مروری بر حملات و پیاده‌سازی نرم‌افزاری الگوریتم‌های رمزنگاری توأم با احراز اصالت مسابقهٔ CAESAR

محسن رضایی[1] و رضا ابراهیمی آتانی[2*]

[1] دانشجوی کارشناسی ارشد گروه مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران
morezaei@webmail.guilan.ac.ir
[2] استادیار گروه مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران
rebrahimi@guilan.ac.ir

چکیده

رمزنگاری احراز اصالت‌شده یک حالت اجرایی در رمزهای قالبی بوده که خدمت‌های احراز اصالت، محرمانگی و تمامیت داده را در فرآیند انتقال اطلاعات فراهم می‌کند. از سال ۲۰۱۴ مسابقه‌ی تحت عنوان مسابقهٔ CAESAR آغاز شده است که هدف از این مسابقه رسیدن به طرح‌های رمزنگاری احراز اصالت شده است که مزایای بیشتری نسبت به طرح AES-GCM ارائه دهند و برای استفاده گسترده مناسب باشند. در این مقاله، تمامی نامزدهای معرفی‌شده به مسابقهٔ CAESAR بر اساس ذات طراحی و معماری (رمز قالبی، رمز جریانی، جایگشتی/اسفنجی، متراکم‌سازی، اختصاصی) دسته‌بندی شده و مروری کلی روی جنبه‌های عملکردی، پارامترهای امنیتی و نیرومندی نامزدها صورت گرفته است؛ سپس تمامی نامزدها از نظر سرعت رمزگذاری، رمزگشایی و تشخیص پیام‌های جعلی روی پردازنده‌هایی از سه معماری AMD64، armeabi و mipso32 مورد مقایسه قرار گرفته‌اند.

واژگان کلیدی: محرمانگی، رمزنگاری، احراز اصالت، پیاده‌سازی نرم‌افزاری، مسابقهٔ CAESAR.

۱- مقدّمه

امروزه اهمیت ایمن نگاه‌داشتن خطوط ارتباطی داده به امری اجتناب‌ناپذیر در زندگی روزمرهٔ افراد تبدیل شده است. از طرفی برای برقراری امنیت ارتباطات و اطلاعات، تأمین محرمانگی و احراز اصالت پیام، دو هدف اصلی است که باید پیاده‌سازی شود. محرمانگی ضمانت می‌کند که اطلاعات تنها برای افراد مجاز قابل درک باشد؛ و احراز اصالت، فرآیندی است که در آن از جامعیت یا دست‌نخوردگیِ اطلاعات در طول تبادل آنها، اطمینان حاصل شده و فرستندهٔ اطلاعات نیز احراز هویت شود. ابزار اصلی برای به‌دست آوردن محرمانگی، استفاده از الگوریتم‌های رمزنگاری است و برای احراز اصالت پیام، استفاده از کدهای احراز اصالت پیام است؛ بنابر دلایلی برای حفظ امنیت اطلاعات و ارتباطات نباید از رمزنگاری بدون احراز اصالت استفاده کرد. به عبارت دیگر محرمانگی و احراز اصالت باید همراه با هم برآورد شوند. طرح‌های رمزنگاری که بتوانند این کار را انجام دهند، طرح‌های رمزنگاری احراز اصالت‌شده نامیده می‌شوند.

طرح رمزنگاری احراز اصالت‌شده. اگر $K \in \{0,1\}^k$، $k,v,t > 0$ کلید محرمانه، $N \in \{0,1\}^v$ تکرارناپذیری تک‌شمار[1]، $M \in \{0,1\}^*$ پیام، $T \in \{0,1\}^t$ برچسب احراز اصالت و $C \in \{0,1\}^*$ متن رمز باشد، آنگاه یک طرح رمزنگاری احراز اصالت‌شده، سه تاییِ $\Pi = (\mathcal{K}, \varepsilon, \mathcal{D})$ است به شکلی که رویهٔ $\mathcal{K}$ تولیدکنندهٔ کلید تصادفی K، $\varepsilon_K(N, M)$ الگوریتم رمزنگاری قطعی و $\mathcal{D}_K(N, C, T)$ الگوریتم رمزگشایی است. خروجی ε همیشه دوتایی برچسب-متن رمز (C, T) و خروجی $\mathcal{D}$، یا متن آشکار M، و در صورت غیر معتبر بودن برچسب احراز اصالت پیام، نماد $\perp$ است[۱]:

[1] Nonce

* نویسندهٔ عهده‌دار مکاتبات

$$\varepsilon : \{0,1\}^{k} \times \{0,1\}^{v} \times \{0,1\}^{*} \rightarrow \{0,1\}^{*} \times \{0,1\}^{t} \quad (1)$$
$$\mathcal{D} : \{0,1\}^{k} \times \{0,1\}^{v} \times \{0,1\}^{*} \times \{0,1\}^{t} \rightarrow \{0,1\}^{*} \cup \{\perp\}.$$

در بسیاری از کاربردها، علاوه‌بر این‌که پیام M رمزگذاری و احراز اصالت می‌شود، لازم است داده‌ای مثل H نیز وجود داشته باشد؛ به‌طوری که این داده، باید احراز اصالت بشود؛ اما رمزگذاری نشود. به‌عنوان مثال در این مورد به بسته‌های شبکه می‌توان اشاره کرد که در آنها محتویات اصلی بسته رمزگذاری و احراز اصالت می‌شود؛ اما سرآیند آن نباید رمزگذاری و تنها باید احراز اصالت شود تا مسیریاب‌ها بتوانند به‌طور مناسبی بسته‌ها را خوانده و تبادل کنند. این نیاز باعث می‌شود تا برخی از طرح‌های AE از قابلیت اضافه‌کردن دادهٔ وابسته به ورودی خود برخوردار باشند. چنین طرح‌هایی، طرح‌های رمزگذاری احراز اصالت‌شده همراه با دادهٔ وابسته [1] نامیده می‌شوند[۲].

طرح رمزنگاری احراز اصالت‌شده همراه با دادهٔ وابسته. اگر $k,v,t>0$ ، $K \in \{0,1\}^{k}$ کلید مخفی، $N \in \{0,1\}^{v}$ تکرارناپذیری تک‌شمار، $H \in \{0,1\}^{*}$ سرآیند (داده‌ی وابسته)، $M \in \{0,1\}^{*}$ پیام، $T \in \{0,1\}^{t}$ برچسب احراز اصالت و $C \in \{0,1\}^{*}$ متن رمز باشد، آنگاه یک طرح رمزنگاری احراز اصالت‌شده به همراه دادهٔ وابسته، سه‌تاییِ $\Pi = (\mathcal{K}, \varepsilon, \mathcal{D})$ است؛ به شکلی که رویهٔ $\mathcal{K}$ تولیدکنندهٔ کلید تصادفی K ، $\varepsilon_K(N,H,M)$ الگوریتم رمزنگاری قطعی و $\mathcal{D}_K(N,H,C,T)$ الگوریتم رمزگشایی است. خروجی ε همیشه دوتایی برچسب-متن رمز (C, T) و خروجی $\mathcal{D}$ یا متن آشکار M است یا در صورت غیر معتبر بودن برچسب احراز اصالت پیام، نماد $\perp$ را برمی‌گرداند [۱]:

$$\varepsilon : \{0,1\}^{k} \times \{0,1\}^{v} \times \{0,1\}^{*} \times \{0,1\}^{*} \rightarrow \{0,1\}^{*} \times \{0,1\}^{t} \quad (2)$$
$$\mathcal{D} : \{0,1\}^{k} \times \{0,1\}^{v} \times \{0,1\}^{*} \times \{0,1\}^{*} \times \{0,1\}^{t} \rightarrow \{0,1\}^{*} \cup \{\perp\}.$$

روش سنتی که به روش ترکیبی عام [2] شهرت دارد، برای به‌دست آوردن یک طرح AE ترکیب مستقیم روش‌های تولیدکنندهٔ محرمانگی و احراز اصالت پیام است؛ به این معنی که ابتدا یک الگوریتم رمزنگاری برای رمزکردن پیام به‌کار می‌رود؛ سپس از یک کد احراز اصالت برای احراز اصالت آن استفاده می‌شود. به‌دلیل جدابودن الگوریتم‌ها در این روش، تحلیل طرح AE مورد نظر تا حدودی ساده است؛ اما مهم‌ترین مسأله در این روش، احتیاج به دو الگوریتم رمزنگاری و احراز صالت جدای از هم با کلیدهای متمایز و نیز انجام دو گذر [3] روی پیام است. در مقابل روش سنتی، دستهٔ دیگری از طرح‌های AE وجود دارند که برای تأمین همزمان محرمانگی و احراز اصالت پیام از یک الگوریتم و یک کلید استفاده کرده و یک‌سری محاسبات(یک گذر) روی پیام انجام می‌دهند. این نوع طرح‌ها را می‌توان با سه روش کلی استفاده از یک رمز قالبی [4]، استفاده از یک رمز دنباله‌ای و سپس طراحی الگوریتم‌های احراز اصالت‌شدهٔ اختصاصی [5] دسته‌بندی کرد که با جزییات بیشتر در بخش سوم مقاله ارایه خواهد شد[۱].

هدف اصلی این مقاله معرفی الگوریتم‌ها و طرح های احراز اصالت‌شدهٔ معرفی‌شده در مسابقهٔ CAESAR است. در بخش دو به توضیح روش‌های ترکیبی عام برای الگوریتم‌های AE و در بخش ۳ به بیان ویژگی‌های تمامی نامزدهای معرفی‌شده به مسابقهٔ CAESAR از قبیل ذات طراحی آنها می‌پردازیم و جنبه‌های عملکردی، پارامترهای امنیتی و نیرومندی نامزدها را معرفی می‌کنیم. در بخش ۴ تمامی طرح‌ها را بر اساس ویژگی‌های ذکرشده در بخش ۳ مورد بررسی قرار می‌دهیم؛ و در بخش ۵ تمامی طرح‌ها را از نظر سرعت رمزنگاری مقایسه خواهیم کرد.

۲- طرح‌های ترکیبی عام

روش کلاسیک برای به‌دست‌آوردن طرح‌های AE، استفاده از یک الگوریتم برای محرمانگی و یک الگوریتم دیگر برای احراز اصالت پیام و ترکیب خروجی این دو الگوریتم است. ضعف‌هایی برای این نوع طرح‌ها شناخته شده است [۹]. برای مثال طرح‌هایی که در آنها از یک تابع چکیده‌ساز بدون کلید مثل h و یک طرح رمزگذاری امن مثل Enc استفاده شده و محرمانگی و احراز اصالت پیام M به‌صورت Enc(M,h(M)) حاصل شود، قابل شکست هستند[۱۰]. یک اشتباه دیگر در طرح‌های ترکیبی عام، استفادهٔ مجدد از کلید است. به‌عبارت دیگر اگر از یک کلید یکسان برای الگوریتم رمزگذاری و الگوریتم احراز اصالت استفاده شود، طرح AE حاصل دارای سستی خواهد بود. باید گفت که برخی طرح‌های ترکیبی نیز وجود دارند که از یک کلید استفاده می‌کنند؛ اما به‌دلیل دقت در طراحی آنها، ضعف گفته شده را ندارند [۹]. با توجه این توضیحات می‌توان گفت که در یک

[1] Authenticated Encryption with Associated Data
[2] Generic Composition
[3] Two Passes
[4] Block Cipher
[5] Dedicated AE

طرح AE ترکیبی لازم است تا از یک کد احراز اصالت پیام با کلید K_1 همراه با یک الگوریتم رمزگذاری با کلید (مستقل و متمایز) K_2 استفاده شود؛ اما مساله‌ای که باقی می‌ماند این است که کدام‌یک از این الگوریتم‌ها ابتدا و کدام در گام بعدی روی پیام به‌کار گرفته شود. در [۱۱] سه روش ترکیبی ممکن در نظر گرفته شده و امنیت آنها بررسی شده است. در ادامه این سه روش ترکیبی معرفی می‌شوند.

احراز اصالت، سپس رمزگذاری [1]: در این روش، ابتدا یک الگوریتم MAC با کلید K_1 روی پیام M به‌کار گرفته شده و برچسب احراز اصالت σ تولید می‌شود؛ سپس جفت (M,σ) با استفاده از الگوریتم رمزنگاری، با کلید K_2 رمزگذاری می‌شوند.

رمزگذاری، سپس احراز اصالت [2]: در این روش، ابتدا پیام M با کلید K_2 رمزگذاری شده و متن رمزی C به‌دست می‌آید؛ سپس الگوریتم MAC با کلید K_1 روی C به‌کار گرفته می‌شود تا جفت (C,σ) به‌دست آید.

رمزگذاری و احرازاصالت [3]: در این روش، رمزگذاری M با کلید K_2 و احراز اصالت با کلید K_1 به‌صورت همزمان انجام می‌شود و جفت (C,σ) به‌دست می‌آید.

با توجه به توضیحاتی که شرح آن رفت، مهم‌ترین مشکلات در استفاده از طرح‌های ترکیبی عام به‌منظور تأمین همزمان محرمانگی و احراز اصالت را می‌توان کوتاه و موردی به صورت زیر بیان کرد:

- نیاز به دو الگوریتم جداگانه برای رمزگذاری و احراز اصالت پیام؛
- نیاز به دو کلید متمایز (برای هریک از الگوریتم‌ها)؛
- دوگذری‌بودن محاسبات.

با توجه با این مشکلات که در طرح‌های ترکیبی عام وجود دارد، باید برای حل آنها چاره‌ای اندیشید. با درنظرگرفتن اهمیت طرح‌های AE در سال‌های اخیر تلاش‌های زیادی در جهت معرفی طرح‌های جدید AE، به‌کارگیری و استانداردسازی آنها انجام شده است. از مهم‌ترینِ این فعالیت‌ها می‌توان به برگزاری نخستین کارگاه آموزشی در زمینهٔ رمزگذاری احراز اصالت‌شده، با عنوان DIAC اشاره کرد. در این کارگاه طرح‌ها و نظرهایی در حوزهٔ رمزهای متقارن(به‌ویژه رمزهای قالبی و توابع چکیده‌ساز)، ارائه شد. در این کارگاه زمزمه‌هایی در رابطه با برگزاری یک مسابقهٔ جهانی در زمینهٔ AE مطرح شد تا اینکه در پانزدهم ژانویه ۲۰۱۳ فراخوان این مسابقه، با عنوان مسابقهٔ CAESAR، صادر و تقویم زمانی آن مشخص شد [۱۲].

۳- مسابقهٔ CAESAR

CAESAR [4] یک میدان هم‌آوری برای ارائهٔ رمزهای مبتنی بر احراز اصالت است. CAESAR مسابقه‌ای است برای ارائهٔ شیوه‌های رمزنگاری مبتنی بر احراز اصالت که امن، کاربردی و نیرومند باشند. CAESAR یک مجموعه از رمزهای مبتنی بر هویت را مشخص می‌کند که ۱) مزایای بیشتری نسبت به طرح AES-GCM [۴] ارائه می‌دهد و ۲) برای استفادهٔ گسترده مناسب است. طراحان الگوریتم‌های رمزنگاری برای ارائهٔ پیشنهادهای خود به CAESAR دعوت شده و همه پیشنهادهای ایشان برای ارزیابی شدن، عمومی شده‌اند. با شروع مسابقه، ۵۷ طرح به‌عنوان نامزد برندهٔ مسابقه معرفی شد که طرح Artemia[۱۳] و سبک CBA[۱۴] توسط هموطنانمان به این مسابقه معرفی شد. Artemia توسط آقایان محمدرضا عارف، نصور باقری و جواد علیزاده طراحی و به مسابقه ارائه شد. CBA نیز توسط آقایان حسین حسینی و شهرام خزائی به مسابقه عرضه شد. این ۵۷ طرح در جدول (۱) آورده شده‌اند. نامزدهایی که نتوانستند به دور دوم راه بیابند در جدول (۳)، نامزدهایی که به دور دوم رفتند، اما نتوانستند به دور سوم راه بیابند در قسمت جدول (۲) و نامزدهای حاضر در دور سوم در جدول (۱) آورده شده‌اند. از میان این ۵۷ نامزد معرفی‌شده به مسابقه، کمیته‌ی برگذارکنندهٔ مسابقه در ۷ جولای ۲۰۱۵، تعداد ۲۹ طرح از ۵۷ طرح معرفی‌شده به مسابقه را به‌عنوان طرح‌های راه‌یافته به دور دوم معرفی کرد. در ۱۵ آگوست ۲۰۱۶ و پس از پایان دور دوم، کمیتهٔ برگذارکنندهٔ مسابقه ۱۶ طرح را به‌عنوان طرح‌های راه‌یافته به دور سوم معرفی کرد [۱].

در ادامه به بررسی جامع همهٔ طرح‌های مسابقهٔ CAESAR می‌پردازیم. البته از ۵۷ طرح معرفی‌شده برخی شکسته شده و پَس گرفته شده‌اند و بالطبع آنها مورد بررسی قرار نخواهند گرفت. نتایج بررسی به شکل جداولی که نشان‌دهندهٔ ویژگی‌های عملکردی منحصربه‌فرد هر طرح مانند قابلیت موازی‌سازی، برخط‌بودن، وارونه نداشتن [5]، پشتبانی از برچسب‌های میانی [6] و تغییرات پله‌ای داشتن و همچنین پارامترهای امنیتی (محرمانگی و جامعیت) و نیز

[1] Encryption then MAC (EtM)
[2] MAC then Encryption (MtE)
[3] Encryption And MAC (E&M)

[4] Competition for Authenticated Encryption: Security, Applicability, and Robustness
[5] Inverse-Free
[6] Intermediate Tag

نیرومنـــدی هـــر طـــرح (ســـوء اســـتفاده از رمزگشـــایی و تکرارناپذیری تک‌شمار) نشان داده شده است [۱].

(جدول-۱): نامزدهای حاضر در دور سوم مسابقه‌ی CAESAR.

نامزد	طراح	نامزد	طراح
ACORN	Hongjun Wu	ELmD	Elmar Tischhauser, Kan Yasuda; Nilanjan Datta, Mridul Nandi
AEGIS	Hongjun Wu, Bart Preneel	Ketje	Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, Ronny Van Keer
AES-COPA	Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink	Keyak	Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, Ronny Van Keer
AES-JAMBU	Hongjun Wu, Tao Huang	MORUS	Hongjun Wu, Tao Huang
AES-OTR	Kazuhiko Minematsu	NORX	Jean-Philippe Aumasson, Philipp Jovanovic, Samuel Neves
AEZ	Viet Tung Hoang, Ted Krovetz, Phillip Rogaway	OCB	Ted Krovetz, Phillip Rogaway
Ascon	Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer	Tiaoxin	Ivica Nikolić
CLOC	Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, Eita Kobayashi	Deoxys	Jérémy Jean, Ivica Nikolić, Thomas Peyrin

(جدول-۲): نامزدهای حاضر در دور دوم مسابقه‌ی CAESAR که نتوانستند به دور سوم برسند.

نامزد	طرح
HS1-SIV	Ted Krovetz
ICEPOLE	Paweł Morawiecki, Kris Gaj, Ekawat Homsirikamol, Krystian Matusiewicz, Josef Pieprzyk, Marcin Rogawski, Marian Srebrny, Marcin Wójcik
Joltik	Jérémy Jean, Ivica Nikolić, Thomas Peyrin
Minalpher	Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, Shoichi Hirose
OMD	Simon Cogliani, Diana-Ştefania Maimuţ, David Naccache, Rodrigo Portella do Canto, Reza Reyhanitabar, Serge Vaudenay, Damian Vizár
PAEQ	Alex Biryukov, Dmitry Khovratovich
π-Cipher	Danilo Gligoroski, Hristina Mihajloska, Simona Samardjiska, Håkon Jacobsen, Mohamed El-Hadedy, Rune Erlend Jensen, Daniel Otte
POET	Farzaneh Abed, Scott Fluhrer, John Foley, Christian Forler, Eik List, Stefan Lucks, David McGrew, Jakob Wenzel
PRIMATEs	Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Florian Mendel, Bart Mennink, Nicky Mouha, Qingju Wang, Kan Yasuda
SCREAM	Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici, Anthony Journault, François Durvaux, Lubos Gaspar, Stéphanie Kerckhof
SHELL	Lei Wang
STRIBOB	Markku-Juhani O. Saarinen, Billy B. Brumley
TriviA-ck	Avik Chakraborti, Mridul Nandi

(جدول-۳): نامزدهای معرفی‌شده در دور نخست مسابقهٔ **CAESAR** که نتوانستند به دور دوم راه بیابند. نامزهایی که روی آنها خط کشیده شده است، از نظر امنیتی نیرومند نبوده، لذا شکسته شده‌اند[۱].

نامزد	طراح
++AE	Francisco Recacha
AES-CMCC	Jonathan Trostle
~~AES-COBRA~~	Elena Andreeva, Andrey Bogdanov, Martin M. Lauridsen, Atul Luykx, Bart Mennink, Elmar Tischhauser, Kan Yasuda
AES-CPFB	Miguel Montes, Daniel Penazzi
Artemia	Javad Alizadeh, Mohammad Reza Aref, Nasour Bagheri
AVALANCHE	Basel Alomair
~~Calico~~	Christopher Taylor
CBA	Hossein Hosseini, Shahram Khazaei
~~CBEAM~~	Markku-Juhani O. Saarinen
Enchilada	Sandy Harris
~~FASER~~	Faith Chaza, Cameron McDonald, Roberto Avanzi
~~HKC~~	Matt Henricksen, Shinsaku Kiyomoto, Jiqiang Lu
iFeed[AES]	Liting Zhang, Wenling Wu, Han Sui, Peng Wang
Julius	Lear Bahack
KIASU	Jérémy Jean, Ivica Nikolić, Thomas Peyrin
LAC	Lei Zhang, Wenling Wu, Yanfeng Wang, Shengbao Wu, Jian Zhang
~~Marble~~	Jian Guo
~~McMambo~~	Watson Ladd
~~PAES~~	Dingfeng Ye, Peng Wang, Lei Hu, Liping Wang, Yonghong Xie, Siwei Sun, Ping Wang
~~PANDA~~	Dingfeng Ye, Peng Wang, Lei Hu, Liping Wang, Yonghong Xie, Siwei Sun, Ping Wang
POLAWIS	Arkadiusz Wysokinski, Ireneusz Sikora
Prøst	Elif Bilge Kavun, Martin M. Lauridsen, Gregor Leander, Christian Rechberger, Peter Schwabe, Tolga Yalçın
Raviyoyla	Rade Vuckovac
Sablier	Bin Zhang, Zhenqing Shi, Chao Xu, Yuan Yao, Zhenqi Li
Silver	Daniel Penazzi, Miguel Montes
Wheesht	Peter Maxwell
YAES	Antoon Bosselaers, Fre Vercauteren

۳-۱- ساختارهای اصولی

طرح‌هایی که به مسابقهٔ سزار معرفی شده‌اند، هرکدام برپایه یک ساختار هستند. در اینجا ساختارهای اصولی[1] که توسط طرح‌های مختلف مورد استفاده قرار گرفته‌اند، به‌طور مختصر بررسی می‌شود.

رمز قالبی. رمز قالبی برای رمزنگاری یک پیام، آن پیام را به قالب‌هایی با اندازهٔ یکسان شکسته و عمل رمزنگاری را بر روی هر قالب انجام می‌دهد. بسیاری از طرح‌های معرفی‌شده به مسابقهٔ CAESAR از جمله ۱۱ طرح راه‌یافته به دور سوم، از نوع رمزهای قالبی هستند.

رمز جریانی. رمز جریانی، در حین ارسال داده، آن را بیت به بیت رمز می‌کند؛ یعنی به‌جای اینکه دادهٔ رمزشده در یک فایل یا قالب قرار گیرد، سپس رمز شود، در هنگام ارسال رمزنگاری می‌شود. دو طرح از طرح‌های حاضر در دور سوم از نوع رمز جریانی هستند.

جایگشت بدون کلید. یک جایگشت بدون کلید، نگاشتی دوسویه روی رشته‌هایی با طول ثابت است. شماری از طرح‌های معرفی‌شده به مسابقهٔ سزار از جایگشت بدون کلید به‌عنوان اولیهٔ اصولی خود استفاده می‌کنند. مشهورترین جایگشت بدون کلید، ساختار اسفنجی [۱۵] است. در رمزنگاری، یک تابع اسفنجی یا یک ساختار اسفنجی، دسته‌ای از الگوریتم‌هایی هستند که دارای وضعیت داخلی متناهی هستند. ساختار یا تابع اسفنجی جریانی با طول متغیر از بیت‌ها را دریافت کرده و جریانی با طول دلخواه از بیت‌ها را خارج می‌کند. ساختارهای دولایه به ساختار اسفنجی بسیار نزدیک هستند [۱۶]؛ ولی برخلاف اسفنج‌ها که بین فراخوانی‌ها بدون وضعیت[2] هستند، ساختار دولایه

[1] Underlying Constructions

[2] State

پذیرای فراخوانی‌هایی است که یک رشتهٔ ورودی را دریافت و یک رشتهٔ خروجی را که وابسته به تمام ورودی قبلی است تولید می‌کنند.

توابع درهم‌ساز/ توابع فشرده‌ساز. توابع درهم‌ساز رشته‌هایی با طول دلخواه را به خروجی‌هایی با طول ثابت نگاشت می‌کنند. برای توابع درهم‌ساز رمزی، پیدا کردن یک برخورد، پیش‌نگاره[1] و پیش‌نگاره دوم امکان‌پذیر نیست. توابع فشرده‌ساز دو ورودی با طول ثابت را گرفته و به یک خروجی با طول ثابت فشرده می‌کنند؛ اما این کار به‌شکلی انجام می‌شود که پس از فشرده‌سازی، امکان بازیابی هر دو ورودی وجود داشته باشد.

اختصاصی[2]. ساختار برخی از طرح‌های معرفی‌شده، شبیه به طرح‌های فایستلی نوع ۳ [۱۷] است. چنین طرح‌هایی یک وضعیت چندبلاکی مثل $S_0,S_1,...,S_n$ را در طول فرآیند رمزگذاری و احراز اصالت نگه می‌دارند. به‌ازای هر بلاک داده، این وضعیت به‌روزرسانی می‌شود(مثلا: $S_0=S_0 \oplus M$). این به‌روزرسانی‌ها باعث تغییر در وضعیت شده و از همین تغییرات برای به‌دست‌آوردن مقدار متن رمزی (در رمزنگاری) و یا متن آشکار (در رمزگشایی) استفاده می‌شود. اگرچه این طرح‌ها نیز مبتنی بر یک سبک عمل خاص هستند، اما اولیه‌هایی که در این سبک‌ها استفاده می‌شود، به‌الزام یک رمز قالبی کامل نیست؛ بلکه می‌تواند بخشی از یک رمز قالبی باشد [۱].

۳-۲- روش‌های پوششی و سبک‌های اصولی

یک الگوریتم که از رمز بلاکی برای فراهم‌کردن امنیت مربوط به محرمانگی و احراز اصالت، استفاده می‌کند، به اصطلاح *سبک عمل* نامیده می‌شود. سبک عمل به‌طورمعمول برای انتقال امن داده‌های بزرگ‌تر از یک بلاک استفاده می‌شود. بنابراین، ما برای نامزدهایی که بر پایهٔ رمز قالبی هستند، سبک‌هایی را که این طرح‌ها از آنها ارث می‌برند، به‌روشنی بیان می‌کنیم. همچنین برای برخی طرح‌هایی که بر پایهٔ رمز قالبی نیستند، سبک اصلی آنها را بیان خواهیم کرد. سبک‌هایی که در جدول(۴) آورده شده، توسط طرح‌های مسابقه پذیرفته شده‌اند.

[1] Preimage
[2] Dedicated

(جدول-۴): روش‌های پوششی و سبک‌های اصولی به‌کارگرفته شده در نامزدهای مسابقهٔ CAESAR[۱].

نام سبک	توضیح
CFB	سبک بازخورد متن رمز[3][۱۸].
CTR	سبک شمارنده.
ECB	سبک کتاب رمز الکترونیکی.
EME	سبک رمزکردن-آمیختن-رمزکردن[4][۱۹].
iFeed	سبک iFeed [۲۰].
JHAE	سبکی بر پایه JH برای رمزگذاری احراز اصالت‌شده[5][۲۱].
LEX	سبک بیرون‌کشیِ نَشت[6][۲۲].
OFB	سبک بازخورد-خروجی.
OTR	فایستلیِ دو دور، دوشاخه[7][۲۳].
PFB	سبک بازخورد متن آشکار[8][۲۴].
PPAE	رمزگذاری احرازاصالت‌شده‌ی برپایه جایگشت که قابل موازی‌سازی است[9][۲۵].
SIV	سبک بردار مقداردهی اولیهٔ هم‌گذاشت[10][۲۶].
TAE	رمزگذاری احراز اصالت‌شدهٔ قابل تنظیم[11][۲۷].
XEX	XOR - رمز کردن - XOR[۲۸].

روش‌های پوششی. بسیاری از طرح‌های نوین که بر پایهٔ رمز قالبی هستند، برای جلوگیری از کنترل‌شدن ورودی و خروجی توسط فرد متخاصم، آن را در پوشش رمز قالبی در می‌آوردند. در طرح‌های معرفی‌شده، از موارد معرفی‌شده در جدول (۵) برای پوشش استفاده شده است.

(جدول-۵): روش‌های پوششی مورد استفاده در نامزدهای مسابقهٔ CAESAR[۱].

نام روش	توضیح
AX	افزایش[12] و XOR.
دوبرابرسازی[13]	XOR با متغیر وابسته به کلید که افزایش دوبرابری در میدان گالوا داشته است [۲۹].
GFM	ضرب با متغیر وابسته در میدان گالوا.
AES	XOR با مقدار زنجیره‌ای که توسط AES پردازش شده است[۳۰].

[3] Ciphertext Feedback Mode (CFB)
[4] Encrypt-Mix-Encrypt mode
[5] JH-based mode for authenticated encryption
[6] Leakage extraction mode
[7] Two-branch two-round Feistel
[8] Plaintext feedback mode
[9] Parallelizable permutation-based authenticated encryption
[10] Synthetic initialization vector mode
[11] Tweakable authenticated encryption
[12] Addition and XOR
[13] Doubling

۳-۳- خصوصیات عملکردی

در این بخش برخی از ویژگی‌های مهم و ویژگی‌های عملکردی معرفی می‌شوند. پشتیبانی از هر کدام از این ویژگی‌ها، باعث کاربردی‌ترشدن الگوریتم‌های رمزنگاری احراز اصالت‌شده می‌شود. در ادامه هریک از این ویژگی‌ها مورد بررسی قرار گرفته‌اند.

قابلیت موازی‌سازی. این قابلیت به این معنی است که یک طرح AE بتواند، قالب‌های پیام و یا متن رمزی را به‌صورت موازی پردازش کند. برخی برای به‌دست آوردن امنیت پایدارتر و برخی برای رسیدن به پیاده‌سازی سبُک‌وزن، ترتیبی‌بودن را برگزیده‌اند. یک کار رمزگذاری، قابل موازی‌سازی نامیده می‌شود، اگر در آن فرآیند برای هر $i \neq j$، پردازش i اُمین بلاک ورودی به خروجی پردازش j اُمین بلاک وابسته نباشد. در حالتی که این ویژگی کمی سست‌تر باشد، می‌توان طرح AE را قابل پیاده‌سازی روی خط لوله دانست اگر رمزگذاری(و نیز رمزگشایی) بتواند به عملیات $f \circ g$ شکسته شود، به‌شکلی که پیش از پایان رمزگذاری بلاک‌های پیشین، نخستین عمل $g(M_i)$ برای i اُمین بلاک انجام شده باشد. این نکته گفتنی است که توانایی موازی‌سازیِ عملیات رمزگذاری و رمزگشایی، جدا از هم هستند و بسیاری از طرح‌ها فقط در یکی از عملیات رمزگذاری یا رمزگشایی، موازی هستند؛ به همین دلیل ویژگی قابلیت موازی‌سازی را برای هر دو عمل نشان داده می‌شود.

برخط‌بودن. یک طرح AE که پیام‌های با طول دلخواه را به‌عنوان ورودی می‌گیرد، برخط است، اگر بتواند قالب‌های رمزی را به‌محض دریافت قالب‌های متن آشکار تولید کند. البته پردازش قالبی رمزی i اُم تنها باید به کلید و $i-1$ قالبی متن آشکار نخست بستگی داشته باشد.

پشنیبانی از دادهٔ وابسته: در بسیاری از کاربردها، علاوه‌بر اینکه پیام M رمزگذاری و احراز اصالت می‌شود، لازم است داده‌ای مثل H نیز وجود داشته باشد؛ به‌طوری که این داده احراز اصالت بشود، اما رمزگذاری نشود. این الزام باعث می‌شود تا برخی از طرح‌های AE از قابلیت اضافه‌کردن دادهٔ وابسته به ورودی خود برخوردار باشند. چنین طرح‌هایی، طرح‌های AEAD نامیده می‌شوند. با توجه به اینکه در طرح‌های AE ترکیبی، کار رمزگذاری و احراز اصالت به‌طور جدا از هم انجام می‌شود، بنابراین مسألهٔ AEAD برای این نوع طرح‌ها به‌سادگی قابل حل خواهد بود؛ اما این کار برای طرح‌های AE اختصاصی تا حدودی سخت است.

تک‌گذری‌بودن. بدین معنی است که یک طرح AE، تنها با انجام یک سری محاسبات روی هر قالب پیام، بتواند قالب رمزی و برچسب احراز اصالت را هم‌زمان با هم تولید کند. اکثر طرح‌های AE اختصاصی تک‌گذری هستند.

پشتیبانی از طول کلید، طول تک‌شمار و طول برچسب احرازاصالت متفاوت. یکی از بهترین ویژگی‌های AES نسخه‌های متنوع آن است. بر فرض مثال، در ساده‌ترین حالت اگر روزی توان پردازشی اجازهٔ حمله جامع کلید روی AES-128 را داد، نباید نگران امنیت AES بود؛ زیرا می‌توان از نسخهٔ AES-192 و AES-256 استفاده کرد. پشتیبانی از طول کلید، تک‌شمار و برچسب احراز اصالت متمایز، نشان از انعطاف‌پذیری یک طرح دارد [۱].

مبتنی بر رمز، تابع تصادفی یا جایگشت‌بودن.

وارون نداشتن: یک طرح AE که فقط یکی از دو تابع رمزگذاری یا رمزگشایی را به‌کار می‌گیرد، می‌تواند به میزان قابل توجهی در مصرف حافظه و مساحت صرفه‌جویی کند. یک طرح AE، بدون وارون است، اگر این طرح نیازی به عملیات وارونِ اولیه‌ی اصولی خود، نداشته باشد؛ به‌عنوان‌مثال فقط نیاز به عمل رمزگشایی رمز قالبی داشته باشد.

مبتنی بر AES بودن. پس از معرفی AES در سال ۲۰۰۱، در طول سال‌ها، تلاش‌های زیادی در رابطه با تحلیل AES انجام شده است؛ به‌شکلی که تا اندازهٔ خیلی خوبی جزئیات مربوط به امنیت آن شناخته شده و ثابت شده است که می‌توان به امنیت آن اعتماد کرد. به‌علاوه، از وقتی که ریزمعماری Westmere به‌عنوان نخستین فراهم‌کنندهٔ دستورالعمل‌های ویژه AES، توانست زمان‌های رمزگذاری و رمزگشایی را به زمانی ثابت و بسیار سریع برساند، طرح‌هایی که از این نخستین استاندارد به‌عنوان اولیه اصولی خود استفاده می‌کنند، می‌توانند از مزیت پشتیبانی اکثریت پردازنده‌های امروزی از دستورالعمل‌های ویژه‌ی AES بهره‌مند شوند. این پشتیبانی برای طراحان می‌تواند وسوسه‌انگیز باشد.

رمزگذاری احراز اصالت‌شدهٔ نموی[1]: ممکن است در پیام‌های پشت سرِ هم، فقط بخشی از پیام (به‌عنوان‌مثال یک بلاک) با پیام بعدی یا قبلی متمایز باشد. در دو پیام M و M'

[1] Incremental AE

که فقط در بخش کوچکی با هم تفاوت دارند، اگر از پیام قبلی یا M، پس از رمزگذاری و احراز اصالت دوتایی (C,T) به‌دست بیاید، آنگاه رمزگذاری و احراز اصالت پیام 'M می‌تواند در زمان مناسبی که به نسبت کمتر از زمان مربوط به رمزگذاری و احراز اصالت کل پیام 'M است، انجام شود. در اینجا می‌توان فقط همان بخشی از داده‌ها را که نسبت به پیام قبلی متمایز است، محاسبه کرد و زمان را کاهش داد. چنین طرح‌هایی را طرح‌های فراهم‌کنندهٔ رمزگذاری احراز اصالت‌شدهٔ نمُوی می‌گویند. البته گفتنی است که برخی از طرح‌ها، با شرط استفاده مجدد از تکرارناپذیر تک‌شمار، این خصیصه را فراهم می‌کنند. استفادهٔ مجدد از تکرارناپذیر تک‌شمار با سوء استفاده از آن متمایز است و سوء استفاده یک اشتباه است و نباید چنین اشتباهی را برای رسیدن به یک ویژگی خوب انجام داد؛ از این رو، ما فقط طرح‌های فراهم‌کنندهٔ رمزگذاری احراز اصالت‌شدهٔ نمُوی(بدون استفاده مجدد از تکرارناپذیر تک‌شمار) را مشخص خواهیم کرد [۱].

دادهٔ وابستهٔ نمُوی. این خاصیت همانند رمزگذاری احراز اصالت‌شدهٔ نموی است. فرض کنید نتیجهٔ پردازش دادهٔ وابستهٔ قبلی دخیره شده باشد، و دادهٔ وابستهٔ کنونی در بخشی کمی از خود، با دادهٔ وابستهٔ پیشین متمایز باشد؛ طرح AE می‌تواند دادهٔ وابسته نمُوی را فراهم کند اگر بتواند از نتیجهٔ پردازش بلاک‌های همانند دادهٔ وابستهٔ قبلی، استفاده کرده و فقط محاسبات را برای بخشی از دادهٔ وابستهٔ کنونی که متمایز با قبلی است، انجام دهد.

استفادهٔ دوباره از دادهٔ وابستهٔ ثابت. برخی کاربردها از دادهٔ وابستهٔ یکسان یا با کمی تغییر به‌ازای هر دادهٔ وابسته، برای پیام‌های بعدی استفاده می‌کنند[۳۱]. طرح‌هایی که می‌توانند از نتیجهٔ پردازش دادهٔ وابسته پیام‌های پیشین استفاده کنند، می‌توانند افزایش سرعت بسیار خوبی داشته باشند. این طرح‌ها می‌توانند استفاده مجدد از دادهٔ وابسته را فراهم کنند. البته به‌شرطی که تکرارناپذیر تک‌شمار به دادهٔ وابسته، ارتباطی نداشته باشد و در طول فرآیند رمزگذاری و احراز اصالت به هم وابستگی نباشند.

برچسب‌های میانی: درصورتی‌که بخشی از یک بلاک رمزگشایی‌شده نامعتبر باشد، برچسب‌های میانی[۳۲] به گیرنده امکان کشف زودتر این عدم اعتبار را می‌دهد. این کار میزان پردازش‌های مربوط به احراز اصالت پیام‌های طولانی را کاهش می‌دهد.

۴- مروری بر نامزدهای مسابقه CAESAR

تا زمان نگارش این مقاله (مهر ۱۳۹۵) از ۵۷ طرحی که در دور نخست مسابقه به‌منظور انجام تحلیل روی آنها، عمومی شدند، تعداد ۹ طرح شکسته شده‌اند. در قسمت بعد معرفی کوتاهی از این طرح‌ها خواهیم داشت.

۴-۱- نامزدهایی که شکسته شده‌اند.

AES-COBRA. یک سبک رمزگذاری احرازاصالت‌شده‌ی بر مبنای رمز قالبی AES است. نَندی[۳۳] یک حمله جعل روی رمز قالبی n بیتی، فقط با O(n) پرس و جو با احتمال موفقیت $\frac{1}{2}$ انجام داد و ادعای امن‌بودن این سبک را باطل کرد.

Calico. یک الگوریتم احرازاصالت‌شده بر پایهٔ رمز جریانی است. دوبرانیگ و همکاران [۳۴] موفق به انجام حمله جعل با زمان و موفقیت صد درصدی روی الگوریتم شدند. همچنین ایشان حملهٔ بازیابی کلید MAC را در زمان 2^{128-N} برای $N \leq 64$ را روی الگوریتم با احتمال موفقیت صد درصد انجام دادند.

CBEAM. یک الگوریتم احرازاصالت‌شده با پشتیبانی از دادهٔ وابسته است. میناود[۳۵] یک حمله تفاضلی با احتمال موفقیت 2^{-43} که بر خلاف 2^{-63} است ارائه داد.

FASER. یک الگوریتم احرازاصالت‌شده با دو نسخهٔ ۱۲۸ و ۲۵۶ بیتی است. ژو و همکاران[۲۰] یک حمله همبستگی روی هر دو نسخه ۱۲۸و ۲۵۶ بیتی ارائه دادند. به‌علاوه، فِنگ و همکاران [۳۶] نشان دادند که حملهٔ بازیابی کلید روی نسخه ۱۲۸ بیتی که کلید ۶۴ بیتی دارد، تمامی کلیدها را به‌صورت بلادرنگ بازیابی می‌کند.

HKC. یک الگوریتم رمزگذاری احراز اصالت‌شده بر مبنای رمز جریانی است. مارکو سارینِن[۳۷] نشان داد که حملهٔ جعل پیام روی این الگوریتم بدیهی است و امنیت ادعاشده درست نیست.

Marble. یک الگوریتم احراز اصالت‌شده با پشتیبانی از دادهٔ وابسته است. فور و همکاران [۳۸] یک حمله جعل ساده را روی سبک عمل Marble انجام دادند که فقط از ۲۶۴ پرس‌وجوی متن آشکار انتخابی بهره می‌برد. لو و همکاران[۳۹] نشان دادند که هنوز هم این الگوریتم در مقابل حمله جعل و حمله بازیابی کلید ناتوان است.

McMambo. یک رمز قالبی با سبک عمل مبتنی بر رمز Mambo است. نِوِس[۴۰] نشان دادند که یک تفاضل تکراری با احتمال 2^{-2} روی دو دور کامل از McMambo وجود دارد.

PAES. یک الگوریتم احرازاصالت‌شده با دو نسخهٔ ۴ و ۸ بیتی است. ساسکی و هکاران[۴۱] نشان دادند که یک حملهٔ جعل فراگیر روی PAES-8 با ۲۱۱ پرس‌وجوی رمزنگاری عملی است.

PANDA. یک خانواده از رمزهای احراز اصالت‌شده است. ساسکی و همکاران[۴۲] یک حملهٔ جعل در شرایطی که تکرارناپذیر تک‌شمار در نظر گرفته شود، روی PANDA-s با هزینهٔ محاسباتی ۶۴ و مقدار اندکی حافظه انجام دادند. همچنین، فِنگ و همکاران[۴۳] حمله بازیابی کلید و همچنین یک حمله جعل دیگر، با پیچیدگی زمانی ۲۴۱ روی PANDA-s انجام دادند [۱].

۴-۲- تحلیل‌های انجام‌شده، روی نامزدهایی که شکسته نشده‌اند.

در این بخش تمامی تحلیل‌های انجام‌شده را روی نامزدهایی که شکسته نشده‌اند، در جدول (۶) و (۷) نشان خواهیم داد.

(جدول-۶): طرح‌های بر مبنای رمز قالبی و جریانی، به همراه تحلیل‌های انجام‌شده روی هر کدام. طرح‌هایی که با * علامت گذاری شده‌اند، به دور دوم مسابقه راه پیدا نکرده‌اند (طرح‌هایی که با + علامت گذاری شده‌اند، به دور دوم مسابقه راه پیدا کردند اما نتوانستند در دور سوم حضور داشته باشند) [۱].

رمز قالبی		رمز جریانی	
کاندید	تحلیل رمز	کاندید	تحلیل رمز
*AE++	جعل	ACORN	بازیابی کلید/ وضعیت
AES-COPA	جعل فراگیر	*Sablier	بازیابی کلید
AES-JAMBU	تمایز	*Wheesht	تمایز و بازیابی کلید و جعل
*AES-CMCC	جعل، تمایز	*Raviyoyla	تمایز و جعل
*AVALANCHE	جعل ، بازیابی کلید		
*CBA	تمایز		
*Julius- ECB	جعل		
*LAC	جعل تفاضلی		
*POET	جعل ، کلید سست		
+iSCREAM	جعل ، کلید سست، بازیابی کلید		

(جدول-۷): طرح‌های بر مبنای رمز قالبی و جریانی، به‌همراه تحلیل‌های انجام‌شده روی هر کدام. طرح‌هایی که با * علامت‌گذاری شده‌اند، به دور دوم مسابقه راه پیدا نکرده‌اند (طرح‌هایی که با + علامت گذاری شده‌اند، به دور دوم مسابقه راه پیدا کردند اما نتوانستند در دور سوم حضور داشته باشند) [۱].

اسفنجی		جایگشتی	
کاندید	تحلیل رمز	کاندید	تحلیل رمز
+ICEPOLE	بازیابی وضعیت	*Prøst-OTR	جعل
+π-cipher	دومین پیش‌نگاره برچسب، جعل		
+PRIMATEs	جعل، حمله‌ی بازیابی کلید مکعبی		

۴-۳- پیمایشی کلی روی همهٔ طرح‌ها.

در ادامه، پیمایشی کلی روی خاصیت‌های امنیتی و کارکردی طرح‌های شکسته‌نشدهٔ مسابقهٔ CAESAR خواهیم داشت. جدول‌های (۸) و (۹) پارامترها و خاصیت‌های طرح‌هایی را که بر پایهٔ رمز قالبی یا دنباله‌ای، تابع فشرده‌سازی، جایگشتی و اسفنجی هستند، فهرست می‌کند.

(جدول-۸): طرح‌های مبتنی بر رمز قالبی. ❋=توصیه اصلی بر استفاده از AES است. ●= پشتیبانی از ویژگی. – = به‌نظر می‌رسد که از ویژگی پشتیبانی نمی‌کند. ○= قابل پیاده‌سازی روی خط لوله[۱].

نامزد	سبک	پوشش	اولیه	ویژگی‌ها							امنیت		
				برچسب‌های میانی	استفاده مجدد از AD	AD/AE نمونی	وارون نداشتن	برخط	Enc/Dec موازی	سوء استفاده ازرمزگشایی	سوء استفاده از تک‌شمار	امنیت اثبات شده
++AE	ECB	AX	AES	–	–	–/–	–	●	●/●	–	●	–
AES-CMCC	CBC	-	AES	–	–	–/–	●	–	–/●	–	●	●
AES-COPA	EME	Doubling	AES	–	●	●/–	●	●	●/●	–	●	●
AES-CPFB	CTR,PFB	-	AES	–	●	●/–	●	●	●/●	–	●	●
AES-JAMBU	OFB	-	AES	–	–	–/–	●	●	–/–	–	●	–
AES-OTR	OTR	Doubling	AES	–	●	●/–	●	●	●/●	–	–	●
AEZ	OTR	-	AES-4	–	●	●/–	●	–	●/●	●	●	●
AVALANCHE	ECB	-	AES	–	–	–/–	●	●	●/●	–	–	●
CBA	ECB	Doubling	AES	–	●	●/–	●	●	●/●	–	–	–
CLOC	CFB	-	AES*	–	●	–/–	●	●	–/–	–	–	●
Deoxys6	TAE	-	Deoxy-BC,AES	–	–	–/–	–	●	●/●	–	–	●
ELmD	EME	Doubling	AES	●	–	–/–	–	●	●/●	–	●	●
iFeed[AES]	iFeed	Doubling	AES	●	●	●/–	●	●	●/–	–	●	●
iSCREAM	TAE	-	iSCREAM,SPN	–	–	–/–	●	●	●/●	–	–	–
Joltik	TAE	-	Joltik-BC,AES	–	–	–/–	–	●	●/●	–	–	●
Julius-CTR	CTR	-	AES	–	–	–/–	●	–	●/●	–	–	●
Julius-ECB	ECB	GFM	AES	–	–	–/–	–	–	●/●	–	●	●
KIASU	TAE	GFM	KIASU-BC,AES	–	–	–/–	–	●	●/●	–	–	●
KIASU	EME	-	KIASU-BC,AES	–	–	–/–	–	●	●/●	–	●	●
LAC	LEX	-	L-Block	–	–	–/–	–	●	●/●	–	–	–
OCB	XEX	Doubling	AES	–	–	–/–	–	●	●/●	–	–	●
POET	ECB	AES-4/10	AES	●	●	●/–	●	●	○/○	●	●	●
SCREAM	TAE	-	SCREAM-SPN	–	–	–/–	●	●	●/●	–	–	–
SHELL	EME	CTR,Doubling	AES	–	–	–/–	–	●	●/●	–	●	●
SILC	CFB	-	AES*	–	–	–/–	●	●	–/●	–	–	●
SILVER	TAE	-	MAES	–	–	–/–	–	●	●/●	–	–	●
YAES	CTR	-	AES	–	●	●/–	●	●	●/●	–	–	–

(جدول-۹): طرح‌های اختصاصی، مبتنی بر رمز دنباله‌ای، تابع فشرده‌سازی، جایگشتی و اسفنجی. ●= پشتیبانی از ویژگی. – = به نظر می‌رسد که از ویژگی پشتیبانی نمی‌کند. **n.n.**= اولیهٔ انتخابی و بدون نام[۱].

ساختار	نامزد	طراحی	اولیه	ویژگی‌ها						امنیت		
				برچسب‌های میانی	استفاده مجدد از *AD*	نمُوی *AD/AE*	وارون نداشتن	برخط	موازی *Enc/Dec*	سوء استفاده از رمزگشایی	سوء استفاده از تک‌شمار	امنیت اثبات شده
اختصاصی	AES-AEGIS	AES	AES_round	–	–	–/–	●	●	●/–	–	–	–
	MORUS	LRX	MORUS	–	–	–/–	●	●	–/–	–	–	–
	Tiaoxin	AES	AES_round	–	–	–/–	●	●	●/●	–	–	–
بر مبنای رمز دنباله‌ای	ACORN	LFSR	ACORN	–	–	–/–	●	●	●/●	–	–	–
	Enchalida	-	ChaCha,Rijndael	–	●	●/–	●	●	●/●	–	–	●
	HIS-SIV	SIV	ChaCha,Poly1305	–	–	–/–	●	–	–/–	–	●	●
	Raviyoyla	-	MAGv2	–	–	–/–	●	●	–/–	–	–	–
	Sablier	LFSR	Sablier	–	●	●/–	●	●	●/●	–	–	–
	TriviA-ck	-	Trivia-SC	●	–	–/–	●	–	●/●	–	–	●
	Wheesht	ARX	Wheesht	–	–	–/–	●	●	–/–	–	–	–
بر مبنای توابع فشرده-ساز	OMD	-	SHA-256/512	–	●	●/–	●	●	–/–	–	–	●
برمبنای جایگشت	Minalpher	SPN-XEX	Minalpher-p	–	–	–/–	–	●	●/●	●	●	●
	PAEQ	PPAE	AESQ	–	●	●/●	●	●	●/●	–	●	●
	Prøst-COPA	SPN-EME	Prøst	–	●	●/–	●	●	●/●	–	●	●
	Prøst-OTR	SPN-OTR	Prøst	–	●	●/–	●	●	●/●	–	–	●
بر مبنای اسفنج	Artemia	SPN	JHAE	–	–	–/–	●	●	–/–	–	●	●
	ASCON	SPN-Duplex	Ascon	–	–	–/–	●	●	–/–	–	●	●
	ICEPOLE	Duplex	Keccak-like	●	–	–/–	●	●	●/●	–	●	●
	Ketje	Duplex	Keccak-f	●	–	–/–	●	●	–/–	–	–	●
	Keyak	Duplex	Keccak-f	●	–	–/–	●	●	●/●	–	–	●
	NORX	LRX, Duplex	n.n.	–	–	–/–	●	●	●/●	–	–	●
	π-cipher	ARX, Duplex	n.n.	–	–	–/–	●	●	●/●	–	–	●
	PRIMATEs GIBBON	SPN, Duplex	PRIMATE	–	–	–/–	●	●	–/–	–	–	●
	PRIMATEs-HANUMAN	SPN, Duplex	PRIMATE	–	–	–/–	●	●	–/–	–	–	●
	PRIMATEs-APE	SPN, Duplex	PRIMATE	–	●	●/–	–	●	–/–	●	●	●
	STRIBOB	Duplex	Streebog	–	–	–/–	●	●	–/–	–	–	●

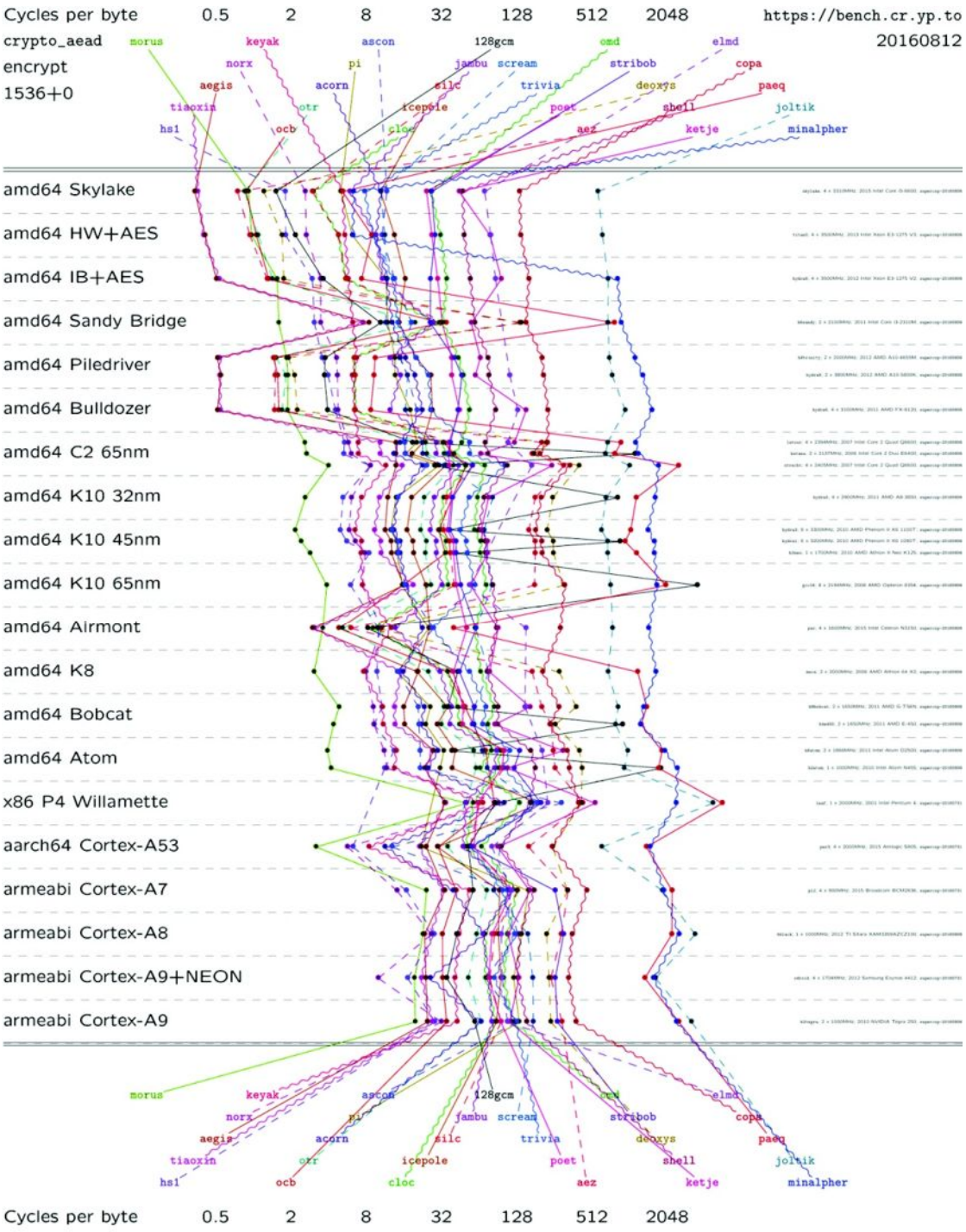
۵- ارزیابی کارآیی

SUPERCOP [۴۴] ابـزاری بـرای انـدازه‌گیـری کـارآیی نـرم‌افـزاری‌هـای رمزنگـاری اسـت کـه توسـط آزمایشـگاه VAMPIRE توسـعه داده شـده اسـت. SUPERCOP برابـر کوته‌سازی، عبارت سامانه‌ای برای ارزیابی کـارآیی یکپارچـه، مرتبط با اولیه‌ها و عملیات رمزنگاری[1] است. در آخرین نسخه آن کارآیی توابع درهم‌ساز، رمزهای جریـانی کلیـد محرمانـه، سامانه‌های امضای کلید عمومی و سامانه‌های رمزی-اشتراکی اندازه‌گیری شده است. این ابـزار تمـامی نامزدهـای مسـابقهٔ سزار را به زبان C در سیستم‌عامل لینوکس پیاده‌سازی کرده اسـت و بـرای ارزیـابی کـارآیی روی بسـترهای متفـاوت در دسترس عموم قرار داده است. علاقه‌مندان می‌توانند این ابزار را از تارنمـای SUPERCOP، دریافـت کننـد و کـارآیی نامزدهای مختلف را در بسترهای متفاوت بیازمایند.

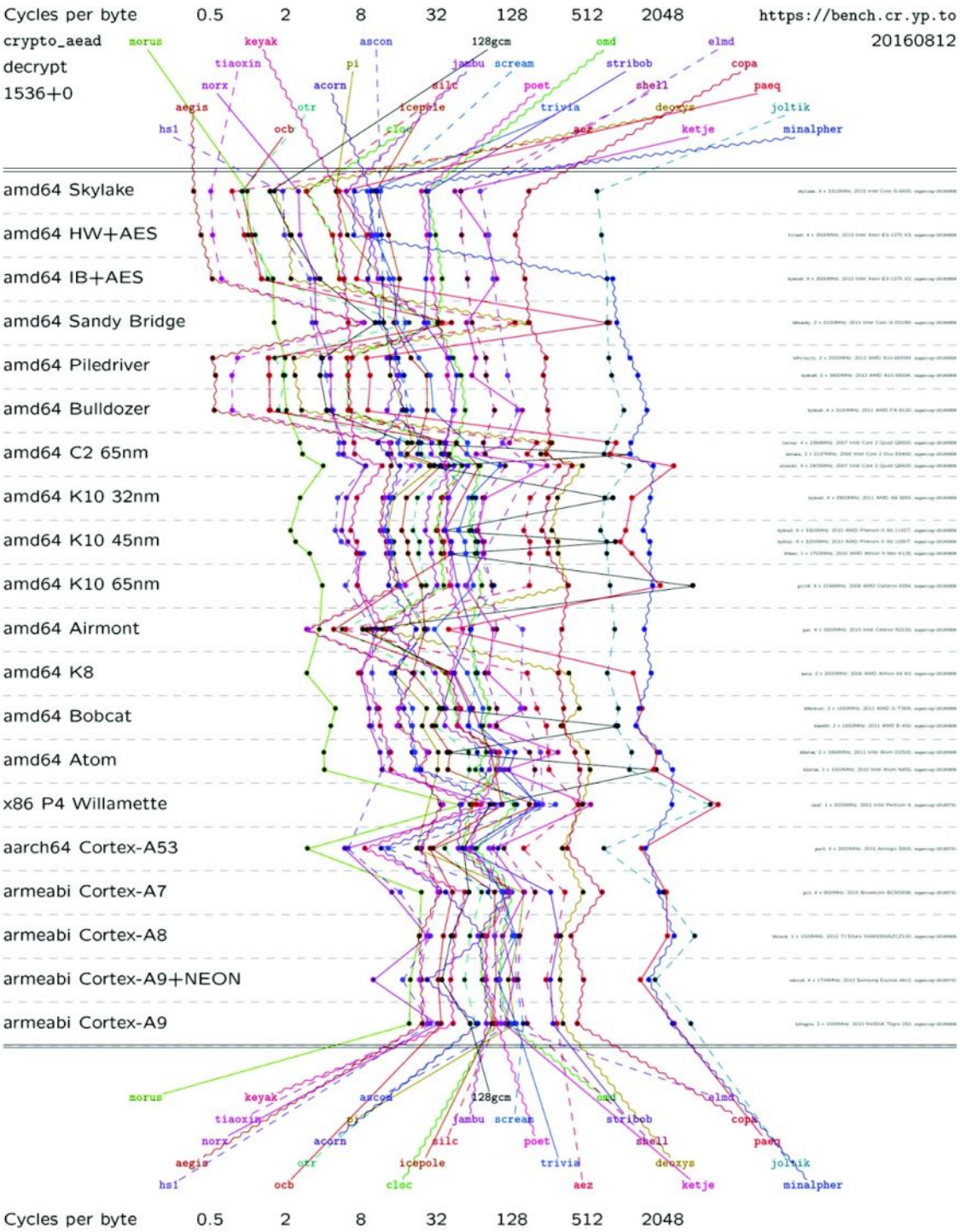
eBAEAD[2] [۴۵]، محـک eCRYPT رمزهـای متقـارن، بـر اساس نتایج SUPERCOP ارزیابی‌هـایی را روی گزیـده‌ای از طرح‌های راه‌یافته به دور دوم مسابقه، روی چندین پردازنـده از سـه معمـاری amd64 و armeabi و mipso32 انجـام داده است. پردازنده‌ها بر اساس معماری آنهـا مرتـب شـده‌انـد. در شکل های (۱) تا (۵) نتایج این ارزیابی‌ها آورده شده اسـت. نتایج ارزیابی برای مراحل رمزنگاری و رمزگشایی و تشخیص جعلی‌بـودن انـواع متفـاوت از داده‌هـا آورده شـده اسـت. در شـکل‌هـا، encrypt 1536+0 بـه ایـن معناسـت کـه نتـایج ارزیابی‌ها سرعت رمزگشایی یک پیام ۱۵۳۶ بایتی بدون دادهٔ وابسته را نشان می‌دهد. همچنـین long+long encrypt نیـز نشان‌دهندهٔ سرعت رمزنگاری یک پیام طولانی با دادهٔ وابستهٔ طولانی است. forgery 1536+0، سرعت تشخیص یک پیام ۱۵۳۶ بایتی جعلیِ بدون دادهٔ وابسـته اسـت. بـا نگـاهی بـه تمامی پیاده‌سازی‌هایی که روی پردازنده‌های مختلـف انجـام شده است، بـا درنظـرگـرفتن نسـخهٔ ۵ ابـزار SUPERCOP، مشاهده می‌شود که در معماری amd64، دو طرح aegis128l و tiaoxinv1 در صدر پرسرعت‌ترین طرح‌ها قرار دارند. دلیـل این نزدیکی در سرعت، ساختار مشابه آنها است. در معمـاری armeabi دو طـرح norx6441v1 و morus640128v1 جـزء بهتـرین‌هـا هسـتند و در معمـاری mipso32 طـرح morus1280128v1 پرسرعت‌تـرین طـرح اسـت. نکتـهٔ قابـل توجه در میان طرح‌های سریع، رمز قـالبی بـودن آنهـا و نیـز مبتنـی بـر AES بـودن آنهاسـت. بـه‌دلیـل آنکـه روش‌هـای گونـاگون و سـریعی بـرای پیـاده‌سـازی AES وجـود دارد، استفاده از این الگوریتم به عنوان یک اولیه در برخی نامزدها، به آنها این امکان را می‌دهد که از پیاده‌سـازی‌هـای متنـوع و سریع AES اسـتفاده کننـد. در بخـش کـم‌سـرعت‌تـرین‌هـا، می‌توان بـه سـه طـرح joltic، minalpher و kayak بـه‌ازای تمامی پیاده‌سازی‌ها، اشاره کرد.

با نگاهی به نامزدهای راه‌یافته به دور سـوم، مشـاهده می‌شود که برای انتخاب نامزدهای برتر، امنیت نامزدها بسیار مهم است. به‌طورمثال از هفده نامزد دور سـوم، دوازده نـامزد مبتنی بر رمز قالبی هسـتند و هـر دوازده نـامزد از الگـوریتم رمزنگاری AES به‌عنوان یک اولیه در خود استفاده کرده‌انـد. این الگوریتم سطوح مختلفـی از امنیـت را ارائـه مـی‌دهـد و امنیت آن نیز بر هیچکس پوشیده نیست. عـلاوه بـر امنیـت، سرعت رمزنگاری و احراز اصالت نامزدها نیز نقـش مهمـی در انتخاب آنها داشته است. با نگاهی به شکل‌هـای (۱) تـا (۵)، مشاهده می‌شود که به‌طورتقریبی بیش‌تر نامزدهـای سـریع، به دور سوم راه‌یافتـه انـد. همـان‌طـورکـه گفتـه شـد، همـهٔ نامزدهای مبتنی بر رمزقـالبی از الگـوریتم رمزنگـاری AES به‌عنوان یک اولیه در خود استفاده کرده‌اند. این انتخـاب هـم به امنیت و هـم بـه افـزایش سـرعت رمزنگـاری آنهـا کمـک می‌کند؛ زیرا می‌تواننـد از دسـتورالعمل ویـژهٔ AES کـه روی بیشتر پردازنده‌های x86 موجود در بازار قابل دسترس اسـت، استفاده کنند و افزایش سرعت بسیار خوبی را به‌دست آورند. ویژگی دیگری که در تمامی نامزدهای دور سوم وجـود دارد، بـرخط‌بـودن آنهاسـت کـه نشـان‌دهنـدهٔ اسـتقبال جامعـهٔ رمزنگاری از این ویژگی است. در میان نامزدهـای دور سـوم، نامزدهایی مثل ACORN که یک الگوریتم رمزنگـاری احـراز اصالت‌شدهٔ سبک‌وزن است نیز دیده می‌شـود کـه مـی‌توانـد بیان‌گر این نکته باشد که شاید یـک طـرح خـاص بـه‌عنـوان برندهٔ مسابقه معرفی نشود، بلکـه در هـر کـاربرد، یـک طـرح به‌عنوان برنده معرفی شود.

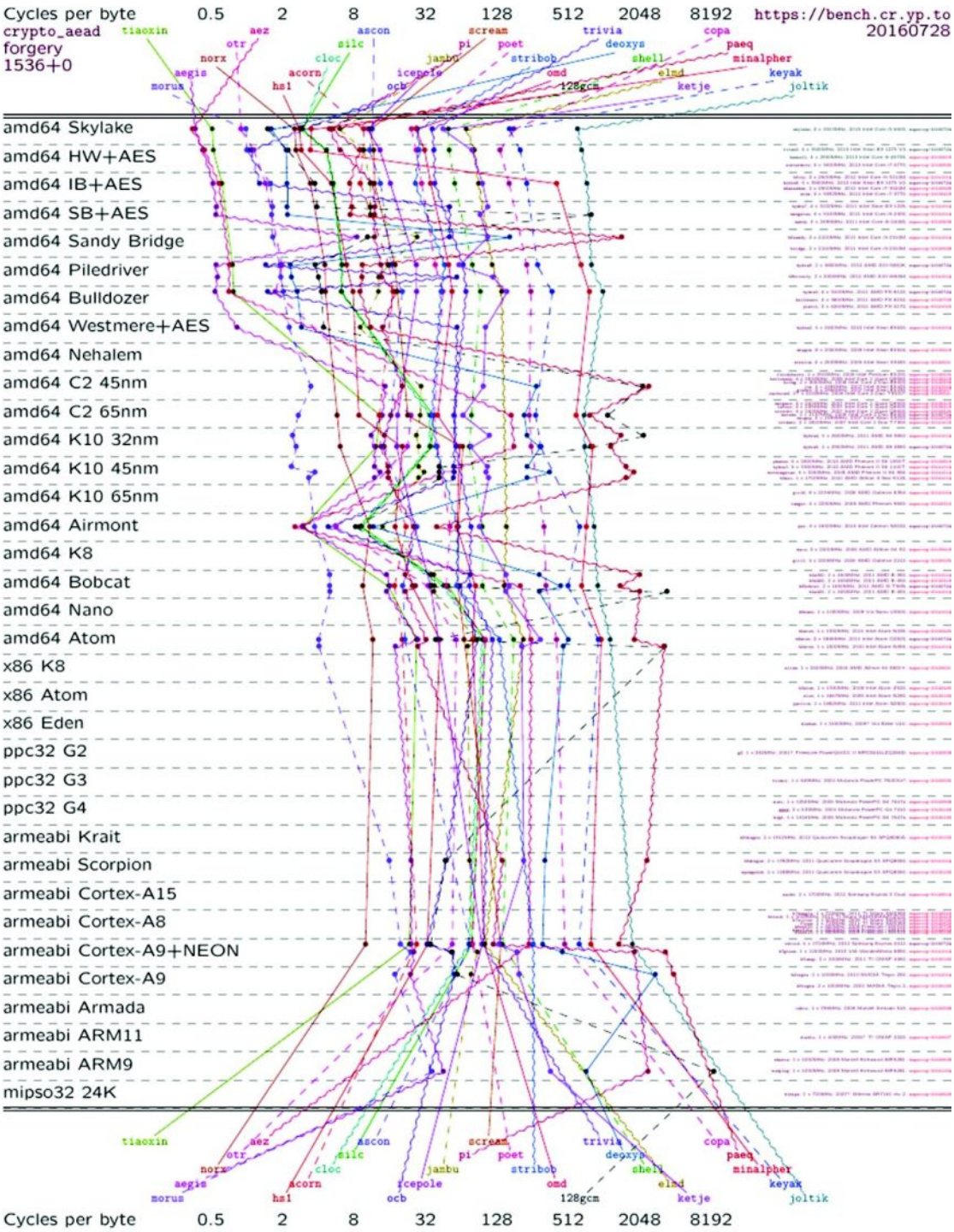
[1] System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives
[2] **E**CRYPT **B**enchmarking of **A**uthentic**a**te**d** Cipher



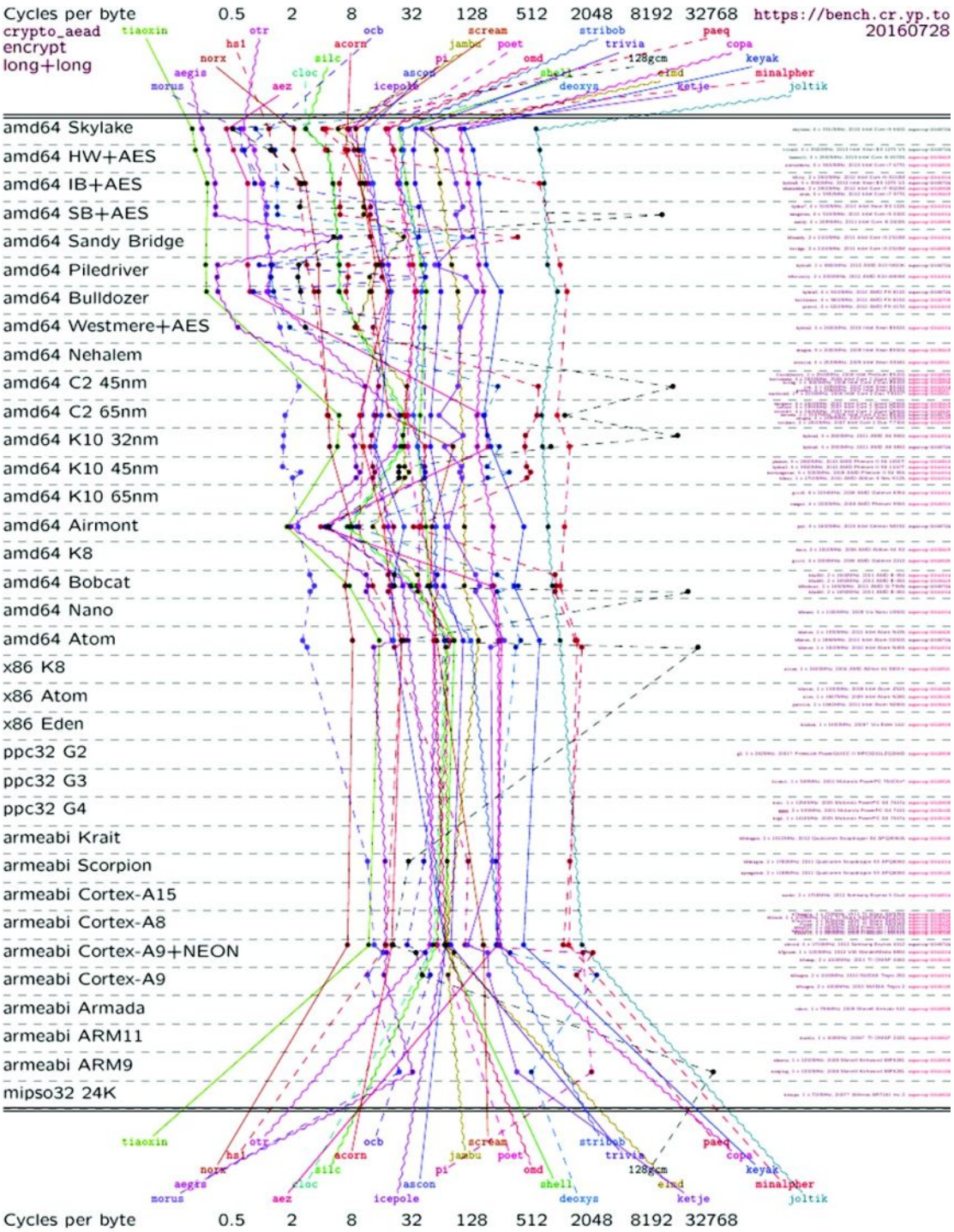
(شکل-۱): ارزیابی سرعت طرح‌های متفاوت برای رمزنگاری یک پیام ۱۵۳۶ بایتی بدون داده‌ی وابسته[۴۵].



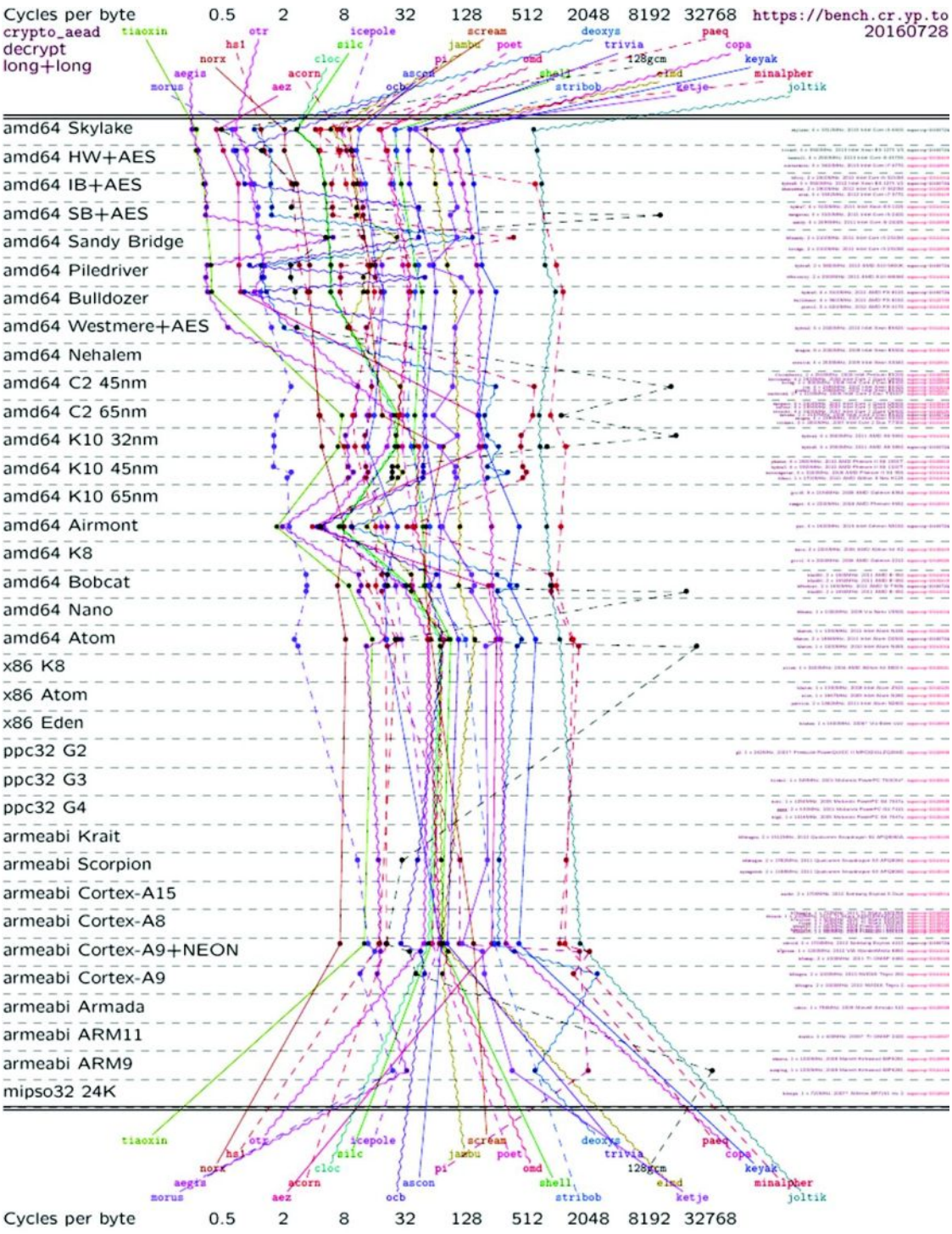
(شکل-۲): ارزیابی سرعت طرح‌های متفاوت برای رمزگشایی یک پیام ۱۵۳۶ بایتی بدون داده‌ی وابسته[۴۵].



(شکل-۳): ارزیابی سرعت طرح‌های متفاوت برای تشخیص یک پیام ۱۵۳۶ بایتی جعلی بدون داده‌ی وابسته [۴۵].



(شکل-۴): ارزیابی سرعت طرح‌های متفاوت برای رمزنگاری یک پیام طولانی با داده‌ی وابسته طولانی [۴۵].



(شکل-۵): ارزیابی سرعت طرح‌های متفاوت برای رمزگشایی یک پیام طولانی با دادهٔ وابسته طولانی [۴۵].

۶- نتیجه‌گیری

در این مقاله، علاوه‌بر معرفی الگوریتم‌های رمزنگاری احراز اصالت‌شده، تمامی نامزدهای معرفی‌شده به مسابقهٔ CAESAR دسته‌بندی شد و مروری کلی روی جنبه‌های عملکردی، پارامترهای امنیتی و نیرومندی نامزدها صورت گرفت؛ سپس تمامی نامزدها از نظر سرعت رمزگذاری،

رمزگشایی و تشخیص پیام‌های جعلی، روی پردازنده‌هایی از سه معماری amd64، armeabi و mipso32 مورد مقایسه قرار گرفته‌اند. مقایسه‌ها نشان داد، علاوه‌بر امنیت نامزدها، سایر ویژگی‌ها نیز برای انتخاب نامزد مهم هستند. به‌عنوان‌مثال نامزدهایی که علاوه‌بر امنیت بالا، سرعت رمزنگاری و احرازاصالت بالایی را فراهم می‌آورند، به دورهای بالاتر مسابقه راه یافته‌اند. همچنین با نگاهی به نامزدهای دور سوم، مشاهده می‌شود که دوازده نامزد از هفده نامزد دور سوم، از نوع مبتنی بر رمز قالبی هستند که نشان‌دهندهٔ نیرومندی این نوع رمزنگاری است. همچنین برخطبودن تمامی نامزدهای دور سوم نشان از اهمیت این ویژگی برای جامعهٔ رمزنگاری است.

۷- منابع

[1] Farzaneh Abed, Christian Forler, and Stefan Lucks. General Overview of the First-Round CAESAR Candidates for Authenticated Encryption Version of February 25, 2015

[2] Phillip Rogaway. Authenticated-Encryption with Associated-Data. In ACM Conference on Computer and Communications Security, pages 98–107, 2002.

[3] Dworkin, Morris J. "Sp 800-38c. Recommendation for block cipher modes of operation: the ccm mode for authentication and confidentiality." (2004).

[4] National Institute of Standards and Technology. Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC . Special Publication 800-38D, 2007.

[5] M Agren, Martin, et al. "Grain-128a: a new version of Grain-128 with optional authentication." International Journal of Wireless and Mobile Computing 5.1 (2011): 48-59.

[6] H.Wu, B.Preneel . AEGIS: A Fast Authenticated Encryption Algorithm. Selected Areas in Cryptography , volume 8282 of Lectute Notes in Computer Scince . Springer (2013)

[7] Jakimoski, Goce, and Samant Khajuria. "ASC-1: an authenticated encryption stream cipher." International Workshop on Selected Areas in Cryptography. Springer Berlin Heidelberg, 2011.

[8] Bogdanov, Andrey, et al. "ALE: AES-based lightweight authenticated encryption." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2013.

[9] J. Black. Authenticated Encryption. Encyclupedia of Cryptography an security.section A.Springer 2005.

[10] Krawczyk, Hugo. "The order of encryption and authentication for protecting communications (or: How secure is SSL?)." Annual International Cryptology Conference. Springer Berlin Heidelberg, 2001.

[11] Mihir Bellare and Chanathip Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In Tatsuaki Okamoto, editor, ASIACRYPT, volume 1976 of Lecture Notes in Computer Science, pages 531–545. Springer, 2000.

[12] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, http://competitions.cr.yp.to/caesar.html, 20/8/2016.

[13] Javad Alizadeh, Mohammad Reza Aref,Nasour Bagheri. Artemia. 2014

[14] Hossein HOSSEINI, Shahram Khazaei.CBA Mode, A SUBMISSION TO CAESAR COMPETITION FOR AUTHENTICATED ENCRYPTION. 2014

[15] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. The Keccak SHA-3 submission. Submission to NIST (Round 3), 2011.

[16] Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications. In Ali Miri and Serge Vaudenay, editors, Selected Areas in Cryptography, volume 7118 of Lecture Notes in Computer Science, pages 320–337. Springer, 2011.

[17] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In Gilles Brassard, editor, Advances in Cryptology - CRYPTO ’89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings, volume 435 of Lecture Notes in Computer Science, pages 461–480. Springer, 1989.

[18] US Department of Commerce. DES Modes of Operation. Technical Report FIPS PUB 81, US Department of Commerce / National Bureau of Standards, December 1998.

[19] Shai Halevi. EME*: Extending EME to Handle Arbitrary-Length Messages with Associated Data. India, December 20-22, 2004.

[20] Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. iFeed[AES]. http:// competitions;cr;yp;to/caesarsubmissions;html; 2014.

[21] Mohammad Reza Aref Javad Alizadeh and Nasour Bagheri. Jhae: An authenticated encryption mode based on jh. Cryptology

http://competitions:cr:yp:to/caesarsubmissions :html, 2014.

[31] Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, and Shoichi Hirose. Minalpher. http://competitions:cr:yp:to/caesar-submissions:html, 2014.

[32] Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications. In Ali Miri and Serge Vaudenay, editors, Selected Areas in Cryptography, volume 7118 of Lecture Notes in Computer Science, pages 320–337. Springer, 2011.

[33] Mridul Nandi. Forging attacks on two authenticated encryptions cobra and poet. Cryptology ePrint Archive, Report 2014/363, 2014. http://eprint:iacr:org/.

[34] Dobraunig, Eichlseder, Mendel and Schläffer. Calico. Cryptographic Competitions Mailing List, 2014.

[35] Brice Minaud. Forgery attacks on cbeam. Cryptographic Competitions Mailing List, 2014.

[36] Bin Zhang, Chao Xu, and Willi Meier. Another attack on faser128/256. Cryptographic Competitions Mailing List, 2014.

[37] Markku-Juhani Olavi Saarinen. Hkc authentication. Cryptographic Competitions Mailing List, 2014.

[38] Thomas Fuhr, Gaëtan Leurent, and Valentin Suder. Forgery and Key-Recovery Attacks on CAESAR Candidate Marble. January 2015.

[39] Jiqiang Lu. On the security of the copa and marble authenticated encryption algorithms against (almost) universal forgery attack. Cryptology ePrint Archive, Report 2015/079, 2015. http://eprint:iacr:org/.

[40] Samuel Neves. Mcmambo iterative differential. Cryptographic Competitions Mailing List, 2014.

[41] Yu Sasaki and Lei Wang. A practical universal forgery attack against paes-8. Cryptology ePrint Archive, Report 2014/218, 2014. http://eprint:iacr:org/.

[42] Yu Sasaki and Lei Wang. A forgery attack against panda-s. Cryptology ePrint Archive, Report 2014/217, 2014. http;//eprint;iacr;org/.

[43] Fan ZHANG Xiutao FENG and Hui WANG. A practical forgery and state recovery attack on the authenticated cipher panda-s. Cryptology ePrint Archive, Report 2014/325, 2014. http://eprint:iacr:org/.

[44] http;//bench.cr;yp;to/supercop;html, 1/8/2016.

[45] eBACS ,"eBACS:ECRYPT Benchmarking of Cryptographic Systems" , https://bench.cr.yp.to/ebasc.html.2/8/2016

ePrint Archive, Report 2014/193, 2014. http://eprint:iacr:org/.

[22] Alex Biryukov. Design of a New Stream Cipher-LEX. In Matthew J. B. Robshaw and Olivier Billet, editors, New Stream Cipher Designs - The eSTREAM Finalists, volume 4986 of Lecture Notes in Computer Science, pages 48–56. Springer, 2008.

[23] Kazuhiko Minematsu. Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. In Phong Q. Nguyen and Elisabeth Oswald, editors, Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings, volume 8441 of Lecture Notes in Computer Science, pages 275–292. Springer, 2014.

[24] US Department of Commerce. DES Modes of Operation. Technical Report FIPS PUB 81, US Department of Commerce / National Bureau of Standards, December 1998.

[25] Dmitry Khovratovich Alex Biryukov. PAEQ: Parallelizable Permutation-based Authenticated Encryption. In International Security Conference, volume 17, 12-14 October 2014.

[26] Phillip Rogaway and Thomas Shrimpton. A Provable-Security Treatment of the Key-Wrap Problem. In Serge Vaudenay, editor, EUROCRYPT, volume 4004 of Lecture Notes in Computer Science, pages 373–390. Springer, 2006.

[27] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable Block Ciphers. In Moti Yung, editor, CRYPTO, volume 2442 of Lecture Notes in Computer Science, pages 31–46. Springer, 2002.

[28] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings, volume 3329 of Lecture Notes in Computer Science, pages 16–31. Springer, 2004.

[29] Bellare, M., Kilian, J., Rogaway, P.: The Security of the Cipher Block Chaining Message Authentication Code. J. Comput. Syst. Sci. 61(3), 362–399 (2000)

[30] Farzaneh Abed, Scott Fluhrer, John Foley, Christian Forler, Eik List, Stefan Lucks, David McGrew, and Jakob Wenzel. The POET Family of On-Line Authenticated Encryption Schemes.

محسن رضایی متولد ۱۳۶۸، مدرک کارشناسی خود را در شهریور ماه ۱۳۹۱ در رشتهٔ مهندسی تکنولوژی نرم‌افزار در دانشگاه تربیت معلم سبزوار و درجه کارشناسی ارشد را در شهریور ماه ۱۳۹۵ در دانشگاه گیلان و در رشتهٔ مهندسی رایانه گرایش نرم افزار دریافت کرده است. زمینهٔ پژوهشی مورد علاقهٔ ایشان امنیت شبکه، رمزنگاری و شبکه‌های نرم‌افزاری تعریف شده است. در زمینهٔ رمزنگاری تا کنون دو مقاله از ایشان در کنفرانس‌های ملی و بین المللی ارائه شده است.

رضا ابراهیمی آتانی استادیار گروه مهندسی رایانهٔ دانشکدهٔ فنی و مهندسی دانشگاه گیلان است. نامبرده مدرک دکترای خود را در سال ۱۳۸۹ در رشتهٔ مهندسی الکترونیک از دانشگاه علم و صنعت ایران دریافت کرد. ایشان عضو پیوستهٔ انجمن رمز ایران و انجمن‌های بین‌المللی IACR و IEEE هستند. از ایشان تاکنون سه عنوان کتاب و بیش از یکصد مقاله در مجلات و کنفرانس‌های داخلی و بین‌المللی به چاپ رسیده است. زمینهٔ پژوهشی مورد علاقهٔ وی، طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری، امنیت شبکه و امنیت نرم‌افزار است.