जा सकती है, पहला कि उस कार्यक्षेत्र में उपस्थित सभी अवयवों/वस्तुओं का पंजीकरण करके, दूसरा कि यदि कोई दो वस्तुएं एक–दूसरे से बातचीत करना चाहती हैं तो उनके बीच मे आपसी समझौता कराकर, तीसरा कि जो भी सामग्री प्रेषित की जाय उसे कूट में बदलकर[2]। विभिन्न परतों व घटकों के साथ "वस्तुओं का अंतर्जाल" वातावरण की स्थापत्यकला **आकृति–१** में दर्शायी गई है।



आकृति–१: "वस्तुओं का अंतर्जाल" स्थापत्यकला– परतें व घटक

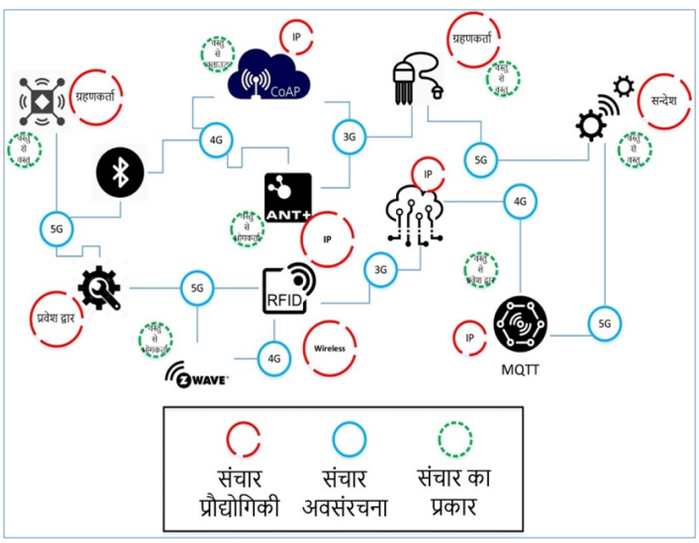
PUF (Physically Unclonable Function) पंजीकरण कार्य के लिए विश्वस्तर पर मान्य सर्वोत्तम तकनीकी है। PUF सभी वस्तुओं को अलग–अलग पहचान क्रमांक उपलब्ध कराता है जो कि एक विशेष प्रकार की गणितीय क्रिया के फलस्वरूप प्राप्त होती है। यह पहचान क्रमांक अपने में वस्तुओं के निर्माण सम्बंधित ब्यौरा भी संकलित रखती है जो कि इन पहचान क्रमांकों को सबसे सुरक्षित और शक्तिशाली बनाता है[3, 4]।

दो वस्तुओं के बीच आपसी समझौता कराने के लिए कई नियमावलियाँ पूर्व में विकसित की गई हैं जिनमें की Diffie Hellman (DH) key exchange algorithm अब तक की सबसे जिम्मेदार व शक्तिशाली नियमावली रही है। यह आपसी समझौते की प्रक्रिया को तीन चरणों में पूर्ण कराती है इसीलिए इसको 3-way authentication भी कहते हैं। जो वस्तु किसी बातचीत की शुरुआत करना चाहता है वो केंद्रीय प्राधिकारी से सम्पर्क स्थापित करता है तथा अपने एवं जिस वस्तु से उसे वार्तालाप स्थापित करना है उसका (दोनों का) पता केंद्रीय नियंत्रण कक्ष को बताता है। इसके बाद केंद्रीय कक्ष दोनों पक्षों को एक ही कूट संकेत अलग–अलग भेजता है। इस कूट संकेत के मिलान से दोनों पक्ष एक–दूसरे को सत्यापित करते हैं उसके बाद सामग्री का आदान–प्रदान शुरू करते हैं[5, 6]।

कूट सामग्री प्राप्त करने के लिए आवश्यक है कि वस्तुएं एक विशेष प्रकार की नियमावली को आत्मसात करें, जिसे Encryption Algorithms कहा जाता है। पूर्व में कई Encryption Algorithms इस कार्य के लिए प्रयोग में लाई जाती रही हैं। कुछ बहुत ही शक्तिशाली एवं सुरक्षित Encryption Algorithms इस प्रकार हैं: RSA, DES, AES, ECC,और Idea। जब भी कोई वस्तु अपनी संग्रहित आधार सामग्री को किसी और वस्तु या केंद्रीय कक्ष को भेजना चाहता है तो संचार माध्यम द्वारा भेजे जाने से पहले ही उस सामग्री

को उपरोक्त में से किसी एक नियमावली से होकर जाना पड़ता है। यह नियमावली भेजे जाने वाली सामग्री के वास्तविक वाक्यों को कूट संकेतों की मदद से कूट वाक्य में बदल देती है। इस कूट वाक्य को तार या तार–रहित संचार माध्यमों से दूसरे वस्तु या केंद्रीय कक्ष को भेजे जाने पर इनके चुराए जाने की सम्भावना शून्य हो जाती है[7]।

एकल अभिकलित्र परिवेश के दृष्टिगत यह तीनों प्रकार की नियमावलियाँ बहुत ही अच्छा कार्य कर रही हैं और इसमें कोई संदेह नहीं कि इन नियमावलियों के मदद से उपयोगकर्ता व्यक्ति अपने बहुत से कार्य बिना संदेह प्रतिपादित करते आ रहे हैं। परन्तु, "वस्तुओं का अंतर्जाल" एक नई परिकल्पना है जिसमें कि बहुत ही छोटे आकार के वस्तु आपस में एक–दूसरे से वार्तालाप या आधार–सामग्री का आदान–प्रदान करना चाहते हैं। इनके सुरक्षित आदान–प्रदान का वातावरण देना ही "वस्तुओं का अंतर्जाल" परिवेश की प्रमुख चुनौती है। यह इसलिए भी और कठिन हो जाती है क्योंकि पूर्व में स्थापित लगभग सभी अच्छी से अच्छी नियमावलियाँ इस नयी परिस्थिति में सही कार्य नहीं कर पा रही हैं। ऐसा इसलिए है क्योंकि पूर्व में स्थापित लगभग सभी नियमावलियां अत्यधिक जटिल थीं, जिनके सुगम परिचालन के लिए अबाध्य विद्युत आपूर्ति या अधिक ऊर्जा संग्रह की जरूरत थी[8]। "वस्तुओं का अंतर्जाल" वातावरण में विभिन्न प्रकार के संचार को **आकृति–२** में दर्शाया गया है।



आकृति २: "वस्तुओं का अंतर्जाल" वातावरण में संचार

"वस्तुओं का अंतर्जाल" परिवेश में उपस्थित वस्तुओं के पास ऊर्जा का संग्रह करने की क्षमता बहुत ही कम होती है। "वस्तुओं का अंतर्जाल" की संरचना के दृष्टिगत बहुतायत वस्तुओं में अबाध्य ऊर्जा का कोई स्रोत नहीं दिया जा सकता है। यही कारण है कि पूर्व में स्थापित समस्त नियमावलियों को अब नए तरीके से पुर्नस्थापित करने की आवश्यकता है। इस क्रम में कई शोधपत्र भी प्रस्तुत किये जा चुके हैं। देश एवं विदेश के भी अनेकोनेक शोधार्थी अब इसी कार्य में लगे हुए हैं कि किस प्रकार एक अत्यंत सुरक्षित और शक्तिशाली कम भार वहन करने वाली नियमावली बनाई जाय जो कि "वस्तुओं का अंतर्जाल" वातावरण के अनुरूप कार्य कर सके[9, 10]।

प्रस्तुत आलेख में शोधार्थी उन सभी चुनिंदा नियमावलियों के बारे में विस्तार से चर्चा करेंगे जो की कम भार वहन करने वाले हैं तथा वस्तुओं का अंतर्जाल वातावरण के लिए पूर्ण रूप से सुरक्षित हैं। आगे के क्रम में, दूसरे भाग में, लेखक पूर्व में प्रस्तुत शोधपत्रों की संछिप्त जानकारी प्रस्तुत करेंगे। तृतीय भाग में कुछ प्रमुख नीतियों को लेकर चर्चा प्रस्तुत की जायेगी जो की इन नियमावलियों के बनाये जाने में उपयोग में ली गई हैं। आवश्यक और अनिवार्य परीक्षण भाग चार में उल्लिखित किये गए हैं। भाग पांच में लेखकगण ने प्रस्तुत शोधपत्र का निष्कर्ष लिखा है।

2. **पूर्व में प्रस्तुत शोधपत्र**– विश्वस्तर के अनेक गणितज्ञों ने अपने शोध पत्रों में उल्लेख किया है कि सबसे कम विद्युत की आवश्यकता shift operations में होती है। इसी के दृष्टिगत shift operations के आधार पर कूट निकालने के कई प्रयास किये गये। इसी कूट के आधार पर किसी भी सरल वाक्य को कूट वाक्य में परिवर्तित किया जाता है। उत्पत्ति के समय में इस प्रयोजन के लिएlinear feedback shift registers (LFSRs) को प्रयोग में लाया गया। समय के साथ कई और भी तकनीक विकसित की गई। इस शोधपत्र में लेखक सभी प्रमुख तकनीकियों के बारे में विस्तार से चर्चा करेंगे। विभिन्न शोधपत्रों से पता चलता है कि सबसे ज्यादा सुरक्षा प्रदान करने वाली

नियमावलियां random numbers और hash functions तकनीकी का उपयोग करते हैं। Hash functions के द्वारा वस्तुओं के बीच भविष्य में की जाने वाली बातों को तो सुरक्षित किया ही जाता है इसके साथ ही नियमावलियां पूर्व में हुए वार्तालापों को भी सुरक्षित रख पाती हैं। वहीं random number एक विशेष प्रकार की अनियमित संख्या होती है जिसके द्वारा भेजे जाने वाले वाक्यों को कूट वाक्यों में परिवर्तित किया जाता है। प्रस्तुत शोधपत्र में शोधार्थी विभिन्न pseudo random numbers और light weight hash constructions के बारे में भी विस्तार से चर्चा करेंगे।

2.1. **PRNG आधारित नियमावलियां**– PRNG (Pseudo Random Number Generator) एक ऐसी तकनीकी है जो एक जटिल गणितीय क्रिया द्वारा एक अनियमित कूट संख्या की उत्पत्ति करती है। इस कूट का प्रयोग वास्तविक वाक्यों को कूट वाक्यों में बदलने के लिए किया जाता है। PRNG पर आश्रित विभिन्न नियमावलियों का संक्षिप्त विवरण निम्नलिखित है–

2.1.1 **ची एवं अन्य काPRNG**– सन २००८ में चार शोधकर्ताओं के एक दल ने १६ चरण LFSR और oscillator आधारित TRNG के समन्वय से प्राप्त होने वाली एक नई PRNG की संकल्पना प्रस्तुत की। इस संकल्पना में वर्णित TRNG एक analog circuit पर आधारित थी जो कि तापीय ऊर्जा संयंत्र के ध्वनि को आधार मानकर कार्य करता है। इस TRNG द्वारा भेजी गई एक bit को LFSR के सभी १६ bit से XOR कराया जाता है, जिससे कि सही अनियमितता की प्राप्ति हो। इस प्रकार १६ घड़ी–चक्रों में एक १६ bit का random number प्राप्त होता है। चूँकि ची एवं अन्य की बनावट सीधी है इसीलिए मेलिया–से जुई एवं अन्य द्वारा इस पर सुरक्षा आघात किया गया। यह आघात "(n+1)/8n" की सम्भावना से सफल भी सिद्ध हुआ जिसमे कि "n" उपयोग में ली गई LFSR की लम्बाई है[11]।

2.1.2 **मेलिया–सेजुई एवं अन्य का PRNG**– सन २०१० में मेलिया–से जुई एवं अन्य ने ची एवं अन्य का ही प्रस्तावित प्रारूप कुछ एक बदलावों के साथ प्रस्तुत किया, जिसे J3 Gen के नाम से जाना गया। जैसे कि एक ही बहुपद के उपयोग की जगह इन्होंने आठ भिन्न–भिन्न बहुपदों के उपयोग को चुना। इन आठ बहुपदों में से एक बार में कोई एक ही बहुपद चुनने की प्रक्रिया के लिए एक विशेष प्रकार के गूढ़–चक्र का उपयोग किया जाता है। इसकी विशेषता यह होती है कि यह हर बार अलग–अलग बहुपद को ही चुनता है। इस प्रकार १६ घड़ी–चक्रों में एक १६ bit का random number प्राप्त होता है जिसका प्रत्येक bit भिन्न बहुपद की उत्पत्ति होती है। यह ची एवं अन्य से अधिक सुरक्षित है।

2.1.3 **पेरिस–लोपेज एवं अन्य का PRNG**– सन २००६ में पेरिस–लोपेज एवं अन्य ने LAMED नाम का एक PRNG प्रस्तुत किया। आतंरिक पदों को पूर्ण करने के लिए ये bit wise XOR operation, modular algebra और bit rotation की मदद लेता है। LAMED का एक आतंरिक पद ६४ bit का होता है जिसमें ३२ bit की key और ३२ bit का Initial Vector (IV) होता है। अन्यथा की स्थिति में IV की जगह और ३२ bit की key का उपयोग किया जा सकता है। LAMED हमेशा ३२ bit का random number ही बनाता है। अगर किसी प्रयोजन के लिए १६ bit के random number की आवश्यकता होती है तो ३२ bit को ही दो १६ bit में तोड़कर और उन्हें XOR करके १६ bit का random number प्राप्त किया जा सकता है[14]।

2.1.4 **मंडल एवं अन्य काPRNG**– सन २०११ में मंडल एवं अन्य ने एक कम भार वहन करने वाली बनावट Warbler प्रस्तुत की जो कि कम खपत RFID Tags के लिए PRNG का निर्माण करती है। इसके द्वारा निर्मित PRNG, NLFSR (Non Linear Feedback Shift Registers) पर निर्भर करती है। इस PRNG की बनावट में तीन NLFSR का प्रयोग होता है जिसमे की एक १७ bit, दूसरा १८ bit, और तीसरा ६ bit का होता है। इस PRNG का आतंरिक पद ६५ bit का होता है जिसमे की ४५ bit का secret seed और २० bit का IV लिया जाता है। इस PRNG की बनावट ३६ घड़ी–चक्रों में key initialization और ८० घड़ी–चक्रों में running phase को पूर्ण करती है। इस बनावट के द्वारा निर्गत random number १६ bit की होती है जो कि विशेष रूप से EPC Class-1 Gen-2 मानक के अनुरूप तैयार की जाती है[15]।

2.1.5 **चैन एवं अन्य का PRNG**– सन् २०१५ में चैन एवं अन्य ने दो तरह के सुझाव प्रस्तुत किये जो कि J3 Gen की बनावट को आधार मान कर बुने गए थे। पहले सुझाव में लेखक ने बहुपद चयन चक्र को चलाने के लिए एक decoding logic लगाने की बात कही। यह decoding logic एक TRNG द्वारा प्राप्त होता है और इसी decoding logic से अंत में (output से ठीक पहले) एक XOR की क्रिया उस bit से कराने की बात कही जो की LFSR के एक क्रिया के बाद प्राप्त होती है। इस प्रकार के समन्वय से लेखक अपनी बनावट द्वारा निर्गत random number के पूरी तरह से अनियमित होने की बात सिद्ध करते हैं। दूसरे सुझाव में लेखक बहुपद चयन चक्र को दो भागों में पृथक करने की बात करते हैं जिसमें कि पहले बहुपद चयन चक्र में ५ बहुपद तथा दूसरे बहुपद चयन चक्र में ३ बहुपद रखने की बात कही गई है। इस बनावट में २ LFSR का उपयोग किया गया है जिसमें कि पहला बहुपद चयन चक्र पहले LFSR को तथा दूसरा बहुपद चयन चक्र दूसरे LFSR को अपना निर्णय साझा करते हैं। अंत में दोनों LFSR की output bit को XOR करके आगे की क्रिया के लिए प्रेषित करते हैं[16]।

3.1 **हैश फंक्शन आधारित नियमावलियां**– हैश क्रियाओं को मुख्य रूप से authentication के लिए प्रयोग में लाया जाता है जैसे कि message authentication code। Cryptography के प्रारम्भिक युग में जो नियमावलियां हैश क्रियाओं के लिए प्रचलन में थीं उनमें से MD5 और SHA सर्वाधिक पसंद किये गये। "वस्तुओं का अंतर्जाल" वातावरण की बढ़ती लोकप्रियता को देखते हुए इसे हैश क्रियाओं द्वारा सुरक्षित किये जाने का निर्णय लिया गया। इस वातावरण में प्रयोग किये जाने से पहले हैश क्रियाओं में कुछ एक बदलाव करके Light

weight Hash क्रियाएं बनाई गईं। इस कार्य के सम्पादन हेतु भिन्न–भिन्न तरीके प्रयोग में लाये गये जिनमें की sponge construction सबसे उपयुक्त पाया गया। Sponge आधारित कुछ Hash Constructions का संक्षिप्त विवरण निम्नवत है।

3.1.1 **क्वार्क (Quark)**– Quark एक कम भार वहन करने वाली हैश क्रिया है जो की Grain और Katan के क्रियाओं पर आधारित है। क्वार्क के तीन दृष्टान्त प्रस्तुत किये गयें जो क्रमशः U-Quark, S-Quark और D-Quark के नाम से जाने जाते हैं। Quark स्वयं में एक कम भार वहन करने वाली नियमावली है उसमें से भी इसके तीनों दृष्टांतों में सबसे कम भार वहन करने वाली नियमावली U-Quark है। Quark की बनावट में दो NLFSR और एक LFSR तीन गैर–रैखिक क्रियाओं द्वारा संचालित होते हैं। एक बार क्रिया शुरू हो जाने पर b-bit माप के states के लिए output state प्राप्ति हेतु आतंरिक state को 4b बार update करना होता है। State update की प्रक्रिया में LFSR update एक रैखिक Boolean क्रिया पर आधारित होता है जबकि NLFSRs का update तीन गैर–रैखिक Boolean क्रियाओं पर आधारित होता है। इन सबके अतिरिक्त एक पृथक गैर–रैखिक Boolean क्रिया दोनों NLFSRs को एक साथ प्रभावित करने के लिए प्रयोग में लाई जाती है। पूर्णतया Sponge Construction पर आधारित होने के कारण Quark 2^c preimage resistance और $2^{c/2}$collision और second preimage resistance की सुविधा प्रदान करता है[17]।

3.1.2 **स्पॉन्जेन्ट (Spongent)**– स्पॉन्जेन्ट की बनावट एक वृहद् PRESENT समरूप क्रमसंचय पर आधारित है। स्पॉन्जेन्ट किसी भी आकार के input को ग्रहण करके नियत आकार का output ही निर्गत करता है। Spongent के विभिन्न दृष्टांतों को Spongent-n/c/r की मदद से जाना जा सकता है। आकार n, क्षमता c,और दर r के अनुसार स्पॉन्जेन्ट के विभिन्न दृष्टांतों को पृथक किया जा सकता है। स्पॉन्जेन्ट के पाँच दृष्टान्त इस प्रकार हैं, SPONGENT-88/88/40, SPONGENT-128/128/64, SPONGENT-160/160/80, SPONGENT-224/224/112, और SPONGENT-256/256/128। सुरक्षा के दृष्टिकोण से Spongent को वो सभी ताकतें अपने आप ही मिल जाती हैं जो की PRESENT में पहले से ही उपस्थित होती हैं। Spongent के विभिन्न दृष्टान्त सुचारु रूप से क्रिया करने के लिए ASIC पर क्रमशः 738, 1016, 1329, 1728 और 1950 GE का क्षेत्र लेते हैं[18]।

3.1.3 **फोटॉन (Photon)**– फोटॉन एक विशेष प्रकार का हार्डवेयर उन्मुखी कम भार वहन करने वाला स्पॉन्ज आधारित हैश क्रिया है। इसका आतंरिक भाग एक matrix की तरह प्रदर्शित किया गया है जिसमें हर एक प्रविष्टि या तो ४ bit की या ८ bit की होती है। क्रमचय के लिए फोटॉन एक fix key का उपयोग करता है जैसा की AES में पहले से होता आया है। फोटॉन की संरचना में कुल १२–चरण होते हैं जिनमें चार मुख्य क्रियाएं Add Constant, Sub Cells, Shift Rows और AES समान Mix Coloum Serial सम्मिलित हैं। फोटॉन के दृष्टान्तों को समझने के लिए इन्हें PHOTON-n/r/r' के रूप में प्रदर्शित किया जाता है। फोटॉन के पाँच दृष्टान्त इस प्रकार हैं, PHOTON-80/20/16, PHOTON-128/16/16, PHOTON-160/36/36, PHOTON-224/32/32, और PHOTON-256/32/32। ये दृष्टान्त क्रमशः P_{100}, P_{144}, P_{196}, P_{256},और P_{288}आतंरिक क्रमचय का उपयोग करते हैं[19–20]।

3.1.4 **ग्लूऑन (Gluon)**– ग्लूऑन एक कम भार वहन करने वाली हैश क्रिया है जो की दो stream ciphers F-FCSR-v3 और X-FCSR-v2 पर आधारित है। ग्लूऑन की बनावट एक word ring FCSR को सम्मिलित करती है जो की एक main shift register और एक carry register पर आधारित होता है। ग्लूऑन के तीन दृष्टान्त प्रस्तुत किये गये जो क्रमशः Gluon-128/8, Gluon 160/16 और Gluon 224/32 थें। विभिन्न दृष्टांतों के लिए ग्लूऑन परिवार का area requirement क्रमशः 2071 GE, 2800 GE और 4724 GE पाया गया[21]।

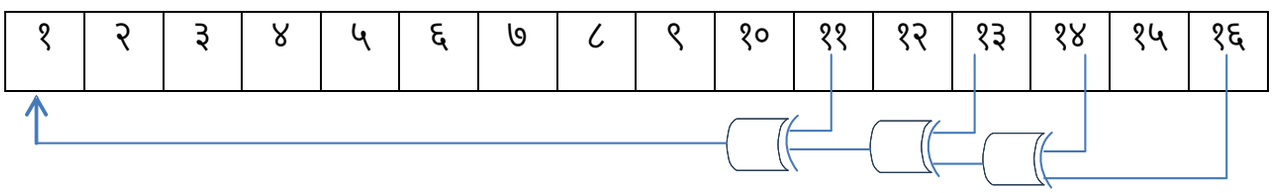
3.1.5 **हैश–वन (Hash-One)**– हैश–वन की बनावट में एक आतंरिक पद १६१ bit का होता है जिसमे की ८० bit और ८१ bit के दो NLFSR कार्य करते हैं। हैश–वन में प्रयुक्त १६१ bit प्राथमिक रूप से गणितीय स्थिर मान Pi का binary समरूप होता है। आतंरिक पद अद्यतन की क्रिया दो गैर–रैखिक Boolean क्रियाओं और एक रैखिक Boolean क्रिया के माध्यम से संपन्न कराई जाती है जिसमें कि गैर–रैखिक Boolean क्रिया ४ चर मानों द्वारा तथा रैखिक Boolean क्रिया ३ चर मानों द्वारा संचालित होती है। गैर–रैखिक Boolean क्रियायें दोनों NLFSR को अलग अलग अद्यतन के लिए प्रयोग में लाई जाती हैं जबकि रैखिक Boolean क्रिया दोनों NLFSR को एक साथ अद्यतन के लिए प्रयोग में लाई जाती है[22]।

4. **उपयोग में लाई गई प्रमुख नीतियाँ**– सुरक्षा सम्बंधित कम भार वहन करने वाली उपरोक्त नियमावलियां विश्वस्तर पर प्रमाणित हैं तथा कई बार अलग–अलग तरह के आक्षेपों को झेल चुकी हैं। इन नियमावलियों की सुरक्षा विभिन्न मानकों के आधार पर सर्वोत्तम पाई गई हैं तथा ये अधिक जटिल और वजनी भी नहीं हैं। इन नियमावलियों के बनावट में मुख्य रूप से दो तकनिकी कार्य करती हैं जिनमे पहली है LFSR और दूसरी है Sponge Construction। प्रस्तुत शोध पत्र के इस भाग में लेखकगण दोनों तकनीकियों को लेकर विस्तृत चर्चा प्रस्तुत कर रहे हैं।

4.1 **एल.एफ.एस.आर. (LFSR-Linear Feedback Shift Register)**– एल.एफ.एस.आर (रैखिक प्रतिक्रिया पारी लेखा) एक विशेष प्रकार की पारी लेखा है जिसमे निविष्ट bit इसके पुराने पद की एक रैखिक क्रिया होती है। किसी भी एल.एफ.एस.आर. के प्राथमिक भाग को मूल कहते हैं। इस मूल को एक रैखिक क्रिया के द्वारा अगले मान में परिवर्तित किया जाता है जो कि एक नियतात्मक प्रक्रिया होने के कारण पहले से ही निश्चित की जा सकती है। क्योंकि लेखायें सीमित आकार की होती हैं इसीलिए एल.एफ.एस.आर. से निर्गत परिणाम भी कुछ समय के बाद पुनरावृत्ति करने लग जाते हैं। अगर किसी प्रयोजन के लिए लम्बे समय तक न दुहराए जाने वाले मान चाहिए तो एल.

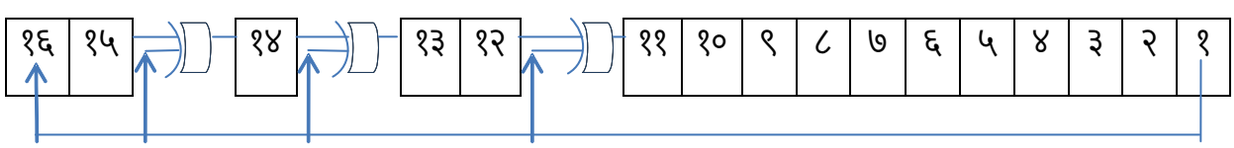
एफ.एस.आर. में उपयोग की जाने वाली लेखा की क्षमता उसी अनुसार ज्यादा लेनी चाहिए[23]।
एल.एफ.एस.आर.का प्रयोग हार्डवेयर और सॉफ्टवेयर दोनों मदों में किया जा सकता है। मुख्य रूप से इसका प्रयोग छद्म अनियमित संख्या, छद्म ध्वनि अनुक्रम, तीव्र डिजिटल गणनाफलक, और whitening अनुक्रम के लिए किया जाता है। कालांतर में कई प्रकार के एल.एफ. एस.आर. प्रयोग में लाये गयें जिनमे Fibonacci और Galios प्रमुख थे।

4.1.1 **फिबोनैक्की एल.एफ.एस.आर.(Fibonacci LFSR)**– मुख्यतः १६ बिट के होते हैं। इन १६ बिट में से जो बिट्स निर्णय को प्रभावित करते हैं उन्हें taps कहा जाता है। उदहारण के लिए, अगर प्रतिक्रिया बहुपद X^{16}, X^{14}, X^{13}, X^{11}, १ लिया गया है तो इसका तात्पर्य है की १, ११, १३, १४, और १६ वें पद tap पद की तरह प्रयोग किये जाएंगे। किसी भी एल.एफ.एस.आर. का सबसे दाहिना पद निर्गत पद कहा जाता है। प्राथमिक मान के १६वें बिट को एक–एक करके १४वें, १३वें, और ११वें पद के साथ XOR किया जाता है और जो मान प्राप्त होता है उसे बाएं की ओर से पहले स्थान पर रखकर बाकी के सभी मानों को एक–एक पद दाहिनी ओर खिसका देते हैं। इस प्रकार प्राप्त अंतिम पद, जो कि पूर्व में १६वें स्थान पर होती है, को अब निर्गत मान की तरह प्रयोग में ले लिया जाता है। इस प्रकार से १६–चरणों के बाद १६ bit का एक अनुक्रम निर्गत होता है। **आकृति–३** एक १६ बिट्स का फिबोनैक्की एल.एफ.एस.आर. दर्शाती है।



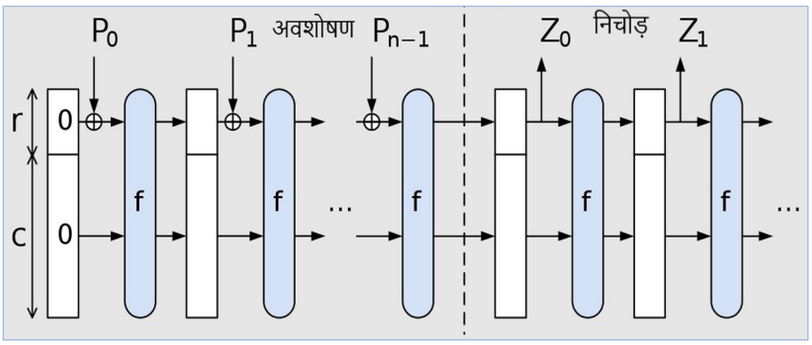
आकृति–३: एक १६ बिट्स का फिबोनैक्की एल.एफ.एस.आर.

4.1.2 **गैलॉइस एल.एफ.एस.आर. (Galois LFSR)**– गैलॉइस एल.एफ.एस.आर. भी मुख्यतः १६ bit का ही होता है। इसे modular LFSR, internal XORs LFSR, या one-to-many LFSR के नाम से भी जाना जाता है। उदहारण के लिए, यहाँ भी पूर्व में दर्शाये हुए प्रतिक्रिया बहुपद X^{16}, X^{14}, X^{13}, X^{11}, १ का प्रयोग ही देखते हैं। गैलॉइस एल.एफ.एस.आर. में प्रथम पद के मान को निर्गत करके इसे १६वें स्थान में डाल देते हैं और क्रमशः एक–एक पद दक्षिण की तरफ सरकाते हुए १४वें, १३वें, व ११वें स्थान में नए मान प्रविष्ट कराते हैं जो की क्रमशः १५वें, १४वें, व १२वें, स्थान के मानों को पहले स्थान के मान से XOR के बाद प्राप्त होते हैं। गैलॉइस एल.एफ.एस.आर. की एक मुख्य विशेषता यह है कि इसमें अगर निर्गत बिट शून्य (०) होती है तो सभी मान बिना बदले हुए ही एक–एक स्थान दाहिनी ओर खिसक जाते हैं तथा निविष्ट बिट भी शून्य (०) हो जाती है एवं जब निर्गत बिट एक (१) होती है तो tap positions के बिट–मान बदल जाते हैं (अगर १ है तो ० हो जाता है और अगर ० है तो १ हो जाता है) और सभी के सभी मान एक–एक स्थान दाहिनी ओर खिसक जाते हैं तथा निविष्ट बिट भी १ हो जाता है। **आकृति–४** एक १६ बिट का गैलॉइस एल.एफ.एस.आर. दर्शाती है।



आकृति–४: एक १६ बिट का गैलॉइस एल.एफ.एस.आर

4.1.3 **स्पॉन्ज गठन**– स्पॉन्ज गठन एक सरल आवर्ती रचना है जो की परिवर्तनीय लम्बाई का निवेश लेता है एवं मनमाने लम्बाई का उत्पाद देता है। यह एक क्रमसंचय की क्रिया पर कार्य करता है जिसमें एक मान की कुल लम्बाई b बिट्स होती है। आतंरिक पदों का आकार $b = (r + c) >= n$ से प्राप्त किया जा सकता है जिसमें की r दर को, c क्षमता को, और b चौड़ाई को दर्शाता है। स्पॉन्ज गठन की प्रक्रिया तीन चरणों में पूर्ण होती है, प्रारम्भिक, अवशोषित, और निचोड़ चरण[19]। स्पॉन्ज गठन की प्रक्रिया **आकृति–५** में दर्शायी गई है।



आकृति–५: स्पॉन्ज गठन

प्रारम्भिक चरण में वास्तविक सन्देश के binary समरूप को दर r के गुणक में लाने के लिए (अगर आवश्यक हो तो) padding की जाती है। Padding करते समय ध्यान रखना है कि वास्तविक सन्देश के अंतिम बिट के बाद पहले १ जोड़ना है और फिर आवश्यकतानुसार ० जोड़ते चले जाना है। जब सन्देश के बिट्स की लम्बाई दर r के गुणक में आ जाय तब padding का कार्य रोक देना चाहिए। उदाहरण के लिए, अगर सन्देश है "9" तो इसका समरूप हुआ (111001), अब यदि दर है ८–बिट की तो इस सन्देश को padding की आवश्यकता पड़ेगी क्योंकि यह सन्देश ६–बिट का है जो की ८ का गुणक नहीं है। इस प्रकार से परिवर्तित सन्देश का binary समरूप 11100110 होगा। इस प्रक्रिया में सबसे पहले ७वें स्थान पर 1 जोड़ा गया और फिर 8वें स्थान पर 0 जोड़ा गया। जब यह ८ के गुणक में आ गया तो padding की क्रिया रोक दी गई।

अवशोषित चरण में प्रारम्भिक चरण द्वारा प्राप्त r-bit के निविष्ट खण्डों को पूर्व में उपस्थित r-bit के साथ XOR किया जाता है। ये XO Red मान आगे की अवशोषित चरणों में r-bit का क्रमसंचय करते रहते हैं। सबसे अंत में निचोड़ चरण में अवशोषित क्रिया द्वारा प्राप्त प्रथम r-bitनिर्गत किया जाता है। यह सम्पूर्ण sponge की क्रिया का निर्गत मान होता है और तब तक r-bit के मान को निर्गत करते रहते हैं जब तक की कुल मान n-bit का न हो जाय।

5. **आवश्यक और अनिवार्य परीक्षण**– "वस्तुओं का अंतर्जाल" वातावरण नए प्रकार से निर्मित वस्तुओं के बीच सुरक्षित एवं सुगम वार्तालाप को बढ़ावा देने के लिए प्रतिबद्ध है। इस कारण जो भी कम भार वहन करने वाली नियमावलियाँ प्रस्तुत की जाती हैं उनका EPC C1 G2 से अनुरूपता होना आवश्यक होता है एवं जो कूट उपयोग में लाये जाते हैं उनका NIST द्वारा परीक्षण अनिवार्य होता है। प्रस्तुत शोधपत्र के इस भाग में लेखकगण NIST और EPC C1 G2 के बारे में विस्तृत चर्चा प्रस्तुत कर रहे हैं।

5.1 निस्ट (**NIST-National Institute of Statistics and Technology)**– राष्ट्रीय सांख्यिकी और प्रौद्योगिकी संस्थान संयुक्त राज्य के वाणिज्य विभाग की एक संस्था है, जिसकी स्थापना ३ मार्च १९०१ को संयुक्त राज्य समागम में की गई थी। यह संस्था "वस्तुओं का अंतर्जाल" वातावरण में सुरक्षा की दृष्टि से उपयोग में लाये जाने वाले कूट का परीक्षण करती है। अगर किसी प्रस्तुत बनावट द्वारा निर्गत कूट निस्ट का परीक्षण उत्तीर्ण करता है तब ही उसका उपयोग सुरक्षा नियमावलियों में किया जा सकता है[24]। निस्ट की परीक्षण रचना १५ अलग–अलग परीक्षणों का एक संकलन है। निस्ट का पहला परीक्षण The frequency (Monobit) test है जो कि पूरे अनुक्रम में ० और १ की उपस्थिति का परीक्षण करता है। अगर पूरे अनुक्रम में ० और १ की उपस्थिति लगभग बराबर है तो ही यह परीक्षण उत्तीर्ण माना जाता है। दूसरा परीक्षण एक नियत लम्बाई के खण्ड के अन्दर आवृत्ति का परीक्षण करता है। तीसरा परीक्षण यह देखता है कि एक साथ कितने ० या कितने १ आ रहे हैं। चौथा परीक्षण सबसे लम्बे अनुक्रम (जो की १ का ही हो) के बारे में जानकारी देता है। परीक्षणों की पूरी जानकारी **तालिका–१** में दी गई है।

तालिका–१: निस्टके परीक्षण

परीक्षण क्रमांक	परीक्षण का नाम
पहला परीक्षण	Frequency (Monobit) test
दूसरा परीक्षण	Test for frequency within a block
तीसरा परीक्षण	Runs test
चौथा परीक्षण	Test for the longest runs of 1s in a block

पांचवा परीक्षण	Random binary matrix rank test
छठवां परीक्षण	Discrete Fourier transform (spectral) test
सातवां परिक्षण	Non-overlapping (Aperiodic) tempelate matching test
आठवां परिक्षण	Overlapping (Periodic) tempelate matching test
नौवां परिक्षण	Maurer's universal statistical test
दसवां परिक्षण	Linear complexity test
ग्यारहवां परिक्षण	Serial test
बारहवां परिक्षण	Approximate entropy test
तेरहवां परिक्षण	Cumulative sums (cusums) test
चौदहवां परिक्षण	Random excursion test
पन्द्रहवां परिक्षण	Random excursions varient test

5.2 **ई.पी.सी. ग्लोबल (EPC global)**– EPC global GS1 और GS1US के मध्य एक संयुक्त उद्यम है। यह १ नवम्बर २००३ में संयुक्त राज्य में स्थापित किया गया था। इसकी स्थापना का मुख्य उद्देश्य "वस्तुओं का अंतर्जाल" वातावरण में RFID के उपयोग को सहारा देकर RFID के उपयोग को बढ़ावा देना था। RFID "वस्तुओं का अंतर्जाल वातावरण" का एक महत्वपूर्ण अंग माना जाता है। RFID एक छोटे आकार का यंत्र होता है जिसकी भण्डारण तथा तरंग संचार क्षमता बहुत ही कम होती है और यह अबाध्य ऊर्जा के स्रोत से भी नहीं जुड़ा होता है। कोई भी नियमावली RFID पर लागू करने से पहले EPC global उनकी योग्यता परीक्षण कराती है। जो नियमावली GS1 मानक को पूरा करते हैं केवल उन्ही को "वस्तुओं का अंतर्जाल" वातावरण में प्रयोग की अनुमति प्रदान की जाती है। "वस्तुओं का अंतर्जाल" वातावरण की बुनियाद स्थापित करने के लिए GS1 ने "व्यापार की अंतर्राष्ट्रीय भाषा" नाम का एक कार्यक्रम प्रारम्भ किया जो कि भौतिक और डिजिटल दुनिया को एक दूसरे से जोड़ने के लिए कार्य करती है। "वस्तुओं का अंतर्जाल" वातावरण की मुख्य आवश्यकता GS1 bar code और EPC / RFID द्वारा संचालित वस्तुओं, परिसम्पत्तियों, और स्थानों की अद्वितीय पहचान स्थापित करना तथा automatic data capture करना है[14]।

6. **निष्कर्ष**– संगणक विज्ञान के अंतर्गत "वस्तुओं का अंतर्जाल" एक नया वातावरण है जिसमें छोटे–छोटे वस्तुओं को अभिकलन की मुख्य धारा से जोड़ने का कार्य किया जाता है। यह वस्तुएं भौतिक जगत में सामान्य रूप से उपयोग में लाई जाने वाली कोई भी वस्तु हो सकती हैं। क्योंकि ये वस्तुएं आकार में छोटी होती हैं इसलिए इनमें उपस्थित नियमावलियाँ भी छोटी व कम भार वहन करने वाली ही उपयोग में लाई जा सकती हैं। ऐसा इसलिए है क्योंकि इन वस्तुओं में एक tiny OS कार्य करता है जो अधिक जटिल नियमावलियों के लिए कार्य करने में समर्थ नहीं होता है। साथ ही साथ, क्योंकि इन वस्तुओं की भण्डारण क्षमता व तरंग संचार की क्षमता भी कम होती है इसलिए "वस्तुओं का अंतर्जाल" वातावरण में उपयोग की जाने वाली छोटी–छोटी वस्तुओं की संख्या बहुत अधिक होती है। अधिक संख्या में होने के कारण परस्पर वार्तालाप भी अधिक होते हैं जो की सुरक्षा के दृष्टिकोण से सही नहीं है। अनेक शोधार्थियों द्वारा इन छोटे–छोटे वस्तुओं को वार्तालाप के लिए एक सुरक्षित वातावरण देने के प्रयास से कई नियमावलियों का गठन किया गया जो कि पी.आर.एन.जी. और स्पॉन्ज गठन की क्रिया पर आधारित थे। क्योंकि कई बार वस्तुओं को ऐसी जगह पर कार्य करना पड़ जाता है जहाँ पर अबाध्य ऊर्जा का कोई स्रोत नहीं होता है इसलिए इन वस्तुओं पर जो नियमावलियाँ लगाई जाती हैं उन्हें कुछ परीक्षणों से होकर जाना पड़ता है जिनमें कि निस्ट परीक्षण और ई.पी.सी. ग्लोबल की नियमावली प्रमुख हैं। "वस्तुओं का अंतर्जाल" वातावरण पूर्ण रूप से अभिकलन की एक नई विधा है जिसमे शोधार्थियों के लिए अनेकोनेक सम्भावनाये हैं। शोधार्थी वातावरण की सुरक्षा, वस्तुओं का अद्वितीय पहचान, परस्पर वार्तालाप प्रमाणीकरण जैसे अनेक दिशा में कार्य कर सकते हैं।

परिशिष्ट–१: शब्दावली

क्र0सं0	अंग्रेजी	हिन्दी
1	Internet of Things	वस्तुओं का अंतर्जाल
2	Data	आधार–सामग्री
3	Storage	भंडारण
4	Transmission	तरंग संचार
5	Lightweight	कम–भार–वहन / हल्का
6	Algorithm	चरण बद्ध आचरण
7	Application	उपयोग
8	Network	संजाल
9	Sensing	संवेदन
10	Sensor	ग्रहण कर्ता
11	Code	कूट
12	Gateway	प्रवेश द्वार
13	Pseudo Random Number	छद्म अनियमित संख्या
14	Pseudo Noise	छद्म ध्वनि अनुक्रम
15	Linear feedback shift registers	रैखिक प्रतिक्रिया पारी लेखा
16	National Institute of Statistics and Technology	राष्ट्रीय सांख्यिकी और प्रौद्योगिकी संस्थान
17	Mutual Authentication	आपसी समझौता
18	Computing	अभिकलन
19	Unique	अद्वितीय
20	Complex	जटिल
21	Input	निविष्ट
22	Insert	प्रविष्ट
23	Output	निर्गत
24	Permutation	क्रमसंचय
25	Absorbing	अवशोषित
26	Squeezing	निचोड़
27	Attack	आक्षेप
28	Constant	स्थिरमान
29	Non-Linear	गैर–रैखिक
30	Updation	अद्यतन
31	Instance	दृष्टान्त
32	Polynomial	बहुपद

References

1. Gupta, D. N.; Kumar, R. and Kumar, A. (2020) Efficient Encryption Techniques for Data Transmission Through the Internet of Things Devices,IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks, 1st ed., V. Jain, O. Kaiwartya, N. Singh, and R. S. Rao, Eds. Pennsylvania, United States: IGI Global, pp. 203228.
2. Kan, R.; Khan, S. U.; Zaheer, R. and Khan, S. (2012) Future internet: The internet of things architecture, possible applications and key challenges, Proc. - 10th Int. Conf. Front. Inf. Technol. FIT pp. 257260.DOI: 10.1109/FIT.2012.53.
3. Huth, C.; Zibuschka,J.; Duplys, P. and Güneysu, T. (2015) Securing systems on the Internet of Things via physical properties of devices and communications, 9th Annu. IEEE Int. Syst. Conf. Proc., pp. 813.DOI: 10.1109/SYSCON.2015.7116721.
4. Nozaki, Y. and Yoshikawa, M. (2019) Countermeasure of lightweight physical unclonable function against side-channel attack,Proc. - 2019 Cybersecurity Cyberforensics Conf. CCC 2019, no. Ccc, pp. 3034.DOI: 10.1109/CCC.2019.00-13.
5. Ben Saied, Y. and Olivereau, A.(2012) D-HIP: A distributed key exchange scheme for HIP-based Internet of Things, 2012 IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM Digit. Proc.DOI: 10.1109/WoWMoM.2012.6263785.
6. Goyal, T. K. and Sahula,V. (2016) Lightweight security algorithm for low power IoT devices, Int. Conf. Adv. Comput. Commun. Informatics, ICACCI, pp. 17251729.DOI: 10.1109/ICACCI.2016.7732296.
7. Gupta, D. N.and Kumar, R. (2020)Generating Random Binary Bit Sequences for Secure Communications between Constraint Devices under the IOT Environment,INCET, pp. 16.
8. Naru,E. R.; Saini, H. and Rathee, G. (2017) Proposed IoT framework using third party with enhanced security,4th IEEE Int. Conf. Signal Process. Comput. Control. ISPCC 2017, vol. 2017-January, pp. 621626, DOI: 10.1109/ISPCC.2017.8269752.
9. Schaumont, P. (2017) Security in the Internet of Things: A challenge of scale,Proc. 2017 Des. Autom. Test Eur, pp. 674679. DOI: 10.23919/DATE.2017.7927075.
10. Gupta, D. N. and Kumar, R. (2019) Lightweight Cryptography : an IoT Perspective,Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 8, pp. 700706. https://www.ijitee.org/download/volume-8-issue-8/.
11. Che, W.; Deng, H.; Tan, W. and Wang, J. (2008) A random number generator for application in RFID tags, Networked RFID Syst. Light. Cryptogr. Rais. Barriers to Prod. Counterfeiting First Ed., pp. 279287,DOI: 10.1007/978-3-540-71641-9_16.
12. Melia-Segui,J.; Garcia-Alfaro,J. and Herrera-Joancomarti, J. (2010) Analysis and improvement of a pseudorandom number generator for EPC Gen2 tags, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6054, LNCS, pp. 3446. DOI: 10.1007/978-3-642-14992-4_4.
13. Melià-Seguí, J.; Garcia-Alfaro, J. and Herrera-Joancomartí, J. (2011) A practical implementation attack on weak pseudorandom number generator designs for EPC Gen2 tags," Wirel. Pers. Commun., vol. 59, no. 1, pp. 2742, DOI: 10.1007/s11277-010-0187-1.
14. Peris-Lopez, P.; Hernandez-Castro, J. C.; Estevez-Tapiador, J. M. and Ribagorda, A. (2009) AMED - A PRNG for EPC Class-1 Generation-2 RFID specification," Comput. Stand. Interfaces, vol. 31, no. 1, pp. 8897, DOI: 10.1016/j.csi.2007.11.013.
15. Mandal, K.; Fan, X. and Gong, G.(2016) arbler: A Lightweight Pseudorandom Number Generator for EPC C1 Gen2 Passive RFID Tags, Int. J. RFID Secur. Cryptogr., vol. 2, no. 2, pp. 8291, DOI: 10.20533/ijrfidsc.2046.3715.2013.0011.
16. Chen,J.; Miyaj,A.; Sato, H. and Su, C. (2015) Improved lightweight pseudo-random number generators for the low-cost RFID tags,Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust., vol. 1, pp. 1724.DOI: 10.1109/Trustcom.2015.352.
17. Aumasson,J. P.; Henzen,L.; Meier, W. and Naya-Plasencia, M. (2013) Quark: A lightweight hash, J. Cryptol., vol. 26, no. 2, pp. 313339. DOI: 10.1007/s00145-012-9125-6.
18. Zhang,W.; Bao, Z.; Rijmen, V. and Liu, M. (2015) A new classification of 4-bit optimal s-boxes and its application to PRESENT, RECTANGLE and SPONGENT,Lect. Notes Comput. Sci. (including Subser. Lect.

Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9054, pp. 494515.DOI: 10.1007/978-3-662-48116-5_24.
19. Guo, J.; Peyrin, T. and Poschmann, A. (2000) The PHOTON Lightweight Hash Functions Family,Crypto, pp. 222239. http://dblp.uni-trier.de/db/conf/crypto/crypto2011.html#GuoPP11.
20. Guo, J.; Peyrin, T. and Poschmann, A. (2011) The PHOTON family of lightweight hash functions," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6841 LNCS, pp. 222239. DOI: 10.1007/978-3-642-22792-9_13.
21.Berger, T. P.; DHayer, J.; Marquet, K.; Minier, M. and Thomas, G. (2012) The GLUON family: lightweight hash function family based on FCSRs," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7374 LNCS, pp. 306323.DOI: 10.1007/978-3-642-31410-0_19.
22.Manayankath, S.; Srinivasan, C.; Sethumadhavan, M. and Mukundan, P. Megha (2016) Hash-One: a lightweight cryptographic hash function," IET Inf. Secur., vol. 10, no. 5, pp. 225231, DOI: 10.1049/iet-ifs.2015.0385.
23. Page, E. C. C.(2003) Linear Feedback Shift Registers (LFSRs) 4-bit LFSR Applications of LFSRs Galois Fields - the theory behind LFSRs Galois Fields - The theory behind LFSRs Galois Fields - The theory behind LFSRs Galois Fields - The theory behind LFSRs Building an LFSR fro.
24. Rukhin,A.; Soto,J. and Nechvatal, J. (2010) SP800-22rev1a, no. April, p. 131.