نشریه علمی «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»

سال اول، شماره ۲، تابستان ۱۴۰۰؛ ص ۸۲- ۷۳

علمی – تخصصی

بررسی فینالیست‌های مسابقه رمزنگاری سبک‌وزن NIST

احسان دلاوری[۱]، علی مددی[۲*]

۱ و ۲- کارشناس ارشد رمز و امنیت، سازمان تحقیقات و جهاد خودکفایی صدر

(دریافت: ۱۴۰۰/۰۱/۰۴، پذیرش: ۱۴۰۰/۰۴/۰۲)

چکیده

موسسه NIST در سال ۲۰۱۹ به‌منظور انتخاب یک استاندارد جدید در اولیه‌های رمزنگاری سبک‌وزن شامل طرح‌های رمزگذاری احراز اصالت‌شده و توابع چکیده‌ساز، مسابقه‌ای را تحت عنوان رمزنگاری سبک‌وزن (LWC) آغاز نمود. در ۲۹ مارس سال ۲۰۲۱، از بین ۳۲ نامزد دور دوم مسابقه، ۱۰ نامزد به‌عنوان فینالیست معرفی شد. یکی از معیارهای مهم برای انتخاب فینالیست مسابقه، وجود یک ساختار امن و کارا با ویژگی‌های طراحی متناسب با محیط‌هایی با منابع محدود است. در این مقاله به بررسی ۱۰ نامزد فینالیست مسابقه LWC از منظر روش به‌کارگیری، اولیه‌ها و ویژگی‌های طراحی پرداخته می‌شود. همچنین تعداد فراخوانی‌های اولیه به‌کاررفته در مرحله مقداردهی اولیه و نهایی طرح‌ها که تعیین‌کننده هزینه فرایند پیش‌پردازش بوده و به‌عنوان یک معیار مهم در کارایی ساختار محسوب می‌شود، مورد بررسی قرار گرفته است. بر اساس بررسی‌های انجام‌شده، طرح‌های مبتنی بر Sponge-duplex و طرح‌های Elephant، Romulus و -128AEAD Grain از منظر کارایی دارای عملکرد مناسبی هستند.

کلیدواژه‌ها: طرح رمزگذاری احراز اصالت‌شده، مسابقه رمزنگاری سبک‌وزن، NIST، رمزنگاری متقارن

۱- مقدمه

با پیشرفت فناوری اطلاعات و ارتباطات، استفاده از اینترنت اشیاء[۱] (IoT) و شبکه‌های حس‌گر بی‌سیم در حوزه‌های گوناگون صنایع الکترونیکی و مخابراتی به امری ضروری و اجتناب‌ناپذیر تبدیل شده است. با توجه به محدودیت‌های سخت‌افزاری و منابع محدود انرژی در این نوع شبکه‌ها و نوع ارتباطات آن‌ها، ارائه سرویس‌های امنیتی متناسب با محدودیت‌های این شبکه‌ها یکی از چالش‌های اساسی حوزه امنیت داده‌ها محسوب می‌شود. یکی از راه‌های تأمین ویژگی‌های امنیتی شامل محرمانگی[۲] و احراز اصالت[۳] در محیط‌هایی با منابع محدود، استفاده از الگوریتم‌های رمزنگاری متقارن سبک‌وزن[۴] است. معیارهای سبک‌وزن بودن الگوریتم‌های رمزنگاری با توجه به ویژگی‌های امنیتی، کارایی و هزینه پیاده‌سازی مشخص می‌شود که در شکل (۱) به آن‌ها اشاره شده است [۱].

طرح‌های رمزگذاری احراز اصالت‌شده با داده همراه (AEAD)[۵] به‌عنوان یکی از اولیه‌های رمزنگاری متقارن که ویژگی‌های محرمانگی و احراز اصالت را به‌طور هم‌زمان محقق می‌کنند، می‌تواند به‌عنوان یک راه‌حل مناسب برای ارتقاء سطح امنیتی داده‌های مخابره‌شده در حوزه IoT و شبکه‌های حس‌گر بی‌سیم محسوب شود [۲].

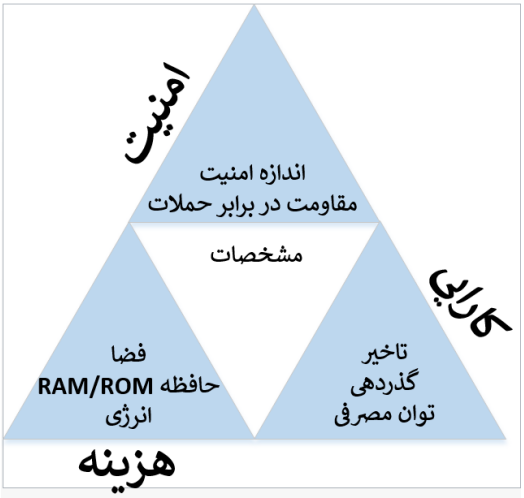
طرح‌های AEAD زیادی وجود دارد که ویژگی‌های امنیتی فوق را محقق می‌کنند، اما اکثر این طرح‌ها برای محیط‌هایی مانند desktop و یا server طراحی شده‌اند لذا خیلی از آن‌ها برای محیط‌هایی با منابع محدود مانند دستگاه‌های مورداستفاده در حوزه IoT مناسب نیستند. بنابراین، طراحی الگوریتم‌های رمزنگاری سبک‌وزن امری ضروری است [۳].

در خصوص طراحی الگوریتم‌های رمزنگاری سبک‌وزن، تلاش گسترده‌ای توسط جامعه رمزنگاری در حال انجام است که بر این اساس مؤسسه ملی استانداردها و فناوری آمریکا (NIST)[۶]

* رایانامه نویسنده مسئول: almadadi93@gmail.com

[1] Internet of Things (IoT)
[2] Confidentiality
[3] Entity Authentication
[4] Lightweight Symmetric Cryptography Algorithms
[5] Authenticated Encryption with Associated Data
[6] National Institute of Standards and Technology

مسابقه‌ای را از سال ۲۰۱۹ تحت عنوان رمزنگاری سبک‌وزن (LWC)[1] برای طراحی و ارزیابی طرح‌های سبک‌وزن AEAD و توابع چکیده‌ساز در دو بستر سخت‌افزاری و نرم‌افزاری آغاز نموده است [۴].



شکل (۱): معیارهای طراحی الگوریتم‌های رمزنگاری سبک‌وزن [۱]

NIST در سال ۲۰۱۳، به‌منظور تبیین نیاز به یک الگوریتم استاندارد رمزنگاری سبک‌وزن اختصاصی، پروژه رمزنگاری سبک‌وزن را آغاز نمود تا یک فرآیند شفاف جهت طراحی استاندارد رمزنگاری سبک‌وزن طی شود. در سال ۲۰۱۶، این مؤسسه مبحثی را در جامعه رمزنگاری اطلاع‌رسانی کرد که به‌واسطه آن، دانش مربوط به الگوریتم‌های رمزنگاری سبک‌وزن ارتقاء یابد. طبق فرض مؤسسه NIST، شرایط پیاده‌سازی و به‌کارگیری این الگوریتم‌ها به‌گونه‌ای است که استفاده از الگوریتم‌های استاندارد مرسوم، نشدنی بوده و شرایط خاصی حاکم بر محیط پیاده‌سازی است. در مارس ۲۰۱۷، NIST خلاصه‌ای از کارهای صورت‌گرفته در طول اجرای پروژه LWC جهت یافتن یک الگوریتم رمزنگاری سبک‌وزن و توضیحات مربوط به ارائه برنامه برای استانداردسازی این الگوریتم را در قالب گزارش NISTIR 8114 منتشر کرد [۵].

ازآنجاکه مسابقه LWC به‌عنوان آخرین مسابقه معتبر در حوزه رمزنگاری متقارن بوده که توسط مؤسسه معتبر NIST انجام شده و طرح‌های پذیرفته‌شده در این مسابقه توسط افراد شناخته‌شده‌ی جامعه رمزنگاری ارائه شده است؛ هم‌چنین با توجه به این‌که تاکنون نامزدهای فینالیست این مسابقه از منظر کارایی نسبت به هم مورد ارزیابی قرار نگرفته‌اند، لذا بررسی این نامزدها امری ضروری است.

یکی از معیارهای مهم برای ارزیابی نامزدهای LWC، بررسی ساختارهای مورداستفاده در طرح‌های شرکت‌کننده مسابقه LWC است. ویژگی‌های طراحی و مؤلفه‌های هر ساختار در انتخاب یک طرح امن و کارا برای راه‌یابی به دورهای بعدی و درنهایت به‌عنوان طرح AEAD سبک‌وزن منتخب تأثیرگذار است. در این مقاله یک مرور کلی بر روی طرح‌های فینالیست مسابقه LWC ارائه شده و مقایسه‌ای از منظر روش به‌کارگیری، اولیه‌ها، ویژگی‌های طراحی و امنیتی و هم‌چنین تعداد فراخوانی اولیه‌های این نامزدها صورت می‌گیرد.

در [۶] به بررسی ویژگی‌های طراحی شامل وارون نداشتن[2]، قابل موازی‌سازی[3]، چابکی کلید[4]، پارامتر ظرفیت[5]، تعداد گیت‌های به‌کاررفته در هر طرح و هم‌چنین تعداد فراخوانی‌های اولیه‌ی به‌کاررفته در هر ساختار بیان شده است. درصورتی‌که در این مقاله علاوه بر ویژگی‌های فوق، به بررسی دو ویژگی برخط بودن[6] بودن[6] و تک‌مسیره بودن[7] پرداخته شده است. در ادامه، انواع روش‌های به‌کارگیری طرح‌های فینالیست و اولیه مورداستفاده در آن‌ها دسته‌بندی و با یکدیگر مقایسه شده است. همچنین تعداد فراخوانی‌های اولیه به‌کاررفته در مرحله مقداردهی اولیه و نهایی ساختار را که تعیین‌کننده هزینه فرایند پیش‌پردازش بوده و به‌عنوان یک معیار مهم در کارایی ساختار است، مورد بررسی قرار گرفته است.

ساختار مقاله: در ادامه مقاله، در بخش ۲ مسابقه LWC معرفی و در بخش ۳، ویژگی‌های طراحی طرح‌های AEAD بیان می‌شود. در بخش ۴ و ۵، به‌ترتیب مقایسه ۱۰ نامزد فینالیست از منظر ویژگی‌های طراحی و روش‌های به‌کارگیری مورد ارزیابی قرار می‌گیرند. درنهایت در بخش ۶، جمع‌بندی و نتیجه‌گیری بیان خواهد شد.

نمادهای به‌کاررفته در این مقاله در جدول (۱)، نشان داده شده است.

[1] Lightweight Cryptography

[2] Inverse-free
[3] Parallelizable
[4] Key Agility
[5] Capacity
[6] Online
[7] One-Pass / Single-Pass

جدول (۱): نمادها

نماد	توضیح
LWC	رمزنگاری سبک‌وزن
AEAD	رمزگذاری احراز اصالت‌شده با داده همراه
BC[1]	رمز قالبی
SC[2]	رمز جریانی
TBC[3]	رمز قالبی تنظیم‌پذیر
SPN[4]	شبکه جانشینی- جایگشت
-/*	دارا بودن/ نبودن

۲- مسابقه LWC

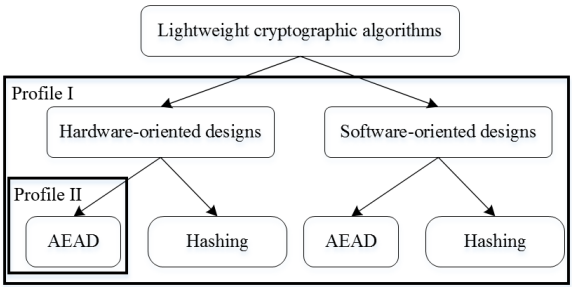
با توجه به اهمیت و ضرورت طراحی اولیه‌های رمزنگاری سبک‌وزن، مؤسسه NIST نیازمندی‌ها و شرایط لازم برای طراحی طرح‌های AEAD و توابع چکیده‌ساز را در ۲۷ آگوست ۲۰۱۸ منتشر کرد. NIST طبق زمان‌بندی که برای ارسال الگوریتم‌ها تا ۲۹ فوریه ۲۰۱۹ تعیین کرده بود، ۵۷ طرح خواهان شرکت در مسابقه بودند. این مؤسسه در ۱۸ آوریل ۲۰۱۹ تعداد ۵۶ نامزد را برای دور اول و در ۹ سپتامبر ۲۰۱۹، تعداد ۳۲ نامزد را به‌عنوان طرح‌های راه‌یافته به دور دوم معرفی کرد [۴]. در ۲۹ مارس ۲۰۲۱ نیز ۱۰ نامزد به‌عنوان فینالیست مسابقه معرفی شدند [۷].

در اکتبر ۲۰۱۹ گزارش وضعیت دور اول مرحله استانداردسازی الگوریتم‌های سبک‌وزن ارائه شد [۴]. در شکل (۲)، نامزدهای دور اول مسابقه نشان داده شده است که از میان آن‌ها، ۱۰ طرح به‌عنوان فینالیست مسابقه با کادر قرمزرنگ قابل‌مشاهده است.

مسابقه LWC به‌منظور جهت‌دهی به روند طراحی الگوریتم‌های رمزنگاری سبک‌وزن، دو نمایه[5] را مدنظر قرار داد که نمایه اول (Profile I) مربوط به طراحی الگوریتم‌های AEAD و چکیده‌ساز در بسترهای نرم‌افزاری و سخت‌افزاری بوده و نمایه دوم (Profile II) فقط مربوط به طراحی الگوریتم‌های AEAD در بسترهای سخت‌افزاری است. شکل (۳) تقسیم‌بندی نمایه‌های موردنظر در مسابقه LWC را نشان می‌دهد. در پیوست (۱) جدول مربوط به مشخصات کلی نمایه اول و دوم مسابقه به‌طور کامل بیان شده است.

Submissions with AEAD and Hashing Functionality	*Submissions with only AEAD Functionality*
Permutation based	*Permutation based*
ACE	CiliPadi
ASCON	Elephant
CLX	Fountain
DryGASCON	ISAP
GAGE and InGAGE	Oribatida
Gimli	SPIX
HERN and HERON	SpoC
KNOT	WAGE
ORANGE	
PHOTON-Beetle	*Block cipher based*
Shamash and Shamashash	COMET
SIV-TEM-PHOTON	FlexAEAD
SNEIK	GIFT-COFB
SPARKLE (SCHWAEMM and ESCH)	HyENA
Subterranean 2.0	LAEM
Sycon	Limdolen
Xoodyak	mixFeed
Yarará and Coral	Pyjamask
	SAEAES
Block cipher based	Simple
Saturnin	SUNDAE-GIFT
SIV-Rijndael	TinyJAMBU
	TRIFLE
Tweakable block cipher based	
SKINNY-AEAD and SKINNY-HASH	*Tweakable block cipher based*
	ForkAE
Stream cipher based	ESTATE
Triad	Lilliput-AE
	LOTUS-AEAD, and LOCUS-AEAD
	Qameleon
	Remus
	Romulus
	Spook
	Thank Goodness It's Friday (TGIF)
	Stream cipher based and others
	Bleep64
	CLAE
	Grain-128AEAD
	Quartet

شکل (۲): نامزدهای دور اول مسابقه LWC [۴]



شکل (۳): نمایه‌های طراحی الگوریتم‌های مسابقه LWC [۵]

در ادامه، به بررسی مختصر و مرور ویژگی‌های مربوط به فینالیست‌های مسابقه LWC پرداخته می‌شود.

۳- ویژگی‌های طراحی

با شروع مسابقه و ارائه طرح‌های AEAD، چندین ویژگی مربوط به روش‌های به‌کارگیری طرح‌ها مطرح شدند که در ادامه به بررسی این ویژگی‌ها پرداخته می‌شود.

[1] Block Cipher (BC)
[2] Stream Cipher (SC)
[3] Tweakable Block Cipher (TBC)
[4] Substitution-Permutation Network (SPN)
[5] Profile

۳-۱- قابلیت موازی‌سازی

قابلیت موازی‌سازی بدین معنی است که یک طرح AE بتواند قالب‌های پیام و یا متن رمزی را به‌صورت موازی پردازش کند. به‌عبارت‌دیگر، در فرآیند رمزنگاری اگر برای هر $i \neq j$، پردازش i-امین قالب ورودی به خروجی پردازش j-امین قالب وابسته نباشد، پردازش موازی صورت خواهد گرفت. این نکته قابل‌توجه است که توانایی موازی‌سازی عملیات رمزگذاری و رمزگشایی جدا از هم هستند و برای طرح‌ها باید به‌صورت جداگانه این ویژگی بررسی شود [۸, ۹].

۳-۲- برخط بودن

یک طرح AE که پیام‌های با طول دلخواه را به‌عنوان ورودی می‌گیرد، دارای ویژگی برخط است اگر بتواند قالب‌های رمزی را به‌محض دریافت قالب‌های متن اصلی تولید کند (رمزگذاری برخط). هم‌چنین پردازش قالب متن رمزی i-ام تنها باید به کلید و i-1 قالب متن اصلی اول بستگی داشته باشد (رمزگشایی برخط). به‌عبارت‌دیگر، برای انجام عملیات رمزگذاری، الگوریتم AE منتظر دریافت تمام پیام‌های ورودی نمی‌ماند بلکه به‌محض دریافت ورودی بتواند قالب‌های متن رمزی را تولید نماید.

پردازش برخط پیام، این امکان را فراهم می‌کند که بدون در اختیار داشتن طول کل پیام، می‌توان محاسبات مربوط به هر دو عمل رمزگذاری و رمزگشایی را انجام داد. در محیط‌هایی که محدودیت حافظه وجود دارد این ویژگی بسیار مفید است [۸ و ۱۰].

۳-۳- تک‌مسیره و دومسیره

طرح‌های AE از یک منظر به دو دسته‌ی طرح‌های AE ترکیبی[1] یا دومسیره[2] و طرح‌های AE یکپارچه[3] یا تک‌مسیره[4] تقسیم می‌شوند. در طرح AE دو مسیره، فرآیند محرمانگی و احراز اصالت به‌صورت جداگانه انجام می‌شوند. به‌عنوان‌مثال، در یک طرح AE ممکن است عملیات رمزگذاری با روش به‌کارگیری CTR انجام شده و بعد از آن فرآیند احراز اصالت با CBC-MAC صورت گیرد. اما در طرح تک‌مسیره فرآیند محرمانگی و احراز اصالت به‌طور یکپارچه و پیوسته انجام می‌شود [۱۱].

نکته: طرحی که برخط نباشد، برون‌خط[5] یا دومسیره است [۸].

رابطه بین برخط بودن و تک‌مسیره بودن نیز بدین‌صورت است:

- اگر طرحی برخط نباشد، دومسیره است.
- اگر طرحی برخط باشد، ممکن است تک‌مسیره یا دومسیره باشد.

۳-۴- وارون نداشتن

ویژگی وارون‌نداشتن بدین معنی است که فقط یکی از دو تابع رمزگذاری یا رمزگشایی در طرح AE به کار می‌رود لذا به میزان قابل‌توجهی در مصرف حافظه و منابع (انرژی، پردازنده و غیره) صرفه‌جویی می‌شود. یک طرح AE وارون‌ناپذیر است، اگر این طرح نیازی به عملیات وارون اولیه خود را نداشته باشد. باوجوداین ویژگی نیازی به داشتن مدار رمزگشایی نیست و برای رمزگشایی از همان فرآیند رمزگذاری استفاده می‌شود. طرح‌هایی که از مد CTR استفاده می‌کنند این‌گونه هستند [۸, ۱۰].

۳-۵- چابکی کلید

ویژگی چابکی کلید بدین معنی است که در روش به‌کارگیری طرح AE، از توسیع کلید استفاده نشده و انتقال کلید سریع انجام می‌شود. در این‌صورت زمان اجرای الگوریتم برای تغییر کلید کاهش می‌یابد [۱۰].

در ادامه، فینالیست‌های مسابقه LWC از منظر روش به‌کارگیری، اولیه‌ها و ویژگی‌های طراحی آن‌ها مورد بررسی قرار می‌گیرد.

۴- مقایسه ویژگی‌های طراحی فینالیست‌ها

در جدول (۲) مشخصات و ویژگی‌های طراحی ۱۰ نامزد فینالیست مسابقه LWC نشان داده شده است.

در جدول (۲)، مشخصات ۱۰ نامزد فینالیست شامل روش به‌کارگیری، نوع و ساختار اولیه به‌کاررفته در طرح و هم‌چنین ویژگی‌های طراحی هر طرح بیان شده است. مشاهده می‌شود که همه طرح‌های AEAD و Hash، بر اساس اولیه مبتنی بر جایگشت طراحی شده‌اند. هم‌چنین با توجه به این‌که طرح‌های نرم‌افزاری و سخت‌افزاری AEAD و Hash بر اساس روش به‌کارگیری Sponge Duplex طراحی شده‌اند لذا دارای

[1] Composed
[2] Two-Pass
[3] Integrated
[4] One-Pass / Single-Pass
[5] Offline

ویژگی‌های برخط بودن، وارون نداشتن، تک‌مسیره بودن و چالاکی کلید هستند.

طرح‌های سخت‌افزاری AEAD نیز از تنوع بیش‌تری در نوع اولیه برخوردار بوده و دارای دو ویژگی مشترک برخط بودن و وارون نداشتن هستند.

از بین ۱۰ نامزد فینالیست تنها طرح Elephant دارای قابلیت موازی‌سازی است. هم‌چنین در اکثر این طرح‌ها، ساختار اولیه SPN بیش‌ترین فراوانی را داراست.

ازآنجاکه طرح‌های مبتنی بر ساختار Sponge-duplex دارای ویژگی چابکی کلید هستند، از منظر کارایی ساختارهای مناسبی برای طرح‌های AEAD سبک‌وزن هستند زیرا در این ساختارها توسیع کلید استفاده نشده و زمان اجرای الگوریتم برای تغییر کلید کاهش می‌یابد. هم‌چنین این ساختارها دارای بیش‌ترین ویژگی‌های طراحی هستند. هم‌چنین این نکته حائز اهمیت است که همه طرح‌های فینالیست AEAD و Hash بر اساس اولیه مبتنی بر جایگشت هستند.

با توجه به جدول (۲)، به‌منظور طراحی یک طرح AEAD سبک‌وزن، می‌بایست روش به‌کارگیری و اولیه بکار رفته در آن را متناسب با ویژگی‌های طراحی و شرایط موردنیاز آن طرح انتخاب نمود.

در پیوست (۲) پارامترهای مربوط به نامزدهای فینالیست به تفکیک نسخه‌های هر طرح بیان شده است.

جدول (۲): مشخصات کلی و ویژگی‌های طراحی فینالیست‌های مسابقه LWC

نوع اولیه طرح	نام طرح	روش به‌کارگیری AEAD / Hash	ساختار اولیه	ویژگی‌ها				
				برخط	وارون نداشتن	تک‌مسیره	قابل موازی‌سازی	چالاکی کلید
طرح‌های AEAD و Hash								
مبتنی بر جایگشت	ASCON [10]	Sponge-duplex (Monkey Duplex) / Sponge	ASCON (SPN)	*	*	*	-	*
	PHOTON-Beetle [12]	Sponge-duplex (Beetle)	PHOTON Permutation (SPN)	*	*	*	-	*
	SPARKLE [13]	AE:SCHWAEMM (Sponge-duplex (Beetle)) / Hash: ESCH (Sponge-duplex)	SPARKLE Permutation (SPN(LTS) , ARX)	*	*	*	-	*
	Xoodyak [14]	Sponge-duplex (Cyclist)	Xoodoo Permutation (KECCAK Permutation-like)	*	*	*	-	*
طرح‌های AEAD								
مبتنی بر جایگشت	Elephant [15]	(OCB-like) Nonce-based Encryption-then-MAC (CTR for Encryption-variant of Wegman-Carter-Shoup MAC for Authentication)	Spongent-π , KECCAK-f Mask: LFSR (Even-Mansour)	*	*	-	*	-
	ISAP [16]	Encryption-then-MAC (Sponge-based Re-keying Function)	KECCAK-Permutation ASCON-Permutation	*	*	-	-	-
	GIFT-COFB [17]	COFB (COmbined FeedBack)	GIFT-BC (SPN)	*	*	*	-	-

	TinyJAMBU [18]	TinyJAMBU (Improved Duplex) (Variant of JAMBU)	NLFSR	❋	❋	❋	–	❋
مبتنی بر TBC	Romulus [19]	Romulus-N (COFB) Romulus-M (SIV)	SKINNY (SPN)	❋	❋	–	–	–
مبتنی بر SC	Grain - 128AEAD [20]	Pre-output (Nonlinear Filter) Generator / Authenticator Generator	LFSR, NLFSR, Pre-output Function / Shift Register , Accumulator	❋	❋	–	–	–

۵- مقایسه روش‌های به‌کارگیری

یکی از معیارهای مهم در طراحی طرح‌های AEAD با سرعت بالا و عملکرد مناسب از منظر پیاده‌سازی، ایجاد کارایی بالا در فرآیند پیش‌پردازش است. بدین منظور ارزیابی تعداد فراخوانی‌های اولیه به‌کاررفته در مرحله مقداردهی اولیه و مرحله نهایی حائز اهمیت بوده و هرچه تعداد فراخوانی‌های اولیه در دو مرحله مقداردهی اولیه و نهایی کم‌تر باشد، فرآیند پیش‌پردازش با هزینه کم‌تری قابل انجام خواهد بود. در جدول (۳)، فینالیست‌های مسابقه LWC بر اساس روش‌های به‌کارگیری دسته‌بندی شده و از منظر فرآیند پیش‌پردازش با یکدیگر مقایسه شده‌اند.

با توجه به این‌که در گزارش همه طرح‌های فینالیست، لزوماً اثبات امنیتی ساختار بیان نشده، لذا در ستون آخر این جدول مراجع مربوط به امنیت قابل‌اثبات هر طرح بیان شده است.

جدول (۳): دسته‌بندی روش‌های به‌کارگیری و مقایسه تعداد فراخوانی اولیه در فینالیست‌های مسابقه LWC

نوع ساختار (روش به‌کارگیری)		نام طرح	تعداد فراخوانی اولیه در مرحله مقداردهی اولیه	تعداد فراخوانی اولیه در مرحله نهایی	امنیت قابل‌اثبات
Monkey Duplex	Duplex Sponge Family	ASCON	۱	۱	[۲۱]
Beetle		PHOTON-Beetle	۱	۱	[۲۲]
		SPARKLE (SCHWAEMM and ESCH)	۱	۱	[۲۲]
Cyclist		Xoodyak	۲	۱	[۲۳ ,۱۴]
Sponge-based Re-keying Function		ISAP	هسته رمز: توسیع کلید هسته MAC: ۱	هسته رمز: ۰ هسته MAC: ۱ + توسیع کلید	[۲۴]
OCB		Elephant	۱	۰	[۱۵]
COFB		Romulus	هسته رمز: ۰ هسته MAC: ۰	هسته رمز: ۰ هسته MAC: ۱	[۱۹]
		GIFT-COFB	۱	۱	[۱۷]
TinyJAMBU		TinyJAMBU	۱	۲	[۱۸]
Pre-output (Nonlinear Filter) Generator		Grain-128AEAD	۱	۰	[۲۵]

طبق جدول (۳) مشاهده می‌شود که علاوه بر بیان جزئی‌تر روش به‌کارگیری، تعداد فراخوانی اولیه در مراحل ابتدایی و نهایی ذکر شده است. بدیهی است که هر چه تعداد فراخوانی اولیه در این مراحل کم‌تر باشد، هزینه پیش‌پردازش کم‌تر بوده و کارایی طرح بیش‌تر خواهد شد.

با توجه به جدول (۳)، طرح‌های Cyclist و TinyJAMBU دارای بیش‌ترین تعداد فراخوانی اولیه در مراحل ابتدایی و نهایی و هم‌چنین طرح‌های Elephant، Romulus و Grain-128AEAD

دارای کم‌ترین تعداد فراخوانی اولیه در مراحل ابتدایی و نهایی هستند.

از بین ساختارهای ذکرشده در جدول (۳)، دو ساختار Monkey Duplex و OCB از اهمیت بالایی برخوردار هستند زیرا این ساختارها در فینال هر دو مسابقه CAESAR و LWC حضور داشته و تاکنون تحلیل‌های مستقل[1] زیادی بر روی آن‌ها صورت گرفته است.

لازم به ذکر است که برخلاف مسابقه CAESAR که برای برخی از فینالیست‌ها امنیت قابل‌اثبات ارائه نشده بود، در این مسابقه تمامی فینالیست‌ها دارای امنیت قابل‌اثبات هستند.

۶- نتیجه‌گیری

در این مقاله به معرفی ۱۰ نامزد فینالیست مسابقه LWC پرداخته شده و پس از بیان ویژگی‌های طراحی موردنیاز در طراحی AEAD، فینالیست‌های مسابقه از منظر روش به‌کارگیری، اولیه‌ها و ویژگی‌های طراحی مورد ارزیابی قرار گرفتند. در ادامه تعداد فراخوانی‌های اولیه به‌کاررفته در مرحله مقداردهی اولیه و نهایی طرح‌ها که تعیین‌کننده هزینه فرایند پیش‌پردازش بوده و به‌عنوان یک معیار مهم در کارایی ساختار محسوب می‌شود، مورد بررسی قرار گرفت.

با توجه به جداول (۲) و (۳)، مشخص شد که طرح‌های مبتنی بر Sponge-duplex دارای ویژگی چابکی کلید بوده و از منظر کارایی ساختارهای مناسبی برای طرح‌های AEAD سبک‌وزن هستند. هم‌چنین طرح‌های Cyclist و TinyJAMBU دارای بیش‌ترین تعداد فراخوانی اولیه در مراحل ابتدایی و نهایی هستند. از بین ۱۰ نامزد فینالیست طرح‌های Elephant، Romulus و -128AEAD Grain دارای کم‌ترین تعداد فراخوانی اولیه در مراحل ابتدایی و نهایی هستند که نتیجه آن ایجاد کارایی مناسب نسبت به سایر طرح‌هاست.

۷- مراجع

[1] https://csrc.nist.gov/CSRC/media/Presentations/on-the-nist-lwc-standardization/images-media/Talk-Elliptic-Curve-Crypto-Meltem_Dec 2019. pdf.

[2] B. Rezvani and W. Diehl, "Hardware Implementations of NIST Lightweight Cryptographic Candidates: A First Look".

[3] M. M. Niknam, S. Sadeghi, M. R. Aref, and N. Bagheri, "Investigation of Some Attacks on GAGE (v1), InGAGE (v1),(v1. 03), and CiliPadi (v1) Variants," ISeCure, Vol. 12, no. 1, 2020.

[4] M. S. Turan, K. A. McKay, Ç. Çalık, D. Chang, and L. Bassham " Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process," 2019 .

[5] L. Bassham, Ç. Çalık, K. McKay, N. Mouha, and M. Sönmez Turan, "Profiles for the Lightweight Cryptography Standardization Process (Retired Draft) ",National Institute of Standards and Technology, 2017 .

[6] E. Bovy, J. Daemen, and B. Mennink, "Comparison of the second round candidates of the NIST lightweight cryptography competition," 2020.

[7] https://csrc.nist.gov/News/2021/lightweight-crypto-finalists-announced .

[8] F. Abed, C. Forler, and S. Lucks, "General overview of the first-round caesar candidates for authenticated encryption," IACR ePrint, Vol. 792, p. 2014, 2014.

[9] F. Abed, C. Forler, and S. Lucks, "General classification of the authenticated encryption schemes for the CAESAR competition," Computer Science Review, Vol. 22, pp. 13-26, 2016.

[10] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schafer, "Ascon v1.2," Submission to NIST Lightweight Cryptography competition, 2019.

[11] T. Krovetz and P. Rogaway, "The software performance of authenticated-encryption modes," in International Workshop on Fast Software Encryption, 2011: Springer, pp. 306-327 .

[12] Z. Bao et al., "Photon-Beetle: Authenticated encryption and hash family," Submission to NIST Lightweight Cryptography Standardization Project (announced as round 2 candidate on August 30, 2019), 2019.

[13] C. Beierle et al., "Schwaemm and Esch: lightweight authenticated encryption and hashing using the Sparkle permutation family," 2019.

[14] J. Daemen, S. Hoffert, M. Peeters, G. V. Assche, and R. V. Keer, "Xoodyak, a lightweight cryptographic scheme," Submission to NIST Lightweight Cryptography competition, 2019.

[15] C. Dobraunig and B. Mennink, "Elephant v1," 2019.

[16] C. Dobraunig et al., "ISAP v2. 0," Submission to NIST Lightweight Cryptography, 2019.

[1] Third-party Analysis

[17] S. Banik et al., "GIFT-COFB," Submission to Round, Vol. 1, 2019.

[18] H. Wu and T. Huang, "TinyJAMBU: A Family of Lightweight Authenticated Encryption Algorithms," Submission to the NIST Lightweight Cryptography Competition, available online at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/TinyJAMBU-spec. pdf, 2019.

[19] T. Iwata, M. Khairallah, K. Minematsu, and T. Peyrin, "Romulus v1," Submission to NIST Lightweight Cryptography Project, 2019.

[20] M. Hell, T. Johansson, W. Meier, J. Sonnerup, and H. Yoshida, "Grain-128AEAD," Submission to NIST Lightweight Cryptography competition, 2019.

[21] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Duplexing the sponge: single-pass authenticated encryption and other applications," in International Workshop on Selected Areas in Cryptography, 2011: Springer, pp. 320-337 .

[22] B. Chakraborty, A. Jha, and M. Nandi, "Security Proof of Beetle and SpoC," 2019.

[23] J. Daemen, B. Mennink, and G. Van Assche, "Full-state keyed duplex with built-in multi-user support," in International Conference on the Theory and Application of Cryptology and Information Security, 2017: Springer, pp. 606-637.

[24] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "On the security of the keyed sponge construction," in Symmetric Key Encryption Workshop, 2011, Vol. 2011 .

[25] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," Journal of computer and system sciences, Vol. 22, no. 3, pp. 265-279, 1981.

[26]

پیوست (۱)

جدول (۴): مشخصات کلی تعیین‌شده در نمایه اول و نمایه دوم مسابقه [۵]

نمایه / ویژگی‌ها	نمایه اول (طراحی AEAD و Hash برای محیط‌های نرم‌افزاری و سخت‌افزاری محدود)	نمایه دوم (طراحی AEAD برای محیط‌های سخت‌افزاری محدود)
تابع‌پذیری[1]	طراحی الگوریتم‌ها باید به‌گونه‌ای باشد که از یک هسته واحد برای الگوریتم چکیده‌ساز و طرح AE استفاده شود.	طراحی الگوریتم رمزگذاری احراز اصالت‌شده با داده همراه
اهداف طراحی[2]	الگوریتم‌ها باید به‌گونه‌ای طراحی شوند که در محیط‌هایی با منابع محدود (در بسترهای سخت‌افزاری و نرم‌افزاری تعبیه‌شده[3]) در مقایسه با الگوریتم‌های استاندارد فعلی NIST عملکرد بهتری داشته باشند.	طراحی الگوریتم باید به‌گونه‌ای باشد که در مقایسه با استانداردهای فعلی NIST عملکرد بهتری داشته باشد.
	الگوریتم AEAD و چکیده‌ساز باید به‌ازای پیام‌هایی با طول کوتاه دارای عملکرد بهینه باشند.	عملکرد طرح AEAD باید به‌ازای پیام‌هایی با طول کوتاه (۸ بایتی) مناسب باشد.
	طول پیام ورودی باید مضرب صحیحی از بایت باشد.	طول پیام ورودی باید مضرب صحیحی از بایت باشد.
مشخصات فیزیکی[4]	پیاده‌سازی‌های سخت‌افزاری متراکم[5] و نرم‌افزاری تعبیه‌شده با حافظه RAM و ROM پایین امکان‌پذیر باشد.	بسترهای سخت‌افزاری محدود، هدف مورد نظر طراحی است.
		طرح باید دارای قابلیت پیاده‌سازی‌های سخت‌افزاری متراکم باشد.

[1] Functionality
[2] Design Goals
[3] Embedded Software Platforms
[4] Physical Characteristics
[5] Compact Hardware Implementations

مشخصات عملکرد[1] (تاخیر[2]، گذردهی[3] یا توان مصرفی[4])		عملکرد طرح باید بر روی بستر ASIC و FPGA طیف وسیعی از کتابخانه‌های استاندارد را پوشش داده و شامل انواع راهبردهای پیاده‌سازی (انرژی کم، توان کم، تأخیر کم) بوده و از این منظر نسبت به استانداردهای فعلی NIST بهبودیافته باشد.	عملکرد طرح باید بر روی بستر ASIC و FPGA طیف وسیعی از کتابخانه‌های استاندارد را پوشش دهد.
		عملکرد طرح بر روی انواع مختلف ریزپردازنده‌ها[5] مانند ریزپردازنده‌های ۸ ۸ بیت، ۱۶ بیتی و ۳۲ بیتی باید مدنظر قرار گیرد.	طراحی الگوریتم باید انعطاف‌پذیر بوده و شامل انواع راهبردهای پیاده‌سازی (انرژی کم، توان کم، تأخیر کم) باشد.
		عملیات پیش‌پردازش کلید (در محاسبه پیچیدگی زمان و حافظه) باید کارا باشد.	عملیات پیش‌پردازش کلید (در محاسبه پیچیدگی زمان و حافظه) باید کارا باشد.
مشخصات امنیتی	AEAD	طول کلید باید تا اندازه ۱۲۸ بیت را پوشش دهد. طول کلید با اندازه‌های بزرگ‌تر نیز تا حد امکان پوشش یابد به‌عنوان مثال، امنیت در حالت کلید چندگانه[6] یا امنیت در برابر رایانه‌های کوانتومی[7] برقرار باشد.	
		طول نانس باید تا اندازه ۱۲۸ بیت را پوشش دهد.	
		طول برچسب[8] باید تا اندازه ۱۲۸ بیت را پوشش دهد.	
		طول متن اصلی باید تا اندازه $۱ - ۲^{۵۰}$ بایت را پوشش دهد.	
		طول داده همراه باید تا اندازه $۱ - ۲^{۵۰}$ بایت را پوشش دهد.	
		باید حداقل $۱ - ۲^{۵۰}$ بایت تحت یک کلید به‌طور امن پردازش شود.	
		پیچیدگی اجرای حمله بر روی رایانه کلاسیک (PC) تحت یک کلید باید حداقل $۲^{۱۱۲}$ باشد.	
		طرح باید دارای مقاومت در برابر انواع حملات کانال جانبی شامل حملات زمانی[9]، تحلیل توان ساده و تفاضلی (SPA/DPA)[10] و تحلیل الکترومغناطیس ساده و تفاضلی (SEMA/DEMA)[11] باشد.	
	چکیده‌ساز	پیچیدگی اجرای حمله بر روی رایانه کلاسیک (PC) تحت یک کلید باید حداقل $۲^{۱۱۲}$ باشد.	
		خروجی تابع چکیده‌ساز باید ۲۵۶ بیت بوده و خروجی‌های با اندازه بزرگ‌تر نیز باید تا حدامکان پوشش یابد.	
		بیش‌ترین طول پیام ورودی $۱ - ۲^{۵۰}$ بایت باشد.	
		طرح باید دارای مقاومت در برابر انواع حملات کانال جانبی شامل حملات زمانی، تحلیل توان ساده و تفاضلی (SPA/DPA) و تحلیل الکترومغناطیس ساده و تفاضلی (SEMA/DEMA) باشد.	

[1] Performance Characteristics
[2] Latency
[3] Throughput
[4] Power Consumption
[5] Microcontrollers
[6] Multi-key
[7] Quantum Computers
[8] Tag
[9] Timing Attack
[10] Simple and Differential Power Analysis
[11] Simple and Differential Electromagnetic Analysis

پیوست (۲)

جدول (۵): پارامترهای مربوط به فینالیست‌های مسابقه LWC

نام طرح	نسخه‌های طرح	پارامترها				
		اندازه قالب (حالت)	اندازه کلید	اندازه تنظیم	اندازه نانس	اندازه برچسب
ASCON	ASCON-128	۳۲۰	۱۲۸	-	۱۲۸	۱۲۸
	ASCON-128a	۳۲۰	۱۲۸	-	۱۲۸	۱۲۸
PHOTON-Beetle	PHOTON-Beetle-AEAD[r=128]	۲۵۶	۱۲۸	-	۱۲۸	۱۲۸
	PHOTON-Beetle-AEAD[r=32]	۲۵۶	۱۲۸	-	۱۲۸	۱۲۸
SPARKLE	SCHWAEMM-256-128	۳۸۴	۱۲۸	-	۲۵۶	۱۲۸
	SCHWAEMM -128-128	۲۵۶	۱۲۸	-	۱۲۸	۱۲۸
	SCHWAEMM -192-192	۳۸۴	۱۹۲	-	۱۹۲	۱۹۲
	SCHWAEMM -256-256	۵۱۲	۲۵۶	-	۲۵۶	۲۵۶
Xoodyak	Xoodyak	۳۸۴	۱۲۸	-	۱۲۸	۱۲۸
Elephant	Dumbo	۱۶۰	۱۲۸	-	۹۶	۶۴
	Jumbo	۱۷۶	۱۲۸	-	۹۶	۶۴
	Delirium	۲۰۰	۱۲۸	-	۹۶	۱۲۸
ISAP	ISAP-K-128A	۴۰۰	۱۲۸	-	۱۲۸	۱۲۸
	ISAP-A-128A	۳۲۰	۱۲۸	-	۱۲۸	۱۲۸
	ISAP-K-128	۴۰۰	۱۲۸	-	۱۲۸	۱۲۸
	ISAP-A-128	۳۲۰	۱۲۸	-	۱۲۸	۱۲۸
GIFT-COFB	GIFT-COFB	۱۲۸	۱۲۸	-	۱۲۸	۱۲۸
TinyJAMBU	TinyJAMBU-128	۱۲۸	۱۲۸	-	۹۶	۶۴
	TinyJAMBU-192	۱۲۸	۱۹۲	-	۹۶	۶۴
	TinyJAMBU-256	۱۲۸	۲۵۶	-	۹۶	۶۴
Romulus	Romulus-N1	۱۲۸	۱۲۸	۲۵۶	۱۲۸	۱۲۸
	Romulus-N2	۱۲۸	۱۲۸	۲۵۶	۱۲۸	۱۲۸
	Romulus-N3	۱۲۸	۱۲۸	۱۲۸	۱۲۸	۱۲۸
	Romulus-M1	۱۲۸	۱۲۸	۲۵۶	۱۲۸	۱۲۸
	Romulus-M2	۱۲۸	۱۲۸	۲۵۶	۱۲۸	۱۲۸
	Romulus-M3	۱۲۸	۱۲۸	۱۲۸	۱۲۸	۱۲۸
Grain -128AEAD	Grain-128AEAD	-	۱۲۸	-	۹۶	۶۴

Journal of "Innovations of Applied Information and Communication Technologies"

Vol. 1, No. 2, 2021 (Serial No. 2)

The Scrutiny of the NIST Lightweight Encryption Competition Finalists

E. Delavari, A. Madadi*

Sadr Self-Sufficiency Research and Jihad Organization

Abstract

In 2019, the NIST institute started a competition called lightweight cryptography (LWC), in order to select a new standard in the pioneers of lightweight cryptography including authenticated encryption schemes and abstract-creating functions. On March 29, 2021, out of 32 candidates in the second round of the competition, 10 candidates were nominated as finalists. One of the important criteria for selecting a competition finalist is the presence of a safe and efficient structure with design features suitable for environments with limited resources. This paper, examines the top 10 finalists for the LWC in terms of the operation mode, primitives and design features. Also, the number of primary calls used in the initial and final initialization phases of the designs, which determines the cost of the preprocessing and is an important criterion in the efficiency of the structure, is examined. Based on the studies performed, Sponge-duplex and Elephant, Romulus and Grain-128AEAD designs have good performance in terms of efficiency.

Keywords: AEAD, LWC, NIST, Symmetric Cryptography

Corresponding author E-mail: almadadi93@gmail.com