DOR: https://csj.isi.org.ir/article_245088.html

DOI : https://doi.org/10.22034/csj.2026.245088

بهار ۱۴۰۵، دوره ۱۱، شماره ۱، پیاپی ۴۰

دریافت مقاله: ۱۴۰۴/۰۵/۱۳

پذیرش مقاله: ۱۴۰۴/۰۶/۱۸

نوع مقاله: پژوهشی

یک الگوریتم رمزنگاری سبک وزن مبتنی بر Ascon و نظریه آشوب برای اینترنت اشیاء

محمد عرفان تنهایی

گروه مهندسی کامپیوتر، دانشکدهٔ فنی و مهندسی، دانشگاه بین‌المللی امام‌خمینی، قزوین، ایران

پست الکترونیکی: m.e.tanhaei79@gmail.com

نستوه طاهری جوان*

گروه مهندسی کامپیوتر، دانشکدهٔ فنی و مهندسی، دانشگاه بین‌المللی امام‌خمینی، قزوین، ایران

پست الکترونیکی: nastooh@eng.ikiu.ac.ir

چکیده

در سال‌های اخیر، توسعه گسترده اینترنت اشیاء (IoT) و به‌کارگیری دستگاه‌های کم‌مصرف، چالش‌های جدیدی در حوزه امنیت و حریم خصوصی پدید آورده است. در چنین بستری، رمزنگاری سبک وزن به‌عنوان رویکردی مؤثر برای محافظت از داده‌ها در دستگاه‌های دارای منابع محدود مطرح شده است. الگوریتم Ascon، که از سوی مؤسسه ملی استاندارد و فناوری ایالات متحده به‌عنوان استاندارد رمزنگاری سبک‌وزن برگزیده شده، یکی از راه‌حل‌های برجسته در این حوزه به‌شمار می‌رود. در این مقاله، با هدف ارتقای امنیت Ascon، یک جعبه جابه‌جایی آشوب‌محور ۵ بیتی معرفی می‌شود. بهره‌گیری از نظریه آشوب در طراحی این جعبه، موجب افزایش غیرخطی بودن و ایجاد ویژگی‌های آماری پیچیده می‌شود که مقاومت در برابر حملات تفاضلی و خطی را بهبود می‌بخشد. وابستگی به کلید رمز و کاهش پیچیدگی محاسباتی نیز از جمله مزایای کلیدی این طرح هستند. نتایج به‌دست آمده نشان می‌دهد که رویکرد پیشنهادی علاوه‌بر افزایش امنیت، عملکرد مناسبی را در دستگاه‌های کم منبع مانند حسگرها و برچسب‌های RFID ارائه می‌دهد و گزینه‌ای مناسب برای محیط‌های IoT محسوب می‌شود.

کلید واژه‌ها: رمزنگاری سبک وزن، نظریه آشوب، اینترنت اشیاء، Ascon، جعبه جابه‌جایی.

مقدمه

در دهه‌های اخیر، اینترنت اشیاء به سرعت در تمامی جنبه‌های زندگی روزمره نفوذ کرده و پیش‌بینی شده است که تا سال ۲۰۲۵ بیش از ۲۵ میلیارد دستگاه متصل به این شبکه وجود دارند [۱]. این دستگاه‌ها که از خانه‌های هوشمند گرفته تا شهرهای هوشمند، کشاورزی، مراقبت‌های پزشکی و مدیریت انرژی کاربرد دارند، قادر به تولید و انتقال داده‌هایی هستند که گاه حاوی اطلاعات حساس و خصوصی مانند سوابق پزشکی بیماران، تصاویر چهره افراد یا شماره پلاک خودروها می‌باشند [۲]. این حجم عظیم از داده‌ها، همراه با آسیب‌پذیری

* نویسندهٔ مسئول

دستگاه‌های اینترنت اشیاء در برابر حملاتی چون حملات انکار سرویس توزیع‌شده (DDos)، اهمیت امنیت و حریم خصوصی را بیش از پیش برجسته می‌کند [۳].

رمزنگاری روشی است که از گذشته برای حفاظت از اطلاعات حساس به‌کار گرفته شده است. در این فرایند متن اصلی (plaintext)، به شکلی ناخوانا به رمز (cipher) تبدیل می‌شود. این فرایند رمزگذاری نام دارد و فرایند معکوس یعنی رمزگشایی، متن رمز شده را به حالت اولیه باز می‌گرداند. هدف اصلی رمزنگاری تأمین امنیت ارتباطات از طریق تضمین محرمانگی، یکپارچگی و احراز هویت داده‌هاست [٤].

رمزنگاری سنتی به‌راحتی بر روی کارسازها، رایانه‌های شخصی و دستگاه‌های هوشمند مانند تلفن‌های همراه پیاده‌سازی می‌شود. با این حال با ظهور دستگاه‌هایی با منابع محدود مانند اینترنت اشیا، حسگرها، برچسب‌های شناسایی فرکانس رادیویی (RFID) و عملگرها که محدودیت‌هایی چون حافظه اندک، فضای فیزیکی کوچک برای پیاده‌سازی، توان محاسباتی پایین و مصرف انرژی محدود دارند، استفاده از الگوریتم‌های رمزنگاری را با چالش مواجه کرده است [٥]. اینجاست که رمزنگاری سبک وزن به‌عنوان نسخه‌ای بهینه شده و کم‌مصرف از رمزنگاری پدیدار می‌شود تا این چالش‌ها را به‌طور مؤثری برطرف سازد [٦].

در میان الگوریتم‌های رمزنگاری سبک‌وزن، Ascon به‌عنوان یک الگوریتم بهینه مطرح است. این الگوریتم که در سال ۲۰۱٤ معرفی شد و در سال ۲۰۲۳ توسط مؤسسه ملی استاندارد و فناوری (NIST) به‌عنوان استاندارد رمزنگاری سبک‌وزن انتخاب شد، بر پایه ساختار اسفنجی عمل می‌کند. طراحی ساده و انعطاف‌پذیر Ascon، همراه با استفاده از تبدیل‌های چرخشی شامل جعبهٔ جابه‌جایی (S-box) غیرخطی و لایه انتشار خطی، آن را به گزینه‌ای ایده‌آل برای دستگاه‌های کم مصرف تبدیل کرده است [۷].

یکی از اجزای حیاتی در الگوریتم‌های رمزنگاری، به‌خصوص در الگوریتم هایی مانند Ascon که از ساختارهای شبکه جایگزینی-جایگشتی بهره می‌برند، جعبه‌های جابه‌جایی[1] هستند. این مفهوم که نخستین بار توسط کلود شانون در سال ۱۹٤۹ معرفی شد، قلب فرایند جایگزینی در رمزنگاری است [۸]. جعبه جابه‌جایی با نگاشت هر عنصر از متن اصلی (بیت یا گروهی از بیت‌ها) به عنصری جدید، خاصیت گنگی را فراهم می‌کند و رابطه بین کلید و رمز را تا حد ممکن پیچیده می‌کند. در ادامه، عملیات جایگشتی با بازچینی عناصر، خاصیت انتشار را به ارمغان می‌آورد. قدرت یک الگوریتم رمزنگاری تا حد زیادی به معماری جعبه جابه‌جایی آن بستگی دارد. در رمزنگاری سبک وزن، جعبه جابه‌جایی‌های کوچک‌تر (مانند ٤ بیتی) به دلیل ساختار فشرده و سهولت پیاده‌سازی محبوبیت دارند، اما امنیت کمتری نسبت به جعبه جابه‌جایی‌های بزرگ‌تر (مانند ۸ بیتی) ارائه می‌دهند. از سوی دیگر جعبه جابه‌جایی‌های بزرگ‌تر اگرچه امن‌تر هستند، اما نیاز به منابع بیشتری دارند که برای دستگاه‌هایی با منابع محدود مناسب نیستند [٦].

در این راستا پژوهش حاضر بر بهبود الگوریتم Ascon با استفاده از جعبه‌های آشوبناک (Chaotic S-box) متمرکز است. این جعبه‌ها که بر پایه نظریه آشوب طراحی شده‌اند، با ایجاد رفتار غیرخطی و تصادفی، می‌توانند امنیت را تقویت کنند. نظریه آشوب، که از دهه ۱۹۸۰ در رمزنگاری مورد توجه قرار گرفته، به‌دلیل سادگی محاسباتی و قابلیت تولید الگوهای غیرقابل پیش‌بینی، ابزاری قدرتمند برای طراحی جعبه جابه‌جایی به‌شمار می‌رود [۹]. ما در این مقاله پیشنهاد یک جعبه جابه‌جایی آشوبناک ٥ بیتی را مطرح می‌کنیم که با بهره‌گیری از نظریه آشوب، تعادلی میان امنیت و کارایی برقرار می‌کند. این رویکرد نه تنها برای پیام‌های کوتاه در دستگاه‌های اینترنت اشیاء مناسب است، بلکه با اندازه‌های مختلف بلوک سازگار است.

روش پیشنهادی چندین مزیت و نوآوری کلیدی ارائه می‌دهد:

1-Substitution Box (s-box)

● امنیت تقویت‌شده: استفاده از نگاشت آشوبناک با پارامترهای بهینه شده، غیرخطی بودن جعبه جابه‌جایی را افزایش می‌دهد و مقاومت را در برابر حملات تفاضلی و خطی بهبود می‌بخشد.

● وابستگی به کلید: استخراج مقدار اولیه از کلید، جعبه جابه‌جایی را به کلید رمزنگاری وابسته می‌کند، که امنیت پویا را تقویت می‌کند.

● کارایی محاسباتی: پیش‌محاسبه جعبه و استفاده از نگاشت‌های آشوبناک ساده، بار محاسباتی را کاهش داده و روش را برای دستگاه‌های کم‌مصرف مانند حسگرها و برچسب‌های RFID مناسب می‌سازد.

ادامهٔ این مقاله به شرح زیر سازماندهی شده است: بخش ۲ به مرور کارهای مرتبط با این پژوهش اختصاص دارد. در بخش ۳ رویکرد پیشنهادی ارائه شده است. سپس، بخش ٤ عملکرد اولیه این راه‌کار را ارزیابی می‌کند. در نهایت، بخش ٥ مقاله با نتیجه‌گیری و ارائه پیشنهادهایی برای کارهای آینده به پایان می‌رسد.

۲- پژوهش‌های مرتبط

الگوریتم‌های رمزنگاری سبک‌وزن زیادی برای انتقال امن اطلاعات در دستگاه‌های اینترنت اشیا معرفی شده‌اند که در این بخش تعدادی از آنها مرور می‌شوند. در [۱۰] یک الگوریتم رمزنگاری سبک‌وزن ارائه شده است که از یک کلید دی‌ان‌ای استفاده می‌کند. داده‌های ورودی به شکل ماتریس دو بعدی تبدیل می‌شوند و سپس از ترکیب سطر و ستون با کلید در هر مرحله برای تولید کلید مرحله استفاده می‌شود. این روش به علت استفاده نکردن از یک جعبه جابه‌جایی قوی، مشکلات خطی بودن و افشای کلید در استفاده طولانی مدت دارد.

در [۱۱] محققان به‌جای استفاده از یک جعبه جابه‌جایی، از یک MLFSR استفاده می‌کنند تا فضای پیاده‌سازی و مصرف انرژی کاهش یابد. همچنین الگوریتم از یک ساختار جابه‌جایی- جایگشتی استفاده می‌کند. این الگوریتم به علت استفاده کردن از MLFSR خاصیت پویایی را ندارد و در استفاده مداوم مشکلات افشای کلید را دارد. مدهیل و همکارانش [۱۲] از یک عدد بزرگ به‌عنوان کلید استفاده کردند و از کلید برای گردش و جایگشت تصادفی در هر مرحله از حلقه استفاده شد. در روش آن‌ها اندازه ورودی داده‌های خام و تعداد مراحل اجرا الگوریتم متغیر است و باید از قبل تعیین شود. اگر اندازه داده‌های ورودی کوچک باشد این الگوریتم سرعت بیشتری دارد و مصرف کمتری نسبت به سایر الگوریتم‌های سبک‌وزن دارد.

این الگوریتم نسبت به حملات همه‌جانبه ضعف دارد و هر چقدر بلوک داده‌های ورودی کوچک‌تر باشد، این الگوریتم ضعیف‌تر عمل می‌کند. در [۱۳]، یک روش رمزنگاری تصویر از یک دنباله شبه‌تصادفی مبتنی بر آشوب با استفاده از شبکهٔ عصبی استفاده شده است. علاوه بر استفاده از عملیات جایگشتی و جایگزینی، بیت دی‌ان‌ای برای نگاشت بیت‌های پیکسل تصاویر رمزنگاری شده استفاده شده است. طرح رمزنگاری متقارن پیشنهادی در [۱٤] از سیستم‌های پویا آشوبناک چندگانه استفاده می‌کند. در این روش، کلید با هر داده ورودی بروزرسانی می‌شود تا سطح بالاتری از تصادفی بودن فراهم کند. ترکیب عملیات جایگشتی، جایگزینی و نگاشت DNA موجب افزایش میزان آنتروپی تصاویر رمزنگاری شده و مقدار آنتروپی خروجی نزدیک به ۷/۹۹ بیت گزارش شده است که تقریباً به حد ایده‌آل ۸ نزدیک است.

نویسندگان در [۱٥] یک پیکربندی تجربی از یک کریپتوسیستم مبتنی بر آشوب برای معماری مبتنی بر اینترنت اشیاء در شبکه‌های ad-hoc ارائه کرده‌اند. این راه‌حل از ویژگی‌های عملگر مشتق مرتبه کسری برای رمزنگاری بهره می‌برد تا ارتباطات امن را ایجاد کند. الگوریتم PRINT [۱٦] که به‌طور اختصاصی برای چاپ مدار مجتمع (IC) طراحی شده است، کوچکترین جعبه جابه‌جایی با ابعاد ۳ بیتی را ارائه می‌دهد. این الگوریتم به‌دلیل پیاده‌سازی مقرون به‌صرفه بر روی برچسب‌های RFID بسیار کم هزینه است

و از نظر سخت‌افزاری و نرم‌افزاری کارآمد است. در عین حال، به‌دلیل تعداد کم احتمالات جعبه جابه‌جایی مختلف، در برابر حملات آسیب‌پذیر است. در این رویکرد در مقابل حملات از نوع invariant subspace، برای کلیدهای ضعیف، با افزایش تعداد دور تغییری در امنیت ایجاد نمی‌شود.

الگوریتم PRESENT که در [۱۷] معرفی شده از جعبه جابه‌جایی ٤ بیتی استفاده می‌کند. این الگوریتم بر سیستم عددی شانزده‌شانزدهی تکیه دارد و در هر لایه جابه‌جایی حالتی را به‌صورت شانزده کلمه ٤ بیتی تشکیل می‌دهد. این طراحی امکان ایجاد حداکثر ۸۰٦٤ طرح جعبه جابه‌جایی مختلف را فراهم می‌کند [۱۸]. این الگوریتم در برابر تحلیل رمزنگاری تفاضلی آسیب‌پذیر است [۱۹]. این طراحی ساده و کم‌مصرف است، اما مطالعات رمزکاوی نشان داده‌اند که در برابر تحلیل تفاضلی آسیب‌پذیر است و در مقابل پیاده‌سازی سخت‌افزاری PRESENT آن را به یکی از کم‌هزینه‌ترین گزینه‌های رمزنگاری سبک‌وزن تبدیل کرده است. کومار و همکارانش [۲۰] با استفاده از الگوریتم PRESENT و بهینه‌سازی جعبه جابه‌جایی توانستند فضای پیاده‌سازی را کاهش بدهند ولی روش پیاده‌سازی باعث کاهش شدید سرعت شد.

قمصیه و همکاران [۲۱] یک طرح رمزنگاری ترکیبی پیشنهاد کردند که ترکیبی از الگوریتم‌های رمزنگاری جریانی و بلوکی است. راه‌حل پیشنهادی مبتنی بر یک مدل ریاضی بهبود یافته است تا سطح امنیتی مورد نیاز با سرعت رمزنگاری بالا به‌دست آید. کریپتوسیستم مبتنی بر آشوب از نسخه بهبود یافته نگاشت Skew tent به‌عنوان لایه جابه‌جایی در این روش استفاده شده است. نتایج شبیه‌سازی نشان دادند که با هر ورودی، کلید به‌صورت پویا به‌روزرسانی می‌شود و در نتیجه سطح تصادفی بودن و مقاومت در برابر حملات آماری افزایش می‌یابد. از سوی دیگر میزان آنتروپی کلیدهای تولید شده در این روش بیش از ۷/۹۹ بیت گزارش شده و آزمون‌های NIST نشان داده‌اند که خروجی‌ها تقریباً توزیع یکنواخت دارند.

مزیت کلیدی این رویکرد، افزایش امنیت در عین حفظ سرعت رمزنگاری بالاست، که آن را برای محیط‌های IoT مناسب‌تر از بسیاری روش‌های صرفاً بلوکی می‌سازد.

در [۲۲] محققان یک جعبه جابه‌جایی ٥ بیتی طراحی کردند که از دو سطر به طول ١٦ تشکیل شده است. برای تولید این جعبه جابه‌جایی تابع آشوب لاجستیک بهبود یافته به‌کار گرفته شده است. آنها این جعبه جابه‌جایی را با جعبه‌های جابه‌جایی سایر الگوریتم‌های رمزنگاری سبک مقایسه کردند که عملکرد آن بهبود داشت.

الگوریتم رمزنگاری PRIMATE [۲۳] از ساختار مبتنی بر جایگشت استفاده می‌کند. این الگوریتم برای رمزنگاری احراز هویت شده و توابع درهم‌ساز بهینه شده است و با جعبه جابه‌جایی ٥ بیتی و اندازه حالت ۸۰ تا ۲۰۰ بیت، امنیت بالا و مصرف انرژی کم را ارائه می‌دهد. PRIMATE در برابر حملات رمزگشایی مقاوم و برای کاربردهایی مانند خانه‌های هوشمند مناسب است. پیاده‌سازی سبک آن در سخت‌افزار و نرم‌افزار، کارایی را در محیط‌های محدود تضمین می‌کند.

الگوریتم ICEPOLE که در سال ۲۰۱٤ معرفی شد، یک رمز احراز هویت‌شده سبک‌وزن با طراحی بهینه برای پیاده‌سازی سخت‌افزاری است [۲٤]. این الگوریتم بر پایه چارچوب دوپلکس و یک جایگشت ۱۲۸۰ بیتی عمل می‌کند و نسخه اصلی آن از کلید و نانس[۲] ۱۲۸ بیتی بهره می‌برد. ساختار ICEPOLE شامل پنج مرحله رمزگذاری است که با الهام از Keccak طراحی شده و برای بهبود امنیت و کاهش هزینه سخت‌افزاری اصلاح شده‌اند. داده‌ها در بلوک‌های ۱۰۲٤ بیتی پردازش و در نهایت به برچسب ۱۲۸ بیتی ختم می‌شوند، بدون نیاز به معکوس‌سازی جایگشت در رمزگشایی. از نظر امنیتی، ICEPOLE در برابر حملات مختلف از جمله تفاضلی، خطی و تحلیل‌های چرخشی مقاوم است و حتی در برابر بازاستفاده محدود نانس نیز محافظت ارائه می‌دهد. در عمل ICEPOLE برای کاربردهای نیازمند سرعت زیاد مناسب است، اما پیچیدگی و ردپای

2-Nonce

سـخت‌افزاری آن مانع استفاده در گره‌های بسیار کم‌منبع IoT می‌شود.

بـرخی از رویکردهای مرتبط در جـدول ۱ با یکدیگر مقایسـه شـده‌اند. با توجه به کارهای انجام شده می‌توان به اهمیت رمزنگاری سـبک وزن در اینترنت اشیاء پی برد. همچنین جعبه جابه‌جایی که به‌عنوان هستهٔ این الگوریتم‌ها برای ایجاد رابطه غیرخطی بین کلید و داده ورودی استفاده می‌شود، باید به‌طوری طراحی شود که در عین کارآمدی، پیچیدگی را نیز حفظ کند.

۳- راهکار پیشنهادی

علی‌رغم پیشـرفت‌های اخیـر در طـراحی جعبه‌های جابه‌جایی، بسیاری از طرح‌های موجود برای کاربردهای سـبک وزن، از نظـر امنیتی ناکافی هسـتند یـا پیچیدگی محاسـباتی بالایی دارند که با محدودیت‌های دستگاه‌های اینترنت اشیاء سـازگار نیسـت. علاوه بر این، استفاده از جعبه جابه‌جایی‌های ثابت و غیر وابسـته به کلید می‌تواند الگوهای قابل اسـتخراجی را برای مهاجمان ایجاد کند، که امنیت کلی سیسـتم را به خطر می‌اندازد. به‌طور خلاصه، انگیزه این پژوهش از نیاز به طراحی جعبه‌های جابه‌جایی با امنیت بالا، نیاز محاسباتی مناسب، و انعطاف‌پذیری برای کاربردهای سـبک وزن ناشی می‌شـود. با بهره‌گیری از سیستم‌های آشوبناک و ادغام آنها با Ascon، این پژوهش به‌دنبال ارائه راه‌حلی نوآورانه است که ضمن حفظ کارایی، مقاومت رمزنگاری را در برابر طیف گسترده‌ای از حملات تقویـت کند. بخش‌های بعـدی این مقالـه، جزئیات روش پیشـنهادی، تحلیل امنیتی و مقایسه با طرح‌های موجود را ارائـه خواهند داد تا پتانسیل ایـن رویکرد در بهبود امنیت رمزنگاری سبک‌وزن به‌طور جامع بررسی شود.

با توجـه به اهمیت رمزنـگاری سـبک‌وزن در تأمین امنیت دسـتگاه‌های اینترنت اشیاء و نقش کلیدی جعبه‌های جابه‌جـایی در الگوریتم‌هایی مانند Ascon، در این پژوهش یک روش نوین برای طراحی یک جعبه جابه‌جایی آشوبناک ۵ بیتی پیشـنهاد می‌شود که با ساختار Ascon ادغام شده تا امنیت و کارایی را بهبود ببخشد. این روش با بهره‌گیری از ویژگی‌های سیستم‌های آشوبناک به دنبال ایجاد تعادل بین خاصیت گنگی، مصرف منابع پایین و مقاومت در برابر حملات رمزنگاری است.

● ساختار Ascon در رویکرد پیشهادی

Ascon یک الگوریتم رمزنگاری سبک‌وزن متقارن است که در سـال ۲۰۱۴ طراحی شـد و در سـال ۲۰۲۳ توسط مؤسسه ملی اسـتاندارد و فناوری ایالات متحده به‌عنوان اسـتاندارد رمزنگاری سبک‌وزن انتخاب شد. این الگوریتم به‌دلیل تعادل مناسب میان امنیت، کارایی و مصرف منابع، به‌ویژه برای دستگاه‌های کم‌منبع مانند حسگرهای پزشکی، خانه‌های هوشمند و گره‌های اینترنت اشیاء بسیار مناسب اسـت. Ascon از رمزنگاری احراز هویت‌شده، رمزنگاری جریانی و توابع درهم‌ساز سـبک‌وزن پشتیبانی می‌کند و انعطاف‌پذیری بالایی در پاسخ به نیازهای متنوع محیط‌های IoT دارد. نسـخه‌های مختلفی از Ascon ارائه شـده‌اند، از جمله: Ascon-128 (اسـتاندارد)، Ascon-128a (با سـرعت بالاتر)، Ascon-80pq (مقاوم در برابر حملات کوانتومی) و Ascon-hash (برای توابع درهم‌سـاز سبک‌وزن). این تنوع نسـخه‌ها باعث تطبیق‌پذیری Ascon با کاربردهای مختلف شده است.

سـاختار Ascon استفاده شـده در رویکرد پیشنهادی بر پایه معماری اسـفنجی بنا شده که از یک تابع جایگشت مرکـزی برای پردازش داده‌ها بهـره می‌برد. حالت داخلی آن ۳۲۰ بیت اسـت که به دو بخـش «نرخ» (برای ورودی/ خروجی) و «ظرفیت» (برای تأمین امنیت) تقسیم می‌شود.

تابع جایگشـت Ascon در راهکار پیشـنهادی شـامل سـه مرحله اسـت: افزودن مقادیر ثابت بـرای جلوگیری از الگوهای تکراری، اسـتفاده از جعبه‌هـای جابه‌جایی ۵ بیتی جهت ایجاد غیرخطی‌بودن و اعمال لایه خطی شـامل چرخش‌ها و جابه‌جایی‌های بیتی برای تقویت انتشـار. این

طراحی ساده، به‌ویژه در پیاده‌سازی‌های سخت‌افزاری و نرم‌افزاری با منابع محدود، بسیار کارآمد و کم‌مصرف است.

فرایند رمزنگاری در Ascon در رویکرد پیشنهادی شامل چهار مرحله کلیدی است: مقداردهی اولیه با کلید و نانس، پردازش داده‌های مرتبط برای احراز هویت، رمزنگاری یا رمزگشایی متن اصلی با تابع جایگشت و عملیات XOR، و در نهایت تولید برچسب احراز هویت برای تضمین اصالت و یکپارچگی پیام. همچنین، در حالت رمزنگاری جریانی، Ascon امکان رمزنگاری داده‌های پیوسته را فراهم می‌سازد که آن را برای داده‌های لحظه‌ای در کاربردهای IoT بسیار مناسب می‌کند.

● مقداردهی توابع آشوب در رویکرد پیشنهادی

برای تحلیل دقیق رفتار سیستم آشوبی مورد استفاده در این پژوهش، از نمودارهای دوشاخه‌ای[3] و نمای لیاپانوف[4] بهره گرفته شده است. نمودار دوشاخه‌ای ابزاری قدرتمند در تحلیل سیستم‌های دینامیکی غیرخطی است که نحوه تغییر رفتار یک سیستم را در پاسخ به تغییرات پارامترهای کنترلی نشان می‌دهد. این نمودار به‌ویژه در نمایش گذار سیستم از رفتار منظم و تناوبی به رفتار آشوبناک اهمیت دارد و به وضوح مرز میان نظم و بی‌نظمی را آشکار می‌سازد. از سوی دیگر، نمودار نمای لیاپانوف، حساسیت سیستم به شرایط اولیه را ارزیابی می‌کند. در این تحلیل، مقدار مثبت نمای لیاپانوف شاخصی از رفتار آشوبناک سیستم بوده و بیانگر واگرایی شدید مسیرهای مجاور در فضای فاز است، در حالی که مقادیر منفی این نما نشان‌دهنده پایداری نسبی و رفتار تناوبی سیستم می‌باشد.

در این پژوهش، هر دو نمودار یادشده برای نگاشت آشوبی منتخب رسم شده‌اند تا رفتار دینامیکی آنها در بازه‌ای از پارامترهای کنترلی بررسی شود. استفاده از این نمودارها امکان تحلیل دقیق‌تری از ویژگی‌های آشوبی هر نگاشت را فراهم کرده و به انتخاب بهینه‌ترین پارامتر تابع برای تولید دنباله‌های رمزنگاری کمک کرده است. شکل ۱ نمودار دو شاخه‌ای و نمای لیاپانوف را برای رویکرد پیشنهادی نشان می‌دهد.

در مورد نگاشت لجستیک، رفتار سیستم به‌شدت به مقدار پارامتر کنترلی r وابسته است. با افزایش مقدار μ و نزدیک شدن آن به عدد ٤، سیستم به‌تدریج از حالت‌های پایدار و تناوبی عبور کرده و وارد ناحیه‌ای با رفتار کاملاً آشوبناک می‌شود. این تغییرات در رفتار سیستم به‌خوبی از طریق نمودار دوشاخه‌ای و همچنین نمای لیاپانوف قابل مشاهده است. به‌طور مشخص، با افزایش مقدار μ به سمت ٤، نمای لیاپانوف از مقادیر منفی به سمت مقادیر مثبت میل می‌کند و در نهایت برای $\mu = ۴$ مقداری مثبت خواهد داشت که نشان‌دهنده بیشینه شدن حساسیت سیستم به شرایط اولیه و آشوبناک بودن کامل رفتار آن است. بر این اساس، در این پژوهش برای بهره‌گیری از حداکثر ویژگی‌های آشوبی نگاشت لجستیک، مقدار پارامتر کنترلی $\mu = ۴$ در نظر گرفته شده است تا تولید دنباله‌ای با بیشترین پیچیدگی و تصادفی بودن ممکن فراهم گردد.

● طراحی جعبه جابه‌جایی پیشنهادی

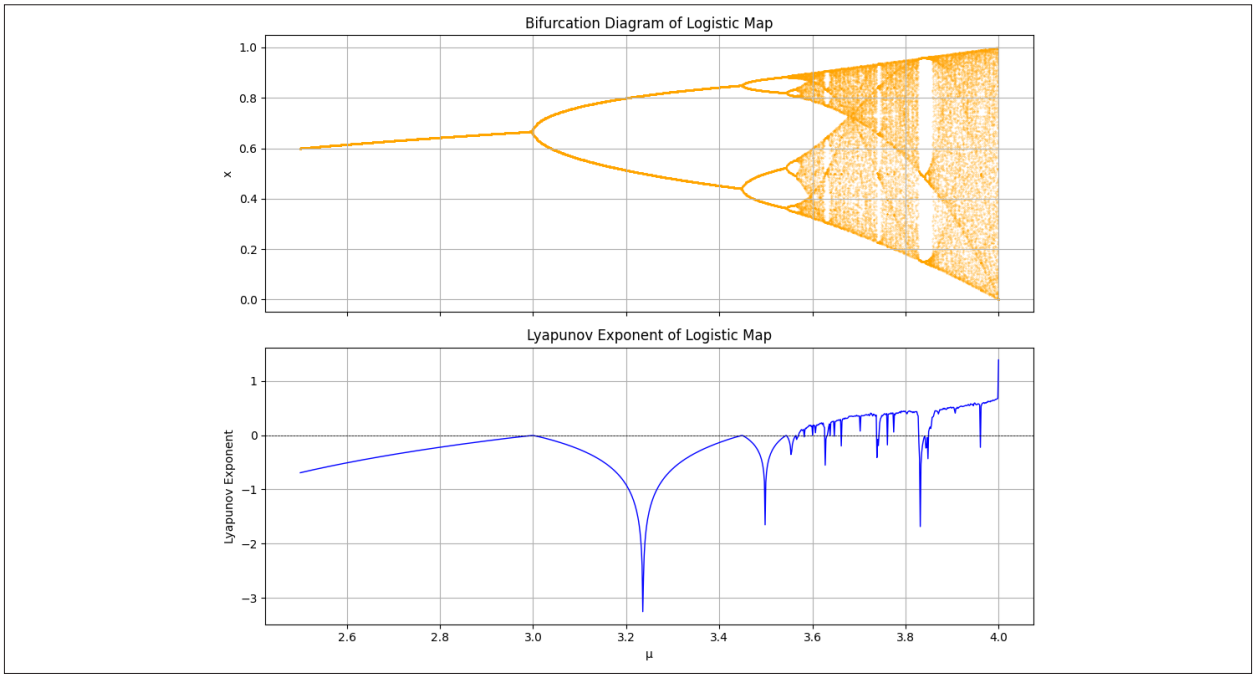
جعبه جابه‌جایی پیشنهادی یک نگاشت از فضای ورودی ۵ بیتی به فضای خروجی ۵ بیتی تعریف می‌کند:

(۱)

$$S : \{۰,۱\}^۵ \rightarrow \{۰,۱\}^۵ : x \rightarrow S(x)$$

این تابع قادر است ۳۲ ورودی ۵ بیتی ($۲^۵ = ۳۲$) را به ۳۲ خروجی یکتا نگاشت کند، که تعداد کل حالات تصادفی ممکن برای این نگاشت برابر با $۳۲! \approx ۲.۶ * ۱۰^{۳۵}$ است. این تنوع عظیم، امکان تولید جعبه‌های جایگزینی با رفتار غیرقابل پیش‌بینی را فراهم می‌کند. مقادیر خروجی $S(x)$ به‌صورت پویا و بر اساس توابع آشوبناک تولید می‌شوند، که رفتار غیرخطی و تصادفی آنها تضمین‌کننده خاصیت

3-Bifurcation Diagram
4-Lyapunov Exponent



شکل ۱: نمودار تقسیمات دودویی و لیاپانوف نگاشت لجستیک

گنگی موردنیاز در رمزنگاری است.

در ایـن پژوهش برای تولید جعبـه جابه‌جایی، از تابع آشـوب لجسـتیک استفاده شـده اسـت. معادله این تابع به‌صورت زیر است:

(۲)

$$x_{n+1} = r x_n(1 - x_n)$$

این تابع از عملگرهای ساده استفاده می‌کند که می‌تواند به سـادگی در فضای محدود پیاده‌سـازی شـود. مقدار اولیه x_0 از کلید رمزنگاری اسـتخراج می‌شود، که این امر وابسـتگی جعبه جابه‌جایی به کلید را تقویت کرده و امنیت را افزایـش می‌دهد. الگوریتم پیشـنهادی برای تولید جعبه جابه‌جایی شامل مراحل زیر است:

- تنظیم پارامترهای ثابت: مقدار پارامتر کنترلی برای تابع لاجستیک تعیین می‌شود.
- مقداردهـی اولیه: مقـدار اولیه x_0 از کلیـد رمزنگاری اسـتخراج می‌شـود. این کلید می‌تواند بخشی از کلید ۱۲۸ بیتی Ascon یا یک مقدار مشتق شده باشد.

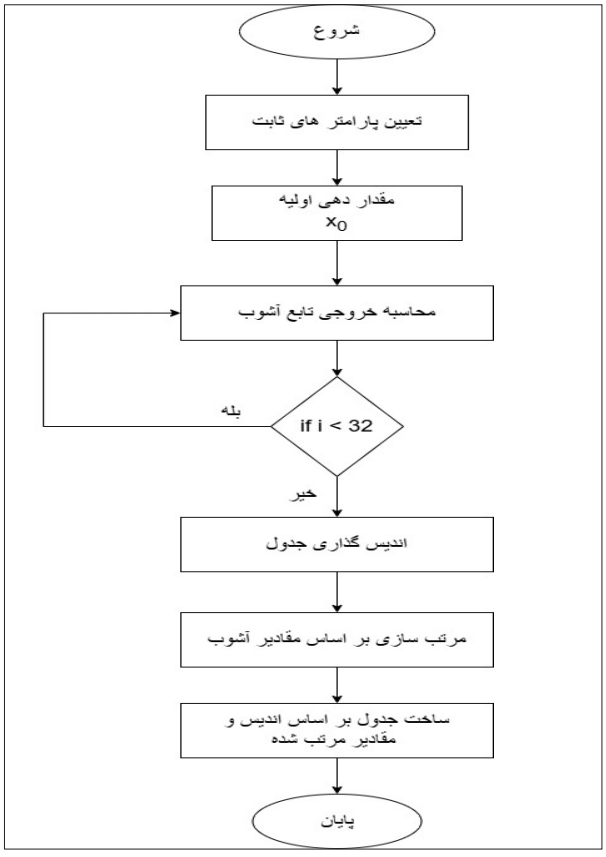
تولید دنباله آشوبناک: تابع نگاشت به‌صورت تکراری ۳۲ بار اجرا می‌شـود تا دنباله‌ای از ۳۲ مقدار آشـوبناک $(x_1, x_2, \ldots, x_{32})$ تولید شود.

- اندیس‌گذاری دنباله: هر مقدار x_i در دنباله با یک اندیس (i) برچسب‌گذاری می‌شود.
- مرتب‌سازی صعودی: دنباله بر اساس مقدار به‌صورت صعودی مرتب می‌شـوند و اندیس‌های مربوطه به‌عنوان خروجی‌های جعبه جابه‌جایی به ورودی‌های ۵ بیتی (۰ تا ۳۱) نگاشت می‌شوند.
- ذخیره جدول: جدول نهایی به‌صورت پیش محاسبه شده ذخیره می‌شود تا بار محاسباتی در زمان اجرا کاهش یابد.

این الگوریتـم به‌گونه‌ای طراحی شـده کـه با حداقل پیچیدگی محاسـباتی، جعبه جابه‌جایی‌های غیرخطی تولید کند. استفاده از مرتب‌سازی صعودی برای نگاشت مقادیر آشوبناک به خروجی‌های جعبه جابه‌جایی، توزیع یکنواخت و تصادفی را تضمین می‌کند.

- **پیاده‌سازی جعبه جابه‌جایی پیشـنهادی و ادغام با Ascon**

در الگوریتـم Ascon-128، لایـه جایگزیـنی ٦٤ بار به



شکل ۲: روندنمای ایجاد جعبه جابه‌جایی آشوبناک

صورت موازی، حالت ۳۲۰ بیتی را به‌روزرسانی می‌کنند. جعبه جابه‌جایی آشوبناک پیشنهادی جایگزین جعبه جابه‌جایی استاندارد Ascon می‌شود، بدون آن که تغییر در ساختار کلی جایگشتی (شامل لایه افزودن ثابت، جایگزینی و انتشار) ایجاد کند. برای اطمینان از کارایی، جدول جعبه جابه‌جایی به‌صورت پیش محاسبه شده در حافظه دستگاه ذخیره می‌شود، که این امر زمان اجرای رمزنگاری را به حداقل می‌رساند. برای این کار به ۱۶۰ بیت فضا برای ذخیره‌سازی جدول نیاز است که با محدودیت‌های حافظه دستگاه‌های اینترنت اشیاء سازگار است. این روش همچنین با اندازه‌های مختلف بلوک (۳۲، ٦٤ یا ۱۲۸ بیت) سازگار است، که انعطاف‌پذیری لازم برای کاربردهای متنوع اینترنت اشیاء را فراهم می‌کند. از نظر سرعت به‌دلیل استفاده از جدول از پیش محاسبه شده، تفاوتی با جعبه جابه‌جایی اصلی Ascon ندارد. شکل ۲ روندنمای رویکرد پیشنهادی را نشان می‌دهد.

۴- ارزیابی رویکرد پیشنهادی

در این بخش، عملکرد و امنیت الگوریتم پیشنهادی مورد ارزیابی قرار می‌گیرد. ابتدا سرعت و فضای موردنیاز آن بررسی می‌شود، سپس تحلیل امنیتی جامعی شامل معیارهایی مانند غیرخطی بودن، مقاومت در برابر حملات تفاضلی و خطی، و اثر بهمنی ارائه می‌گردد. این تحلیل‌ها بر پایه روش‌های استاندارد و آزمون‌های آماری انجام می‌شوند. در پایان، الگوریتم پیشنهادی با الگوریتم‌های سبک‌وزن رایج نظیر ICEPOLT [۲٤]، PRIMATE [۲۳] و Ascon استاندارد [۷] مقایسه می‌شود تا میزان کارایی و نوآوری آن در کاربردهای اینترنت اشیا مشخص گردد.

از زبان برنامه‌نویسی پایتون برای شبیه‌سازی و تحلیل‌های امنیتی استفاده شده است. تمامی کدها بر روی سیستم با مشخصات پردازنده intel core i7 13650 و 16GB حافظه اصلی اجرا شده است. بر اساس نمودارهای تقسیمات دودویی و لیاپانوف که در شکل ۱ آمده است، بیشترین آشوب با مقدار کنترلی $r = 4 r = 4$ رخ می‌دهد. مقدار اولیه $x.x.$ نیز کلید در نظر گرفته شده است، که می‌تواند از کلید اصلی الگوریتم استخراج یا از طریق فرایند مشتق‌سازی کلید تولید شود.

برای ارزیابی امنیت روش پیشنهادی، که شامل یک جعبه جابه‌جایی آشوبناک ۵ بیتی مبتنی بر نگاشت لجستیک است، معیارهای کلیدی رمزنگاری مانند خاصیت یک به یک، غیرخطی بودن و مقاومت در برابر حملات تفاضلی و خطی بررسی می‌شوند و برای تحلیل کارآیی رویکرد پیشنهادی در زمینهٔ سرعت، تاخیر رویکردهای مختلف با هم مقایسه شده‌اند.

۴-۱- مقایسهٔ سرعت اجرای رویکردها

برای اندازه‌گیری سرعت و مصرف انرژی روش استفاده شده، از شبیه‌سازی در محیط پایتون استفاده شده است. جدول ۲ مقایسه‌ایی از عملکرد سرعت با حجم داده‌های ورودی مختلف را نشان میدهد.

جدول ۲: مقایسه تاخیر الگوریتم‌ها

اندازهٔ بلوک	Ascon	رویکرد پیشنهادی	PRIMATE	ICEPOLT
۱۲۸	۰/۰۰۰۳۶۸	۰/۰۰۰۵۵۷	۰/۰۰۰۵۹۸	۰/۰۰۰۲۵
۱۰۲۴	۰/۰۰۱۸۰۴	۰/۰۰۳۲۴۳	۰/۰۰۵۴۲۱	۰/۰۰۲۰۳۶
۴۰۹۶	۰/۰۰۶۵۸۵	۰/۰۱۲۳۱۷	۰/۰۲۲۶۳۸	۰/۰۰۸۰۶۴
۱۶۳۸۴	۰/۰۲۸۰۸۹	۰۶۱۵۴۷	۰/۰۹۶۹۸۵	۰/۰۳۲۸۷۴

همان‌طور که از نتایج جدول ۲ مشخص است، الگوریتم Ascon دارای کمترین زمان اجرا در تمامی سطوح داده است. الگوریتم پیشنهادی عملکردی بسیار نزدیک به Ascon داشته و به‌ویژه در اندازه‌های پایین داده، تفاوت زمانی اندکی نشان می‌دهد. از سوی دیگر، الگوریتم PRIMATE در تمامی اندازه‌ها زمان اجرای بیشتری دارد، که بیانگر پیچیدگی بالاتر یا سربار محاسباتی بیشتر آن است. نتایج فوق نشان می‌دهند که روش پیشنهادی، با وجود به‌کارگیری ساختارهای پیچیده‌تر برای افزایش امنیت، همچنان از نظر کارایی در سطح قابل قبول و مناسبی قرار دارد.

۴-۲- خاصیت یک به یک

یک تابع را یک به یک می‌گویند اگر هر مقدار ورودی به یک مقدار خروجی یکتا نگاشت شود و هر مقدار خروجی دقیقاً یک مقدار ورودی متناظر داشته باشد. این خاصیت حیاتی است، زیرا تضمین می‌کند که جعبه جابه‌جایی معکوس‌پذیر بوده و تمام ۳۲ مقدار ممکن (۰ تا ۳۱) را در خروجی پوشش می‌دهد [۲۴]. جعبه جابه‌جایی پیشنهادی از طریق تحلیل وزن همینگ (Hamming weight) بررسی شده است.

وزن همینگ برای یک بردار خروجی $Y = (b_1, b_2, \dots, b_5)$ که در آن $b_i \in \{0,1\}$ به‌صورت زیر تعریف می‌شود: [۲۵]

$$H_w(Y) = \sum_{k=1}^{2^5} (b_1^k \oplus b_2^k \oplus \dots \oplus b_5^k) = 2^{5-1} \quad (۲)$$

دراینجا، $b_i \in \{0,1\}$ و بردار $(b_1, b_2, \dots, b_5) \neq (0,0,\dots,0)$ برای هر تابع بولی صدق می‌کند.

جدول ۳: مقادیر ورودی، خروجی، وزن همینگ و فاصله همینگ

ورودی	خروجی	H_d	H_w	ورودی	خروجی	H_d	H_w
۰۰۰۰۰	۰۰۱۰۱	۲	۰	۱۰۰۰۰	۱۱۰۱۱	۳	۰
۰۰۰۰۱	۰۰۱۱۰	۳	۰	۱۰۰۰۱	۱۰۱۱۱	۲	۰
۰۰۰۱۰	۰۰۱۱۱	۲	۱	۱۰۰۱۰	۰۰۰۱۱	۲	۰
۰۰۰۱۱	۰۱۰۰۰	۳	۱	۱۰۰۱۱	۰۱۱۱۰	۴	۱
۰۰۱۰۰	۱۰۰۰۰	۲	۱	۱۰۱۰۰	۰۱۱۰۰	۲	۰
۰۰۱۰۱	۱۱۰۰۱	۲	۱	۱۰۱۰۱	۱۱۱۱۱	۲	۱
۰۰۱۱۰	۱۱۱۰۱	۴	۰	۱۰۱۱۰	۰۱۰۱۱	۴	۱
۰۰۱۱۱	۰۱۰۰۱	۳	۰	۱۰۱۱۱	۰۱۱۰۱	۳	۱
۰۱۰۰۰	۱۰۰۰۱	۲	۰	۱۱۰۰۰	۰۰۰۱۰	۳	۱
۰۱۰۰۱	۱۱۰۱۰	۳	۱	۱۱۰۰۱	۱۰۰۱۱	۳	۱
۰۱۰۱۰	۱۰۱۱۰	۳	۱	۱۱۰۱۰	۰۰۰۰۰	۳	۰
۰۱۰۱۱	۱۱۱۱۰	۳	۰	۱۱۰۱۱	۱۰۱۰۱	۳	۱
۰۱۱۰۰	۰۱۰۱۰	۲	۰	۱۱۱۰۰	۱۱۱۰۰	۰	۱
۰۱۱۰۱	۰۰۰۰۱	۲	۱	۱۱۱۰۱	۱۱۰۰۰	۲	۰
۰۱۱۱۰	۱۰۰۱۰	۳	۰	۱۱۱۱۰	۰۱۱۱۱	۲	۰
۰۱۱۱۱	۱۰۱۰۰	۳	۰	۱۱۱۱۱	۰۰۱۰۰	۴	۱

تحلیل جعبه جابه‌جایی پیشنهادی نشان می‌دهد که این جعبه جابه‌جایی تمام مقادیر یکتای ۰ تا ۳۱ را در خروجی تولید می‌کند. این امر یک به یک بودن را تایید می‌کند، زیرا هر ورودی ۵ بیتی دقیقاً به یک خروجی ۵ بیتی نگاشت می‌شود و هیچ مقداری در فضای خروجی از قلم نمی‌افتد. علاوه بر این، مجموع وزن‌های همینگ برای تمام خروجی‌های $S(x)$ برابر با ۱۶ است (رجوع شود به جدول ۳).

۴-۳- خاصیت غیرخطی

غیرخطی بودن یکی از مهمترین ویژگی‌های جعبه‌های جایگزینی در الگوریتم‌های رمزنگاری مانند Ascon است، زیرا تضمین می‌کند که الگوریتم در برابر حملات خطی، که به‌دنبال کشف همبستگی بین ورودی‌ها و خروجی‌ها از طریق حل معادلات خطی هستند، مقاوم باشد [۲۶].

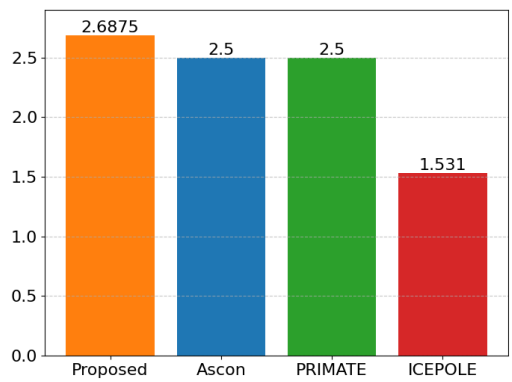
در این پژوهش، برای سنجش میزان غیرخطی بودن جعبه جابه‌جایی پیشنهادی، از فاصله همینگ[5] بین ورودی‌ها و خروجی‌های متناظر استفاده شده است. فاصله همینگ بین دو بردار دودویی x_i و $S(x_i) = y_i$، به‌صورت تعداد بیت‌هایی تعریف می‌شود که مقادیر متناظر آنها با

5-Hamming Distance

یکدیگر متفاوت است. فاصله همینگ بین یک جفت ورودی (x_i, y_i) کـه در آن $S(x_i) = y_i$ به‌صـورت زیر تعریف می‌شود:

$$H_d(x_i, y_i) = \#\{ j \mid x_{i,j} \neq y_{i,j} \} \quad (۳)$$

در اینجا، $x_{i,j}$ و $y_{i,j}$ به ترتیـب j–امین بیت از ورودی x_i و خروجی y_i هسـتند، و H_d تعداد بیت‌هایی را نشـان می‌دهد که در این جفت ورودی– خروجی متفاوت هستند. برای یک جعبه جابه‌جـایی ۵ بیتی، فاصله همینگ می‌تواند بین ۰ (در صورت یکسـان بـودن ورودی و خروجی) تا ۵ (در صورت تفاوت تمام بیت‌ها) باشـد. شـکل ۳ تحلیل جعبه جابه‌جایی پیشنهادی نشان می‌دهد که حداقل فاصله همینـگ برابر با ۰ و حداکثر آن برابر با ٤ اسـت. میانگین فاصلـه همینگ برای تمـام جفت‌هـای ورودی– خروجی محاسبه شده برابر با ۲/٦۸۷۵ است. هر چه فاصله همینگ بالاتر باشـد، غیرخطی بودن S-box بیشتر است، زیرا این امر نشـان‌دهنده عدم وجود الگوهای قابـل پیش‌بینی بین ورودی‌ها و خروجی‌هاست.



شکل ۳: مقایسهٔ خاصیت غیر خطی

۴-۴- احتمال تقریب خطی

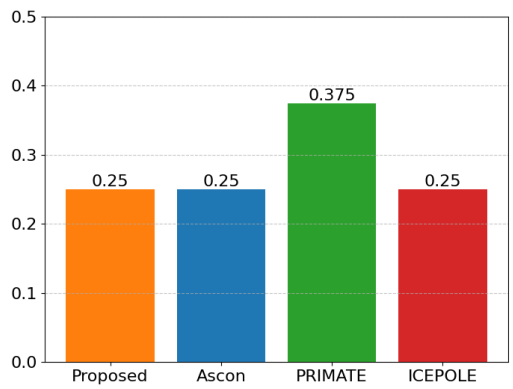
احتمـال تقریـب خـطی (Linear Approximation Probability) که توسـط ماتسوی در سـال ۱۹۹۳ معرفی شد [۲۷] یکی از معیارهـای کلیدی بـرای ارزیابی مقاومـت جعبه‌های جایگزینی در برابر حملات خطی اسـت. این معیار حداکثر میزان عـدم تعادل در رابطه بین ورودی‌ها و خروجی‌های جعبه جابه‌جایی را اندازه‌گیری می‌کند، که می‌تواند توسط مهاجمان برای کشـف همبستگی‌های خطی و بازیابی کلید رمزنـگاری مورد بهره‌برداری قرار گیـرد. احتمال تقریب خطی برای یک جعبـه جابه‌جایی به‌صـورت زیر تعریف می‌شود:

$$LP = max \left| \frac{\#\{ x \in X \mid x.\Delta x = S(x).\Delta y \}}{۲^n} - \frac{۱}{۲} \right| \quad (٤)$$

تحلیل جعبه جابه‌جایی پیشـنهادی نشـان می‌دهد که بالاترین تعداد تطابق برای شرط $x.\Delta x = S(x).\Delta y$ برابر با ۸ اسـت. با جایگذاری این مقدار در فرمول فوق، حداکثر احتمـال تقریب خطی بـرای جعبه جابه‌جایی پیشـنهادی به‌صورت زیر محاسبه می‌شود:

$$LP = \left| \frac{۸}{۲^۵} - \frac{۱}{۲} \right| = ۰.۲۵ \quad (۵)$$

مقدار LP برابر با ۰/۲۵ نشـان‌دهنده سطح قابل‌قبولی از امنیت است، زیرا مقادیر نزدیک به صفر بیانگر مقاومت بالاتر در برابر حملات خطی هستند. در حالت ایده‌آل، برای یک جعبه جابه‌جایی کاملاً تصادفی $lp = ۰$ خواهد بود، اما بـرای جعبه‌های جابه‌جایی ۵ بیتی، مقادیر LP در بازه ۰/۲ تا ۰/٤ مطلوب تلقی می‌شوند. شکل ٤ مقایسهٔ تقریب خطی را نشان می‌دهد.



شکل ۴: مقایسهٔ تقریب خطی

۴-۵- تحلیل رمزنگاری تفاضلی

تحلیل رمزنگاری تفاضلی(Differential Cryptanalysis)، که در سال ۱۹۹۰ توسط بیهام و شامیر معرفی شد [۲۸]، یکی از روش‌های آماری قدرتمند برای حمله به الگوریتم‌های رمزنگاری مبتنی بر شبکه جایگزینی- جایگشتی مانند Ascon است. این روش از جدول توزیع تفاضلی (Differential Distribution Table) جعبه‌های جایگزینی برای شناسایی الگوهای قابل استخراج در تغییرات خروجی نسبت به تغییرات ورودی استفاده می‌کند. برای مقاومت در برابر تحلیل تفاضلی، جعبه جابه‌جایی باید تغییرات خروجی غیرقابل پیش‌بینی و یکنواختی را ارائه دهد تا مهاجمان نتوانند از تفاوت‌های ورودی و خروجی برای بازیابی کلید رمزنگاری بهره‌برداری کنند. این مقاومت با معیار احتمال تقریب تفاضلی (Differential Approximation Probability)، که به‌عنوان یکنواختی تفاضلی (differential uniformity) شناخته می‌شود، سنجیده می‌شود. شکل ۵ مقایسهٔ احتمال تقریب در تحلیل تفاضلی را نمایش می‌دهد.

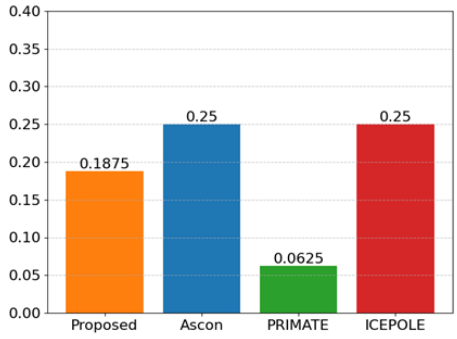
احتمال تقریب تفاضلی برای یک جعبه جابه‌جایی به‌صورت زیر تعریف می‌شود:

$$DAP = max\left(\frac{\#\{x \in X \mid S(x) \oplus S(x \oplus \Delta y) = \Delta y\}}{2^n}\right) \quad (6)$$

تحلیل جعبه جابه‌جایی پیشنهادی نشان می‌دهد که حداکثر تعداد تطابق برای شرط $S(x) \oplus S(x \oplus \Delta y) = \Delta y$ برابر با ۶ است. با جایگذاری این مقدار در فرمول DAP، حداکثر احتمال تقریب تفاضلی به‌صورت زیر محاسبه می‌شود:

$$DAP = \frac{6}{2^5} = 0.1875$$

مقدار DAP برابر با ۰/۱۸۷۵ نشان‌دهنده مقاومت مطلوب جعبه جابه‌جایی در برابر تحلیل تفاضلی است. برای یک جعبه جابه‌جایی ایده‌آل، مقدار DAP باید برابر با $\frac{1}{2^n} = \frac{1}{32} \approx 0.03125$ باشد، که در عمل غیرممکن است، زیرا این مقدار نشان‌دهنده عدم وجود هرگونه اطلاعات



شکل ۵: احتمال تقریب در تحلیل تفاضلی

تفاضلی در رابطه ورودی- خروجی است. با این حال، مقادیر DAP پایین (نزدیک به صفر) نشان‌دهنده یکنواختی تفاضلی بهتر و مقاومت بالاتر در برابر حملات تفاضلی هستند.

۴-۶- اثر بهمنی

اثر بهمنی (Avalanche Effect) یکی از ویژگی‌های اساسی در طراحی الگوریتم‌های رمزنگاری مانند Ascon است که تضمین می‌کند تغییر کوچک در بیت‌های ورودی منجر به تغییرات قابل توجه در بیت‌های خروجی شود. این خاصیت که برای افزایش مقاومت در برابر حملات رمزنگاری مانند تحلیل تفاضلی حیاتی است، با معیار دقیق بهمنی (Strict Avalanche Criterion) سنجیده می‌شود. SAC که توسط وبستر و تاوارس معرفی شد [۲۹]، بیان می‌کند که تغییر یک بیت در ورودی باید به‌طور متوسط حداقل نیمی از بیت‌های خروجی را تغییر دهد.

برای ارزیابی SAC، یک ورودی ۵ بیتی X در نظر گرفته می‌شود و مجموعه‌ای از بردارهای ورودی $X_1, X_2, \ldots, X_5$ با تغییر تنها بیت j–ام تولید می‌شود. بردارهای خروجی متناظر $S(X_j) = Y_j$ با استفاده از تابع جایگزینی S-box محاسبه می‌شوند. بردار بهمنی V_j از طریق عملیات XOR بین خروجی اصلی و خروجی تغییر یافته به‌صورت $Y_j \oplus Y = V_j$ محاسبه می‌شود. سپس، یک ماتریس وابستگی ۵ × ۵ به نام A تشکیل می‌شود، که در آن عنصر $a_{i,j}$ برابر با مجموع بیت i–ام بردارهای بهمنی V_j است.

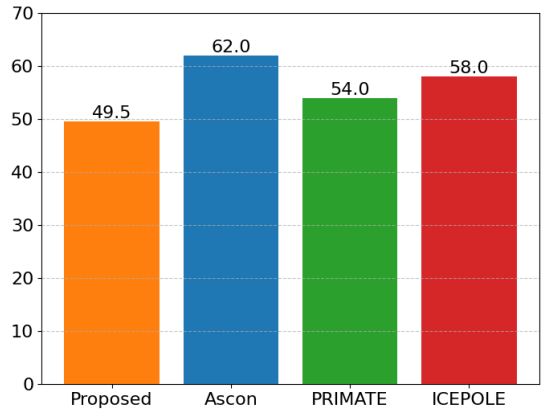
این فرایند برای تعداد زیادی ورودی X تکرار شـــده و هر عنصر ماتریس A بر ۲^n تقسیم می‌شـــود تا ماتریس SAC محاسبه شود.

برای ارزیابی SAC، یک ورودی ۵ بیتی X در نظر گرفته می‌شود و مجموعه‌ای از بردارهای ورودی $X_۱, X_۲, \dots, X_۵$ بـــا تغییر تنها بیتj–ام تولید می‌شـــود. بردارهای خروجی متناظـــر $S(X_j) = Y_j$ با اســـتفاده از تابـــع جایگزینی S-box محاســـبه می‌شـــوند. بردار بهمنی V_j از طریق عملیات XOR بیـــن خروجی اصلی و خروجی تغییریافته به‌صورت $Y_j \oplus Y = V_j$ محاســـبه می‌شـــود. ســـپس، یک ماتریس وابستگی ۵ × ۵ به نام A تشکیل می‌شود، که در آن عنصر $a_{i,j}$ برابر با مجموع بیت i–ام بردارهای بهمنی V_j است. این فرایند برای تعداد زیادی ورودی X تکرار شده و هر عنصر ماتریس A بر ۲^n تقسیم می‌شود تا ماتریس SAC محاسبه شود. شـــکل ٦ مقایســـهٔ مقدار SAC را برای رویکردهای مختلف نشان می‌دهد.

تحلیل جعبه جابه‌جایی پیشـــنهادی نشـــان می‌دهد که میانگیـــن اثر بهمـــنی برابر بـــا ٤٩/٥٠ درصد اســـت. این مقـــدار بسیار نزدیک به مقـــدار ایده‌آل ۵۰ درصد اســـت، که نشان‌دهنده برآورده شـــدن معیار دقیق بهمنی توسط جعبه جابه‌جایی پیشـــنهادی است. مقایسه اثر بهمنی جعبه جابه‌جایی پیشـــنهادی با دیگر جعبه‌های جابه‌جایی ۵ بیتی نشان می‌دهد که میانگین مقدار SAC پیشنهادی نزدیکترین مقدار به ایده‌آل است و از رقبا پیشی می‌گیرد.

برای تأیید کامل بودن (Completeness) و اثر بهمنی، دو تعریف زیر ارائه می‌شوند که ویژگی‌های جعبه جابه‌جایی پیشنهادی را از منظر رمزنگاری بررسی می‌کنند: برای یک تابع چندخروجی $S: F_۲^m \rightarrow F_۲^n$ کـــه m- بیت خروجی را در پاسخ به n- بیت ورودی تولید می‌کند، کامل بودن زمانی برقرار اســـت که هر بیت خروجی به تمام بیت‌های ورودی وابسته باشد.

$$C = ۱ - \frac{۱}{nm} \#\{(i,j) | b_{i,j} = ۰\} \quad (۷)$$



شکل ۶: مقایسه مقدار SAC

کـــه در آن $b_{i,j}$ تعداد دفعاتی را نشـــان می‌دهد که بیت j–ام خروجی در پاســـخ به تغییر بیـــت i–ام ورودی تغییر می‌کنـــد. مقدار C نزدیک به ۱ نشـــان‌دهنده غیرخطی بودن قوی اســـت. جعبه جابه‌جایی پیشنهادی با تولید جفت‌های ورودی– خروجی یکتا با اســـتفاده از ۵ بیت، مقدار C=1 را به‌دست می‌آورد، که نشـــان‌دهنده کامل بودن و وابستگی قوی هر بیت خروجی به تمام بیت‌های ورودی است.

بـــرای یک تابع F، اگر تغییر یـــک بیت ورودی به تغییر نیمی از بیت‌های خروجی منجر شـــود، معیار دقیق بهمنی برقرار است. این خاصیت به‌صورت زیر تعریف می‌شود:

$$Avl = ۱ - \frac{۲}{\#T.nm} \sum_{i=۱}^{n} \sum_{j=۱}^{m} | b_{i,j} - \frac{۱}{۲} \#T | \quad (۸)$$

در اینجا #T تعداد ورودی‌ها است و $b_{i,j}$ تعداد تغییرات بیت خروجی را نشـــان می‌دهـــد. مقـــدار Avl نزدیک به ۱ نشـــان‌دهنده اثر بهمنی قوی اســـت. این مقدار برای جعبه جابه‌جایی پیشـــنهادی برابر با ۰/۸۵ است، که تأیید می‌کند معیار دقیق بهمنی را به‌خوبی برآورده کرده است.

۴-۷- استقلال بیت‌های خروجی

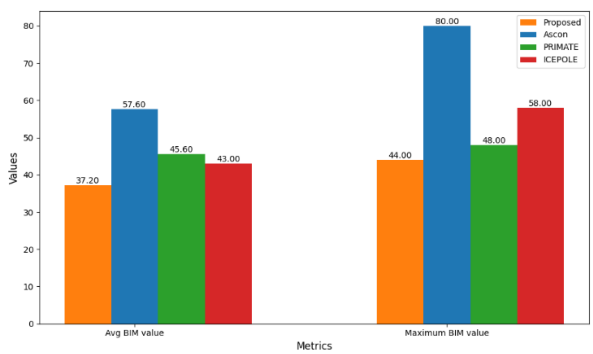
معیـــار اســـتقلال بیـــت (Bit Independence Criterion)، که توســـط وبســـتر و تاوارس معرفی شـــد [۲۹]، یکی از ویژگی‌های کلیدی در طراحی جعبه‌های جابه‌جایی اســـت

که تضمین می‌کند تغییر در یک بیت ورودی به‌صورت مستقل بر تمام بیت‌های خروجی تأثیر بگذارد. به‌عبارت دیگر، تغییر در بیت i–ام ورودی باید تغییرات مستقلی در بیت‌های خروجی j و k ایجاد کند. این خاصیت برای افزایش غیرخطی بودن و کاهش همبستگی‌های قابل‌استخراج بین بیت‌های خروجی حیاتی است. شکل ۷ مقایسهٔ استقلال بیت‌های خروجی را در رویکردهای مختلف نشان می‌دهد.

تحلیل جعبه جابه‌جایی پیشنهادی، نشان می‌دهد که مقدار متوسط BIC برابر با ۳۷/۲۰ و در بیشترین حالت ٤٤ است. هر چقدر این مقادیر کوچکتر و به هم نزدیکتر باشند بهتر است.

۴-۸- پیچیدگی محاسباتی در کاربرد اینترنت اشیاء

از آنجا که الگوریتم پیشنهادی برای به‌کارگیری در حوزهٔ اینترنت اشیاء طراحی شده است، لازم است معیارهای ارزیابی با محدودیت‌های رایج این حوزه هماهنگ باشند. دستگاه‌های اینترنت اشیاء به‌طور معمول دارای توان پردازشی محدود، حافظهٔ اندک و نیاز به مصرف انرژی پایین هستند. در این راستا، عملکرد الگوریتم پیشنهادی در این بخش از نظر پیچیدگی محاسباتی سنجیده و با سایر رویکردها مقایسه می‌شود.



شکل ۷: مقایسهٔ استقلال بیت‌های خروجی

برای پیاده‌سازی جعبه جابه‌جایی پیشنهادی به ۱٦۰ بیت فضا برای ذخیره سازی جدول نیاز است که با محدودیت‌های حافظه دستگاه‌های اینترنت اشیاء سازگار است. برای مقایسهٔ دقیق پیچیدگی محاسباتی تعداد عملیات‌های (operations) انجام شده در الگوریتم‌ها با یکدیگر مقایسه می‌شوند. برای این منظور یک فایل نمونه با اندازهٔ ۱۷۵ کیلوبایت، به‌عنوان دادهٔ ورودی انتخاب شده و فرایند رمزنگاری بر روی آن اعمال می‌شود. در این آزمایش، زمان اجرای الگوریتم از لحظه دریافت داده خام تا تولید خروجی رمز شده اندازه‌گیری شده و پیچیدگی الگوریتم به‌صورت کمی ارزیابی شده است.

نتایج حاصل نشان می‌دهد از نظر زمان اجرا برای رمزنگاری تصویر در مقیاس داده‌های متداول اینترنت اشیاء مناسب بوده و سربار محاسباتی آن در مقایسه با الگوریتم‌های Ascon و PRIMATE در یک سطح قابل رقابت قرار دارد. این مقایسه هم از منظر تعداد عملیات پایه و هم از منظر زمان واقعی اجرا روی داده تصویری انجام شده است. جدول شماره ٤ نتایج این مقایسه را نشان می‌دهد.

جدول ۴: مقایسه تعداد عملیات مورد نیاز برای رمزنگاری یک فایل ۱۷۵ کیلوبایتی پایه توسط رویکردهای مختلف

Ascon	رویکرد پیشنهادی	PRIMATE
۵,۸۱۵,۶۸۰	۶,۴۴۱,۴۰۸	۹,۳۲۵,۲۱۴

همان‌طور که در جدول شماره ٤ قابل مشاهده است، رویکرد پیشنهادی در مقایسه با Ascon افزایش اندکی در حجم محاسبات مورد نیاز ایجاد کرده است، اما کماکان اختلاف معنا داری با رویکرد PRIMATE دارد. در این آزمایش جهت سادگی کلیهٔ محاسبات ریاضی (مانند جمع، تفریق، AND، OR و XOR) یک واحد در نظر گرفته شده‌اند.

۵- جمع‌بندی نتایج ارزیابی

در این فصل، امنیت و کارایی الگوریتم پیشنهادی به‌صورت جامع ارزیابی شده است. تمرکز اصلی بر سنجش مقاومت جعبه جابه‌جایی طراحی شده در برابر حملات رایج رمزنگاری مانند حملات خطی، تفاضلی، و

تحلیل آماری بوده است. جعبه ۵ بیتی پیشنهادی خاصیت یک‌به‌یک، غیرخطی بودن مناسب، و وزن همینگ متعادل (۲/۶۸۷۵) را نشان می‌دهد که بیانگر گنگی و پراکندگی خوب در خروجی است.

معیارهایی مانند احتمال تقریب خطی (۰/۲۵)، تقریب تفاضلی (۰/۱۸۷۵) و اثر بهمنی (۴۹/۵ درصد) در بازه‌های قابل قبول قرار دارند. همچنین، شاخص کامل بودن (۱/۰) و شاخص شدت اثر بهمنی (۰/۸۵) نشان می‌دهند که تغییرات ورودی به‌خوبی در کل خروجی پخش می‌شوند. میانگین استقلال بیت خروجی (BIC) برابر با ۳۷/۲۰ نیز حاکی از پراکندگی مستقل و غیرهمبسته بیت‌هاست.

مقایسه با الگوریتم‌های سبک‌وزن مرجع مانند، Ascon PRIMATE و ICEPOLE نشان می‌دهد که ساختار پیشنهادی با وجود استفاده از جعبه جابه‌جایی پویا و توابع آشوب، عملکرد امنیتی بهتری در برخی شاخص‌ها دارد. همچنین، با نیاز به تنها ۱۶۰ بیت حافظه برای جدول جعبه، الگوریتم از نظر مصرف منابع نیز برای محیط‌های محدود مناسب است. همچنین رویکرد پیشنهادی پیچیدگی محاسباتی قابل قبولی داشته و در مقایسه با رویکرد Ascon تنها حدود ۱۰ درصد محاسبات بیشتری نیاز دارد که با توجه به توان محاسباتی موجود در شبکه‌های مبتنی بر اینترنت اشیا قابل پذیرش است.

در مجموع، تحلیل‌های عددی و آماری انجام شده در محیط پایتون، نشان می‌دهند که الگوریتم پیشنهادی از نظر امنیت و کارایی، قابلیت رقابت با الگوریتم‌های استاندارد را داشته و گزینه‌ای مؤثر برای کاربردهای اینترنت اشیاء محسوب می‌شود.

۶- نتیجه‌گیری

جعبه‌های جابه‌جایی به‌عنوان تنها مؤلفه‌ای که قابلیت غیرخطی را در الگوریتم‌های رمزنگاری مبتنی بر شبکه جایگزینی- جایگشتی مانند Ascon فراهم می‌کنند، نقش حیاتی در تعیین هزینه، عملکرد، و ویژگی‌های امنیتی این الگوریتم‌ها ایفا می‌کنند.

در این پژوهش، به چالش‌های رمزنگاری سبک‌وزن در محیط‌های با منابع محدود مانند اینترنت اشیاء پرداخته شد. با توجه به نیاز روزافزون به امنیت در این فضاها، یک الگوریتم جدید با استفاده از توابع آشوبی برای تولید جعبه‌های جابه‌جایی دینامیک طراحی شد. این الگوریتم ضمن حفظ ساختار کلی Ascon، ویژگی‌هایی مانند مقاومت در برابر حملات کلاسیک، تحقق اثر بهمنی قوی، و سازگاری با معماری‌های محدود را ارائه می‌دهد.

از مهمترین مزایای الگوریتم پیشنهادی می‌توان به تولید جعبه جابه‌جایی وابسته به کلید، پراکندگی بالا در خروجی، و مصرف پایین منابع اشاره کرد. با این حال، چالش‌هایی مانند پیچیدگی تولید اولیه جعبه، وابستگی به پارامترهای آشوبی، نبود سخت‌افزارهای بهینه و نیاز به آزمون‌های گسترده‌تر در محیط‌های واقعی نیز مطرح هستند که برای تجاری‌سازی و پذیرش گسترده باید برطرف شوند.

در پایان، مسیرهایی برای تحقیقات آتی پیشنهاد شده است؛ از جمله توسعه جعبه‌های جابه‌جایی پیشرفته با توابع آشوبی چندبُعدی، تولید پویا در زمان اجرا، پیاده‌سازی سخت‌افزاری بر روی FPGA، ترکیب با الگوریتم‌های نوظهور مانند رمزنگاری DNA، و تحلیل مقاومت در برابر حملات پیشرفته مانند حملات جانبی و یادگیری ماشین. این مسیرها می‌توانند زمینه‌ساز نسل جدیدی از الگوریتم‌های امن و بهینه برای کاربردهای حساس و کم‌منبع باشند.

۷- مراجع

[1] Al-Shargabi, B. & Sabri, O. (2017).”Internet of Things: An exploration study of opportunities and challenges,” in 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia.

[2] Beg, T. A.-K. a. A. A.-N. A. (2019). “Performance Evaluation and Review of Lightweight Cryptography in an Internet-of-Things Environment,” in 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019.

[3] Wolf, D. S. a. M. (2019). “Challenges and Opportunities in VLSI IoT Devices and Systems,” IEEE Design & Test, vol. 36, no. 4, pp. 24-30.

[4] Mohd, B. J., & Hayajneh, T. (2018). “Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques,” IEEE Access, vol. 6, pp. 35966-35978.
[5] Mohd, B. J., Hayajneh, T., & Vasilakos, A. V. (2015). “A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues,” Journal of Network and Computer Applications, vol. 58, pp. 73-93.
[6] Vishal, T. A., Razzaque, M. A. & Khandaker, M. R. (2021). “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities,” IEEE Access, vol. 9, pp. 28177-28193.
[7] Dobraunig, C., Eichlseder, M., Mendel, F. & Schläffer, M. (2021). “Ascon v1.2: Lightweight Authenticated Encryption and Hashing,” Journal of Cryptology, vol. 34, 2021.
[8] Shannon, C. E. (1949).”Communication theory of secrecy systems,” The Bell System Technical Journal, vol. 28, pp. 656-715.
[9] Matthews, R. (1989). “On the derivation of a chaotic encryption algorithm,” Cryptologia, vol. 13, pp. 29-42.
[10] Fadhil Al-Husainy, M. A., Al-Shargabi, B., & Aljawarneh, S. (2021). “Lightweight cryptography system for IoT devices using DNA,” Computers and Electrical Engineering, vol. 95, p. 107418.
[11] P. P, M. M, S. K & M. Sayeed, S. (2021). “An Enhanced Energy Efficient Lightweight Cryptography Method for various,” ICT Express, vol. 7, no. 4, pp. 487-492.
[12] Medileh, S., & Laouid, A. (2020) .”A flexible encryption technique for the internet of things environment,” Ad Hoc Networks, vol. 106, p. 102240.
[13] Rarhi, K. & Saha, S. (2019). “Image Encryption in IoT Devices Using DNA and Hyperchaotic Neural Network,” Design Frameworks for Wireless Networks, vol. 82, pp. 347-375.
[14] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017).”Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions,” Ambient Intell Human Comput, vol. 15, p. 1625–1642.
[15] Montero-Canela, R., Zambrano-Serrano, E., Tamariz-Flores, E., Muñoz-Pacheco, J. M. & Torrealba-Meléndez, R. (2020).”Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks,” Ad Hoc Networks, vol. 97, p. 102005.
[16] Knudsen, L., Leander, G., Poschmann, A. & Robshaw, M. J. (2010).”PRINTcipher: A Block Cipher for IC-Printing,” in Cryptographic Hardware and Embedded Systems, Berlin.
[17] Bogdanov, A. (2007). “PRESENT: An Ultra-Lightweight Block Cipher,” in Cryptographic Hardware and Embedded Systems, Berlin.
[18] Zhang, W., Bao, Z., Rijmen, V. & Liu, M. (2015). “A New Classification of 4-bit Optimal S-boxes and Its Application to PRESENT, RECTANGLE and SPONGENT,” in Fast Software Encryption, Berlin.
[19] Blondeau, C. & Nyberg, K. (2014). “Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities,” in Advances in Cryptology, Oswald.
[20] Goyal, T. K., Sahula, V. & Kumawat, D. (2022). “Energy Efficient Lightweight Cryptography Algorithms for IoT Devices,” IETE Journal of Research, vol. 68, no. 3, pp. 1722-1735.
[21] Qumsieh, R., Farajallah, M. & Hamamreh, R. (2019). “Joint block and stream cipher based on a modified skew tent map,” Multimedia Tools and Applications, vol. 78, p. 33527–33547.
[22] Thakor, V. A., Razzaque, M. A., Darji, A. D., & Patel, A. R. (2023). “A novel 5-bit S-box design for lightweight cryptography algorithms,” Journal of Information Security and Applications, vol. 73, p. 103444.
[23] Li, Y., Wang, M., Liu, W., & Wang, W. (2019).”Cryptanalysis of PRIMATEs,” Science China Information Sciences, vol. 63, p. 112106.
[24] Jia, Y. M., Li, C. J., Zhang, Y. & Chen, J. (2020). “The high-order completeness analysis of the scaled boundary finite element method,” Computer Methods in Applied Mechanics and Engineering, vol. 362, p. 112867, 2020.
[25] Wei, V. K., & Yang, K. (1993).”On the generalized Hamming weights of product codes,” IEEE Transactions on Information Theory, vol. 39, pp. 1709-1713.
[26] Cusick, T., & Stanica, W. (2017). Pantelimon, Cryptographic Boolean functions and applications, Academic Press.
[27] Matsui, M. (1993). “Linear Cryptanalysis Method for DES Cipher,” in EUROCRYPT 1993, Berlin, 1993.
[28] Biham, E. & Shamir, A. (1991). “Differential cryptanalysis of DES-like cryptosystems,” Journal of Cryptology, vol. 4, pp. 3-72, 1991.
[29] Williams, H., Webster, A. & Tavares, S. (1986).”On the design of s-boxes,” Advances in Cryptology, vol. 218, pp. 523-534.