یک تحلیل تفاضل ناممکن از الگوریتم رمزقالبی Zorro

هادی سلیمانی*، علیرضا مهرداد، سعیده صادقی و فرخ‌لقا معظمی
پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران، ایران

چکیده

تحلیل تفاضل ناممکن ابزاری قوی به منظور ارزیابی امنیتی رمزهای قالبی است که بر پایه یافتن یک مشخصه تفاضلی با احتمال به‌طوردقیق صفر بنا شده است. سرعت انتشار لایهٔ خطی یک رمز قالبی، نقشی اساسی در امنیت الگوریتم رمز در مقابل تحلیل تفاضل ناممکن دارد و با تغییر لایهٔ خطی، امنیت الگوریتم در مقابل تحلیل تفاضل ناممکن به‌شدت تغییر می‌کند. در این مقاله، روشی کارا و متفاوت برای یافتن مشخصه‌های تفاضلی رمز قالبی سبک‌وزن Zorro ارائه می‌کنیم که مستقل از ویژگی‌های لایهٔ خطی الگوریتم است. به بیان دیگر در این مقاله نشان خواهیم داد که مستقل از ویژگی‌های عناصر الگوریتم، می‌توان برای نُه دور از الگوریتم Zorro مشخصه تفاضل ناممکن کارایی به‌دست آورد؛ همچنین برپایه این مشخصه نُه‌دوری، یک حمله بازیابی کلید برای ده دور الگوریتم Zorro ارائه می‌کنیم.

واژگان کلیدی: رمز قالبی، تحلیل رمز، تحلیل تفاضل ناممکن، الگوریتم رمز قالبی Zorro

Novel Impossible Differential Cryptanalysis of Zorro Block Cipher

Hadi Soleimany*, Alireza Mehrdad, Saeideh Sadeghi & Farokhlagha Moazemi
Cyberspace Research Institute Department, Shahid Beheshti University, Tehran, Iran

Abstract

Impossible difference attack is a powerful tool for evaluating the security of block ciphers based on finding a differential characteristic with the probability of exactly zero. The linear layer diffusion rate of a cipher plays a fundamental role in the security of the algorithm against the impossible difference attack. In this paper, we show an efficient method, which is independent of the quality of the linear layer, can find impossible differential characteristics of Zorro block cipher. In other words, using the proposed method, we show that, independent of the linear layer feature and other internal elements of the algorithm, it is possible to achieve effective impossible differential characteristic for the 9-round Zorro algorithm. Also, based on represented 9-round impossible differential characteristic, we provide a key recovery attack on reduced 10-round Zorro algorithm. In this paper, we propose a robust and different method to find impossible difference characteristics for Zorro cipher, which is independent of the linear layer of the algorithm. The main observation in this method is that the number of possible differences in that which may occur in the middle of Zorro algorithm might be very limited. This is due to the different structure of Zorro. We show how this attribute can be used to construct impossible difference characteristics. Then, using the described method, we show that, independent of the features of the algorithm elements, it is possible to achieve efficient 9-round impossible differential characteristics of Zorro cipher. It is important to note that the best impossible differential characteristics of the AES encryption algorithm are only practicable for four rounds. So the best impossible differential characteristic of Zorro cipher is far more than the best characteristic of AES, while both algorithms use an equal linear layer. Also, the analysis presented in the article, in contrast to previous

* Corresponding author

*نویسندهٔ عهده‌دار مکاتبات

● تاریخ ارسال: ۹۶/۱۲/۰۸ ● تاریخ پذیرش: ۹۸/۰۳/۲۹ ● تاریخ انتشار: ۲۸ ۹۸/۱۲

[DOI: 10.29252/jsdp.16.4.17]

analyzes, can be applied to all ciphers with the same structure as Zorro, because our analysis is independent of the internal components of the algorithm. In particular, the method presented in this paper shows that for all Zorro modified versions, there are similarly impossible differential characteristics. Zorro cipher is a block cipher algorithm with 128-bit block size and 128-bit key size. Zorro consists of 6 different sections, each with 4 rounds (24 rounds in all). Zorro does not have any subkey production algorithm and the main key is simply added to the value of the beginning state of each section using the XOR operator. Internal rounds of one section do not use the key. Similar to AES, Zorro state matrix can be shown by a 4 × 4 matrix, which each of these 16 components represent one byte. One round of Zorro, consists of four functions, which are SB*, AC, SR, and MC, respectively. The SB* function is a nonlinear function applying only to the four bytes in the first row of the state matrix. Therefore, in the opposite of the AES, where the substitution box is applied to all bytes, the Zorro substitution box only applies to four bytes. The AC operator is to add a round constant. Finally, the two SR and MC transforms are applied to the state matrix, which is, respectively, the shift row and mixed column used in the AES standard algorithm. Since the analyzes presented in this article are independent of the substitution properties, we do not use the S-box definition used by Zorro. Our proposed model uses this Zorro property that the number of possible differences after limited rounds can be much less than the total number of possible differences. In this paper, we introduce features of the Zorro, which can provide a high bound for the number of possible values of an intermediate difference. We will then present a model for how to find Zorro impossible differential characteristics, based on the limitations of the intermediate differences and using the miss-in-the-middle attack. Finally, we show that based on the proposed method, it is possible to find an impossible differential characteristic for 9 rounds of algorithms with a Zorro-like structure and regardless of the linear layer properties. Also, it is possible to apply the key recovery attack on 10 rounds of the algorithm. So, regardless of the features of the used elements, it can be shown that this number of round of algorithms is not secure even by changing the linear layer.

Keywords: block cipher, cryptanalysis, impossible difference attack, Zorro block cipher algorithm

۱- مقدمه

یکی از چالش‌های جدی در به‌کارگیری اولیه‌های سبک‌وزن، نحوه پیاده‌سازی امن این اولیه‌ها در مقابل حملات کانال جانبی است. پیاده‌سازی ناامن یک طرح رمزنگاری که به‌لحاظ ریاضیاتی، امن است، ممکن است سبب ایجاد ضعف در مقابل حملات کانال جانبی شده و به‌صورت عملی شکسته می‌شود (به‌عنوان نمونه به [1] و مراجع یادشده در کتاب مراجعه شود). در پاسخ به این چالش، طیف وسیعی از پژوهش‌گران بر روی پیاده‌سازی امن الگوریتم‌های رمزنگاری کار کرده و روش‌های متعدد فراوانی برای مقابله با حملات کانال جانبی پیشنهاد داده‌اند؛ اما این روش‌ها سبب افزایش قابل توجه ابعاد پیاده‌سازی الگوریتم رمزنگاری می‌شود که در حوزه کاربردهای رمزنگاری سبک‌وزن بسیار چالش برانگیز است. طراحی یک رمز قالبی با درنظرگرفتن حملات کانال جانبی برای نخستین‌بار توسط Gerard و همکاران در CHES 2013 مورد بررسی قرار گرفت. نویسندگان مقاله این مسأله را بررسی کردند که چگونه می‌توان الگوریتم رمزنگاری استاندارد AES را به‌نحوی بازتعریف کرد که اعمال روش‌های نقاب‌گذاری به آن، کمینه سربار اضافه را داشته باشد. آنها با کاهش تعداد جعبه‌های جانشینی در هر دور و همچنین تغییر جعبه جانشینی به‌کاررفته، الگوریتم جدیدی را به نام Zorro معرفی کردند. هدف از این مقاله بررسی امنیت ساختار Zorro در مقابل تحلیل تفاضل ناممکن است.

۱-۱- کارهای پیشین

تحلیل الگوریتم‌های رمزنگاری به‌منظور فهم امنیت آنها بسیار اهمیت دارد. بدین منظور الگوریتم‌های رمزنگاری بسیاری پس از ارائه، توسط جامعه رمزنگاری در مقابل تحلیل‌های آماری مورد مطالعه قرار گرفته‌اند [2]. الگوریتم رمزنگاری Zorro به‌خاطر ساختار نوین آن به‌صورت گسترده مورد توجه جامعه رمزنگاری قرار گرفته است. در [3] نشان داده شده که شانزده دور الگوریتم با پیچیدگی سریع‌تر از جست‌وجوی کامل شکسته می‌شود. در [4] نشان داده شد که تعداد 2^{64} از 2^{128} کلید ممکن، کلیدهای ضعیف هستند؛ بدین معنی که درصورت استفاده از آنها سامانه رمزنگاری سریع‌تر از جست‌وجوی جامع شکسته می‌شوند. به‌طور مشابه در [7] دسته دیگری از کلیدهای ضعیف ارائه شد. مقالات [3]، [4] و [7] از ضعف مقادیر ثابت دور به‌کاررفته در الگوریتم بهره می‌برند. در مقالات [5] و [6] نویسندگان نشان دادند که تمام دور Zorro در مقابل حمله تفاضلی و خطی امن نبوده و با پیچیدگی بسیار کمتر از جست و جوی جامع می‌توان به تمام دور الگوریتم حمله کرد. این دسته از مقالات نیز از ضعف لایه خطی الگوریتم استفاده می‌کنند. برهمین اساس در مقاله [8] این مسأله بررسی شد که چگونه می‌توان با تغییر لایه خطی، امنیت ساختار الگوریتم Zorro را بهبود بخشید.

[DOI: 10.29252/jsdp.16.4.17]

(جدول-۱): حملات پیشین بر روی الگوریتم Zoror
(Table-1): Previous attacks on Zorro

مرجع	داده	زمان	تعداد دور	مدل	نوع حمله
[3]	2^{54} CP	$2^{54.3}$	تمام دور	کلید ضعیف	تفاضلی
[4]	$2^{123.6}$ KP	$2^{123.8}$	۱۶	تک کلید	حمله لغزشی
[5]	$2^{105.3}$ KP	$2^{105.3}$	تمام دور	تک کلید	خطی
[5]	$2^{112.4}$CP	2^{108}	تمام دور	تک کلید	تفاضلی
[6]	$2^{56.7}$KP	$2^{56.8}$	تمام دور	تک کلید	خطی
[6]	$2^{45.4}$CP	$2^{45.5}$	تمام دور	تک کلید	تفاضلی
[8]	2^{45}KP	2^{45}	تمام دور	تک کلید	خطی
[8]	$2^{44.4}$CP	$2^{45.5}$	تمام دور	تک کلید	تفاضلی
این مقاله	$2^{91.5}$CP	$2^{120.2}$	۱۰	تک کلید (مستقل از لایه خطی)	تفاضل ناممکن

CP: متن منتخب، KP: متن معلوم

۲-۱- نوآوری مقاله

در این مقاله، روشی کارا و متفاوت برای یافتن مشخصه‌های تفاضل ناممکن رمز قالبی Zorro ارائه می‌کنیم که مستقل از ویژگی‌های لایه خطی الگوریتم است. مشاهده اصلی در این روش این است که تعداد تفاضل‌های ممکن که در حالت میانی الگوریتم Zorro ممکن است اتفاق بیافتد، بسیار محدود است. دلیل این امر نیز به ساختار متفاوت Zorro باز می‌گردد. ما نشان می‌دهیم که این ویژگی چگونه می‌تواند برای ساخت مشخصه‌های تفاضل ناممکن به‌کار آید؛ سپس با استفاده از روش توصیف‌شده، نشان می‌دهیم که مستقل از ویژگی‌های عناصر الگوریتم، می‌توان برای نُه دور از الگوریتم Zorro مشخصات تفاضل ناممکن کارایی به‌دست آورد. توجه به این نکته ضروری است که بهترین مشخصه تفاضل ناممکن الگوریتم رمزنگاری AES تنها چهار دور دارد؛ بنابراین بهترین مشخصه تفاضل ناممکن Zorro به‌مراتب بیشتر از بهترین مشخصه تفاضل ناممکن AES است و این درحالی است که هر دو الگوریتم از یک لایه خطی استفاده می‌کنند. همچنین تحلیل ارائه‌شده در مقاله خلاف تحلیل‌های گذشته [3-7]، قابل اعمال به تمامی رمزهای با ساختار مشابه Zorro است چرا که مستقل از مشخصات اجزای داخلی الگوریتم است. به‌طور ویژه روش ارائه‌شده در این مقاله نشان می‌دهد که برای تمامی طرح‌های اصلاح‌شده Zorro که در EUROCRYPT 2015 ارائه شده است [8]، مشخصات تفاضل ناممکن مشابهی وجود دارد. نتایج این مقاله و حملات پیشین در جدول (۱) نشان داده شده‌اند.

۳-۱- ساختار مقاله

در این مقاله ابتدا در بخش ۲ الگوریتم رمز قالبی Zorro به‌اختصار توضیح داده می‌شود. پس از آن در بخش ۳ تحلیل تفاضل ناممکن که یکی از کارآمدترین حملات روی رمزهای قالبی است، به‌همراه روش‌های یافتن مشخصات تفاضل‌های ناممکن تشریح می‌شود. در بخش ۴ چارچوبی به‌منظور پیداکردن مشخصه‌های تفاضل ناممکن در Zorro ارائه می‌شود. به عبارت دقیق‌تر در بخش ۴ نشان می‌دهیم که چرا برخلاف آنکه سرعت انتشار در الگوریتم رمز قالبی Zorro مناسب است، مقادیر ممکن برای تفاضل‌های میانی بسیار محدود است؛ سپس مدلی را ارائه می‌دهیم که چگونه می‌توان از این خاصیت به‌منظور کشف مشخصات تفاضل ناممکن بهره برد. در بخش ۵ روش به‌دست‌آوردن مشخصه‌های تفاضل ناممکن برای نُه دور Zorro را با استفاده از مدل ارائه‌شده در بخش ۴ شرح می‌دهیم. در بخش ۶ نشان می‌دهیم که با استفاده از مشخصه تفاضل ناممکن نُه‌دوری ارائه‌شده می‌توان به ده دور الگوریتم یک حمله بازیابی کلید اعمال کرد. درنهایت در بخش ۷ جمع‌بندی خود را ارائه می‌کنیم.

۲- الگوریتم رمز قالبی Zorro

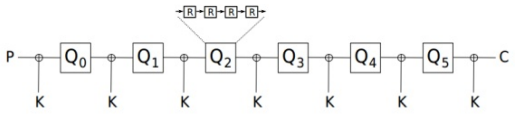
الگوریتم رمزنگاری Zorro یک الگوریتم رمز قالبی با طول قالب و کلید ۱۲۸ بیت است. Zorro از ۶ بخش مشابه تشکیل شده است که هر بخش دارای ۴ دور می‌باشد (در مجموع ۲۴ دور دارد). Zorro دارای الگوریتم تولید زیرکلید نیست. کلید اصلی به‌صورت ساده در ابتدای هر بخش به مقدار حالت[1] با استفاده از عملگر Xor اضافه می‌شود. دورهای درون یک بخش از کلید استفاده نمی‌کنند. مقادیر حالت Zorro را می‌توان همانند AES به‌صورت یک ماتریس 4×4 نشان داد که هر مؤلفه ماتریس نشان‌دهندهٔ یک بایت است. یک دور شامل چهار تابع است که به‌ترتیب عبارتند از: *SB، AC، SR و MC. تابع *SB یک تابع غیرخطی است که شامل اعمال یک جعبه

[1] State

[DOI: 10.29252/jsdp.16.4.17]

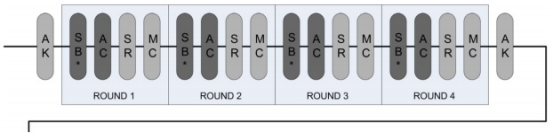
جانشینی یکسان به چهار بایت موجود در نخستین سطر ماتریس حالت است. بنابراین برعکس AES که جعبه جانشینی به تمامی بایت‌ها اعمال می‌شود، در Zorro جعبه جانشینی تنها به چهار بایت اعمال می‌شود. عملگر AC، عبارت است از اضافه‌کردن ثابت دور. ثابت دور در دور i-ام، به‌صورت چهار بایت (i, i, i, i << 3) تعریف شده و به صورت xor به چهار بایت سطر نخست اضافه می‌شود. سرانجام، دو تبدیل SR و MC به ماتریس حالت اعمال می‌شوند که به‌ترتیب عبارت‌اند از تغییر سطری و مخلوط‌ساز ستونی که در الگوریتم استاندارد AES به‌کار رفته‌اند [9].

از آنجایی‌که تحلیل‌های ارائه‌شده در این مقاله مستقل از خواص جانشینی است، از تعریف S-box استفاده‌شده در Zorro خودداری کرده و علاقمندان را به [10] ارجاع می‌دهیم. ساختار Zorro در شکل (۱) و شکل (۲) قابل مشاهده است.



(شکل-۱): ساختار الگوریتم Zorro
(Figure-1): Zorro cipher structure

الگوریتم رمز از ۶ بخش (که با $\mathbf{Q_0} \dots \mathbf{Q_5}$ نمایش داده شده است) که هر کدام شامل چهار دور هستند، استفاده می‌کند. دورها تنها در ثابت‌هایی که به قالب اضافه می‌شود، تفاوت دارند.



(شکل-۲): الگوریتم رمزنگاری Zorro
(Figure-2): Zorro cipher algorithm

بلوک‌های خاکستری کم‌رنگ بیان‌گر بلوک‌هایی همانند AES و بلوک‌های خاکستری پررنگ دارای طراحی جدید هستند.

با توجه به ساختار الگوریتم Zorro، کلید در انتهای دور آخر نیز به آن اضافه شود. همان‌طورکه در [11] توضیح داده شده است، به دلیل خطی‌بودن دو تبدیل مخلوط‌ساز ستونی و جمع با کلید، می‌توانیم این دو تبدیل را با یکدیگر جابه‌جا کنیم با این تفاوت که درعمل جمع با کلید، به‌جای استفاده از کلید $\boldsymbol{k}$ باید از زیر کلید معادل آن یعنی $\mathbf{w} = \mathbf{MC^{-1}(k)}$ استفاده کنیم، زیرا داریم:

$$\mathbf{MC(x) \oplus k = MC(x) \oplus MC\left(MC^{-1}(k)\right) = MC(x \oplus MC^{-1}(k))}$$

همان‌طور که در بخش ۶ خواهیم دید، این امر سبب می‌شود که حمله بازیابی کلید با پیچیدگی کمتری انجام شود.

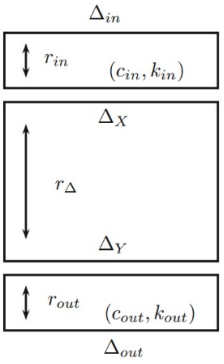
۳- تحلیل تفاضل ناممکن

۳-۱- ساختار کلی حملات تفاضل ناممکن

تحلیل تفاضل ناممکن به‌طور مستقل توسط نادسن[1] و بیهام[2] و همکارانش به‌ترتیب در [12] و [13] معرفی شده‌اند. خلاف تحلیل تفاضلی که بر اساس استفاده از مشخصه‌های تفاضلی با احتمال بالا است، تحلیل تفاضل ناممکن از تفاضل‌هایی استفاده می‌کند که با احتمال صفر رخ می‌دهند. تحلیل تفاضل ناممکن اغلب از دو بخش کلی تشکیل می‌شود. نخستین بخش، یافتن یک مشخصه تفاضل ناممکن با طول بیشینه‌ای است، که تفاضل ورودی آن $\boldsymbol{\Delta_X}$ و تفاضل خروجی $\boldsymbol{\Delta_Y}$ باشد. به عبارت دقیق‌تر هدف، یافتن یک مشخصه تفاضلی است، به‌طوری‌که احتمال آنکه تفاضل ورودی $\boldsymbol{\Delta_X}$ بعد از $\mathbf{r_\Delta}$ دور، به تفاضل خروجی $\boldsymbol{\Delta_Y}$ منجر شود، صفر باشد. به‌عبارت دیگر $\mathbf{Pr}\left[\Delta_X \xrightarrow{r_\Delta} \Delta_Y\right] = \mathbf{0}$. بخش دوم حمله، استفاده از مشخصه تفاضل ناممکن به‌منظور بازیابی (بخشی از) زیرکلیدهای دور است که مرحله فیلترکردن کلید نیز نامیده می‌شود. در حالت کلی، الگوریتم رمزنگاری $\mathbf{r_{in} + r_{out} + r_\Delta}$ دوری را در نظر می‌گیریم (با اضافه‌کردن $\mathbf{r_{in}}$ دور به ابتدا و $\mathbf{r_{out}}$ دور به انتهای مشخصه تفاضل ناممکن) [16]. سپس تعدادی زوج متن اصلی و متن‌های رمزشده معادل آنها در نظر گرفته می‌شوند؛ پس از آن زیرکلیدهای دورهای ابتدائی و انتهائی حدس زده می‌شود و زوج متن‌های اصلی داده شده برای $\mathbf{r_{in}}$ دور نخست رمزنگاری و زوج متن‌های رمزشده معادل آنها برای $\mathbf{r_{out}}$ دور آخر رمزگشائی می‌شوند. اگر به‌ازای یک کلید حدس زده شده، یکی از زوج متن‌ها به تفاضل $\boldsymbol{\Delta_x}$ در دور $\mathbf{r_{in}}$ام و تفاضل $\boldsymbol{\Delta_y}$ در انتهای دور $(\mathbf{r_{in} + r_\Delta})$ام منجر شود، می‌توان نتیجه گرفت که کلید حدس‌زده‌شده غلط است و باید آن را از فضای نامزدهای احتمالی کلید حذف کرد. ساختار حمله تفاضلی ناممکن در شکل (۳) ارائه شده است.

[1] Knudsen
[2] Biham

[DOI: 10.29252/jsdp.16.4.17]

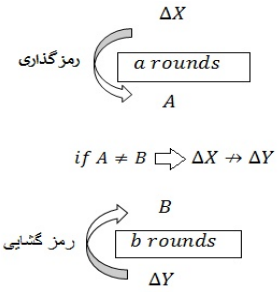


(شکل-۳): ساختار حمله تفاضلی ناممکن

(Figure-3): Structure of impossible differential attack

۲-۳- یافتن مشخصه تفاضل ناممکن

یافتن تفاضل غیرممکن، به‌طورمعمول به روش فقدان در میانه[1] انجام می‌شود. در این روش اگر $\mathbf{r_\Delta}$ توضیح‌داده‌شده در بخش ۳-۱ را به‌صورت جمع $r_\Delta = (a + b)$ نشان دهیم، ابتدا یک مشخصه تفاضلی همچون $\Delta X \xrightarrow{\text{دور } a} A$ برای $\mathbf{a}$ دور از الگوریتم با احتمال یک در جهت رمزگذاری پیدا می‌کنیم؛ سپس به‌صورت مشابه یک مشخصه تفاضلی همچون $B \xleftarrow{\text{دور } b} \Delta Y$ برای b دور از الگوریتم با احتمال یک در جهت رمزگشایی پیدا می‌کنیم. اگر بتوان نشان داد که تفاضل‌های A و B هیچگاه نمی‌توانند با هم برابر باشند، می‌توان نتیجه گرفت که مشخصه تفاضلی $r_\Delta = (a + b)$ دوری $\Delta X \xrightarrow{\text{دور } r_\Delta} \Delta Y$، یک تفاضل غیرممکن خواهد بود (شکل (۴)).



(شکل-۴): روش فقدان در میانه برای یافتن مشخصه تفاضل ناممکن

(Figure-4): using miss-in-the-middle for finding impossible differential characteristic

دسته گسترده‌ای از مشخصه‌های تفاضل ناممکن که با استفاده از روش فقدان در میانه به‌دست می‌آیند، از این ویژگی استفاده می‌کنند که در صورت انتخاب هوشمندانه تفاضل‌های ورودی و خروجی یک مشخصه تفاضلی، برخی بیت‌های تفاضل در حالت میانی الگوریتم با احتمال یک برابر تفاضل صفر می‌شوند. برهمین اساس اگر لایه خطی به گونه‌ای طراحی شود که تغییر هر کدام از بیت‌های ورودی منجر به تاثیرپذیری تمامی بیت‌های حالت میانی پس از $\mathbf{r}$ دور شود. در این حالت اصطلاحا می‌گویند که الگوریتم پس از $\mathbf{r}$ دور به انتشار کامل می‌رسد که در این حالت می‌توان به صورت تقریبی انتظار داشت که طول بهترین مشخصه تفاضلی ممکن حدود $\mathbf{2r}$ دور است. به‌عنوان مثال الگوریتم رمزنگاری استاندارد AES پس از دو دور به انتشار کامل می‌رسد و بهترین مشخصه تفاضل ناممکن ارائه شده برای AES چهاردوری است.

ما در بخش بعد نشان می‌دهیم که چگونه می‌توان از روش فقدان در میانه به صورتی متفاوت استفاده کرد تا بر محدودیت ذکر شده غلبه کنیم. یعنی بتوان علی‌رغم سرعت انتشار مناسب Zorro (که همانند AES دو دور است)، مشخصه تفاضل ناممکنی به مراتب طولانی‌تر برای الگوریتم Zorro پیدا کنیم.

۴- چارچوبی به‌منظور پیداکردن مشخصه‌های تفاضل ناممکن در Zorro

مدل پیشنهادی ما از این ویژگی Zorro استفاده می‌کند که تعداد تفاضل‌های ممکن بعد از تعداد محدودی دور می‌تواند بسیار کمتر از تعداد کل مقادیر ممکن باشد. در این بخش ابتدا ویژگی‌هائی از الگوریتم Zorro را ارائه می‌کنیم که براساس آن بتوان کران بالائی برای تعداد مقادیر ممکن برای یک تفاضل میانی ارائه کرد؛ سپس مدلی را ارائه می‌کنیم که چگونه می‌توان براساس محدودیت مقادیر تفاضل‌های میانی و با استفاده از روش فقدان در میانه، مشخصه‌های تفاضل ناممکن مؤثری برای Zorro پیدا کرد.

۱-۴- برخی ویژگی‌های الگوریتم Zorro

برای آنکه بتوانیم تعداد مقادیر ممکن برای تفاضل حالت میانی الگوریتم رمز قالبی Zorro را بشماریم، ابتدا چند ویژگی این الگوریتم را مطرح و اثبات می‌کنیم. این ویژگی‌ها نشان می‌دهند که چگونه می‌توان با انتخاب هوشمندانه مقادیر تفاضل‌های ورودی (یا خروجی) نشان داد که مقادیر ممکن برای یک تفاضل در میانه الگوریتم محدود بوده و بسیار کوچک‌تر از تعداد کل حالات ممکن (یعنی 2^{128}) است.

[1] Miss-in-the-middle

[DOI: 10.29252/jsdp.16.4.17]

قضیه ۱. در یک جعبه جانشینی $\mathbf{n}$ بیتی یک‌به‌یک، هر تفاضل ورودی غیرصفر مانند $\Delta_{in} \in \mathbb{F}_2^n$، می‌تواند حداکثر به 2^{n-1} مقدار متفاوت در تفاضل خروجی تبدیل شود. به‌عبارت دیگر داریم:

$$\left|\{\Delta_{out} \in \mathbb{F}_2^n : \exists\, x\ \Delta_{out} = S(x) \oplus S(x \oplus \Delta_{in})\}\right| \leq 2^{n-1} \qquad (۲)$$

اثبات: اثبات این قضیه از این حقیقت سرچشمه می‌گیرد که مقادیر $S(x) \oplus S(x \oplus \Delta_{in})$ و $S(x \oplus \Delta_{in}) \oplus S(x)$ به‌دلیل تقارن برابر هستند؛ درنتیجه تعداد دفعاتی که به‌ازای یک تفاضل خاص Δ_{in} در ورودی، یک مقدار در تفاضل خروجی می‌تواند رخ دهد زوج است. گفتنی است که این قضیه پیش از این به‌منظور بهبود حملات ملاقات در میانه بر روی AES استفاده شده است [14].

براساس قضیه ۱، هر تفاضل ورودی غیرصفر مانند $\Delta_{in} \in \mathbb{F}_2^8$، می‌تواند، حداکثر به 2^7 مقدار متفاوت در تفاضل خروجی جعبه جانشینی Zorro تبدیل شود.

طبق قضیه ۱ می‌توان این‌گونه بیان کرد که برای تفاضل ثابت $?_1$ در ورودی، حداکثر 2^7 مقدار متفاوت تفاضل $?_2$ در خروجی وجود دارد به‌نحوی که $? \rightarrow ?$ را برآورده سازد.

قضیه ۲. در یک جعبه جانشینی $\mathbf{n}$ بیتی یک‌به‌یک، اگر تفاضل ورودی غیرصفر و غیر مشخص (متغییر)، می‌تواند حداکثر به $2^n - 1$ مقدار متفاوت در تفاضل خروجی تبدیل شود.

اثبات: اگر ورودی فعال باشد، خروجی نیز فعال خواهد بود و یک خروجی n-بیتی فعال، حداکثر $2^n - 1$ حالت مختلف دارد.

طبق قضیه ۲ می‌توان این‌گونه بیان کرد که برای تفاضل $?_1$ در ورودی، حداکثر 2^8 مقدار متفاوت تفاضل $?_2$ در خروجی وجود دارد به نحوی که $?_2 \rightarrow ?_1$ را برآورده سازد.

بنابراین براساس آنچه که در این بخش دیدیم، زمانی که تعداد جعبه‌های فعال به‌اندازهٔ کافی کم باشند، مانند آنچه در الگوریتم Zorro وجود دارد، تعداد تفاضل‌های ممکن بعد از تعداد محدودی دور، بسیار کمتر از تعداد کل تفاضل‌های ممکن خواهد بود. در بخش بعد، مدلی را به‌منظور ساختن مشخصه‌های تفاضل ناممکن در Zorro ارائه می‌کنیم.

۲-۴- یافتن مشخصه‌های تفاضل ناممکن با استفاده از محدودیت مقادیر ممکن برای تفاضل میانی

هدف ما در این بخش بازتعریف روش فقدان در میانه به گونه‌ای است که بتوان از خواص یادشده در بخش ۴-۱ به‌منظور ساخت مشخصه‌های تفاضل ناممکن استفاده کرد. بدین منظور $\mathbf{r_1} + \mathbf{r_2}$ دور از یک الگوریتم رمز قالبی $\mathbf{n}$ بیتی را در نظر می‌گیریم. در این روش ابتدا برای یک مقدار تفاضل ورودی، تمام مقادیر ممکن برای تفاضل خروجی بعد از $\mathbf{r_1}$ دور رمزگذاری را پیدا کرده و آنها را در مجموعه‌ای نظیر $\mathbf{D_1}$ ذخیره می‌کنیم. به‌طور مشابه، برای یک مقدار تفاضل خروجی، تمام مقادیر ممکن برای تفاضل خروجی در $\mathbf{r_1}$ ام را با انجام عمل رمزگشائی برای $\mathbf{r_2}$ دور آخر الگوریتم پیدا کرده و آنها را در مجموعه‌ای نظیر $\mathbf{D_2}$ ذخیره می‌کنیم. درصورتی‌که دو مجموعه $\mathbf{D_1}$ و $\mathbf{D_2}$ هیچ اشتراکی با یکدیگر نداشته باشند، می‌توان نتیجه گرفت که تفاضل ورودی مورد نظر هیچگاه نمی‌تواند به تفاضل خروجی یادشده منجر شود.

احتمال عدم اشتراک دو زیرمجموعه از مجموعه‌های $\mathbf{D_1}$ و $\mathbf{D_2}$ برابر است با $\frac{\binom{N-d_1}{d_2}}{\binom{N}{d_2}}$ و لذا احتمال اشتراک برابر با $1 - \frac{\binom{N-d_1}{d_2}}{\binom{N}{d_2}}$ خواهد بود. درنتیجه کارایی این روش به اندازه دو مجموعه $\mathbf{D_1}$ و $\mathbf{D_2}$ بستگی دارد. یعنی هرچقدر اندازه دو مجموعه $\mathbf{D_1}$ و $\mathbf{D_2}$ کوچک‌تر باشند، احتمالِ یافتن یک مشخصه تفاضل ناممکن بیشتر است. به عبارت دیگر کارایی این روش به این بستگی دارد که تعداد مقادیر ممکن برای تفاضل میانی در نظر گرفته‌شده، محدود باشد. در این صورت با احتمال بالایی می‌توان انتظار داشت که پس از تشکیل دو مجموعه $\mathbf{D_1}$ و $\mathbf{D_2}$، اشتراکی بین دو مجموعه وجود نداشته باشد.

در بخش بعد نشان می‌دهیم که چگونه براساس این مدل می‌توان مشخصه‌های تفاضل ناممکن متعددی برای Zorro پیدا کرد.

۵- مشخصه تفاضل ناممکن نُه‌دوری Zorro

روند یافتن مشخصه تفاضل ناممکن نُه‌دوری در شکل (۵) قابل مشاهده است این عملیات را می‌توان همانند [15] به‌صورت گام‌های زیر بیان کرد:

۱- طبق شکل (۵)، تعداد حالت‌هایی که برای تفاضل ورودی در نظر گرفتیم می‌تواند 2^{96} تفاضل ممکن را اخذ کند. در انتهای دور نخست و مستقل از لایه خطی استفاده‌شده در رمز قالبی Zorro، به‌طور متوسط $2^{96-8\times4} = 2^{64}$ جفت با مشخصه تفاضلی مشخص‌شده خواهیم داشت و به همین صورت در انتهای دور دوم، به‌طور متوسط $= 2^{64-8\times4}$

[DOI: 10.29252/jsdp.16.4.17]

2^{32} جفت با مشخصه تفاضلی مشخص‌شده خواهیم داشت. همان‌طورکه توضیح داده شد، دلیل این امر این است که احتمال آنکه مقدار تفاضل خروجی MC (با در نظر گرفتن محدودیت عدد انشعاب) در یک بایت خاص برابر 0 باشد به‌طور متوسط برابر 2^{-8} است. بنابراین انتظار داریم که $2^{96-8\times8} = 2^{32}$ تفاضل در انتهای دور سوم داشته باشیم که مشخصه تفاضلی معادل آنها تا انتهای دور دوم، با احتمال یک صادق است.

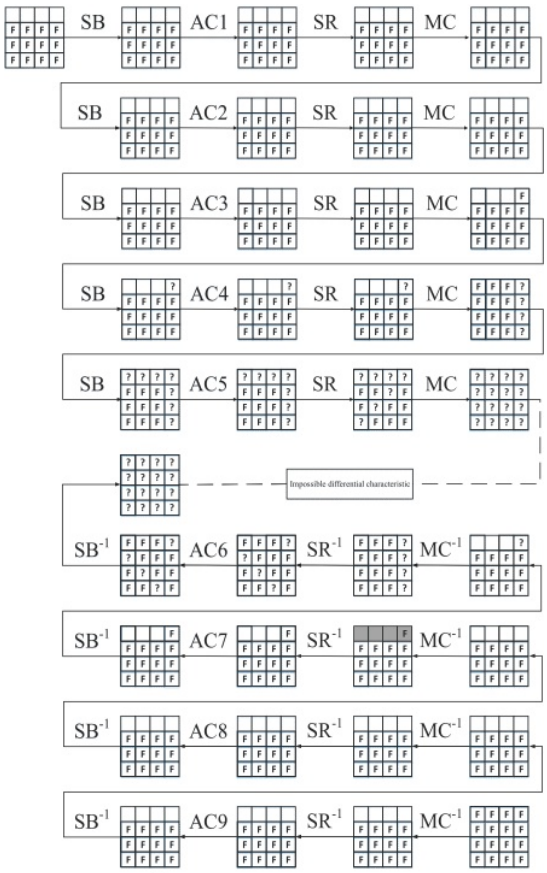
۲- در انتهای دور سوم، با توجه به این‌که به سه بایت با تفاضل صفر نیاز داریم، می‌توان انتظار داشت که تعداد $2^{32-8\times3} = 2^{8}$ جفت، باقی بماند.

۳- از کل 2^{8} جفت باقی‌مانده از مراحل بالا، فقط یک جفت را در نظر می‌گیریم و نام آن را $\boldsymbol{\delta_{in}}$ می‌گذاریم. بنابراین $\boldsymbol{\delta_{in}}$ پس از سه دور می‌تواند تنها به یک مقدار تفاضلی منتقل شود و همچنین این خاصیت را دارد که در انتهای دور سوم (و بالطبع در ابتدای دور چهارم) تنها یک بایت فعال در سطر نخست آن وجود دارد. بنابر قضیه ۱ این تفاضل F می‌تواند به بیشینه 2^{7} حالت ممکن ? در ابتدای دور چهارم تبدیل شود. با توجه به خطی‌بودن MC، می‌دانیم که در انتهای دور چهارم هم 2^{7} حالت مختلف خواهیم داشت.

۴- بنابر قضایای ۱ و ۲، هرکدام از این 2^{7} حالت ممکن می‌توانند پس از عبور از SB دور پنجم به حداکثر $(2^{7})^{3} \times 2^{8} = 2^{29}$ حالت مختلف در انتهای دور پنجم منتقل شوند (سه تفاضل ثابت F و یک بایت فعال ? داریم). بنابراین درصورتی‌که تفاضل ورودی $\boldsymbol{\delta_{in}}$ باشد، تفاضل در انتهای دور پنجم می‌تواند حداکثر $2^{29} \times 2^{7} = 2^{36}$ مقدار مختلف داشته باشد. در اینجا به این نکته توجه می‌کنیم که این مقدار به مراتب کوچک‌تر از تعداد کل حالات ممکن (یعنی 2^{128}) است. ما تمامی تفاضل‌های ممکن حاصل از رمزنگاری پنج دوری به‌ازای تفاضل ورودی $\boldsymbol{\delta_{in}}$ را محاسبه و در مجموعه $\mathbf{D_1}$ ذخیره می‌کنیم.

۵- حال در مسیر رو به عقب، تمامی 2^{128} تفاضل ممکن در انتهای دور نهم الگوریتم را در نظر می‌گیریم. انتظار داریم که تعداد $2^{128-8\times4} = 2^{96}$ مشخصه تفاضلی، با احتمال یک در ابتدای دور نهم الگوریتم داشته باشیم. به همین روش، در ابتدای دور هشتم $2^{96-8\times4} = 2^{64}$ جفت داریم.

۶- در قسمت میانی دور هفتم (قبل از عملگر MC) که با هاشور در شکل (۵) مشخص شده است، نیاز داریم که فقط یکی از بایت‌های سطر نخست غیرفعال باشند، اما مکان این بایت فعال برایمان اهمیت ندارد؛ ازاین‌رو در قسمت میانی دور هفتم که سطر نخست آن با هاشور در شکل (۵) مشخص شده است، می‌توان انتظار داشت که تعداد $2^{64-8\times3} \times \binom{4}{1} = 2^{42}$ جفت، باقی بماند. هر یک از 2^{42} مقادیر تفاضلی را با $\boldsymbol{\delta_{out}^{i}}$ نشان می‌دهیم که $1 \le i \le 2^{42}$.



(شکل-۵): مشخصه تفاضل ناممکن نُه‌دوری

(Figure-5): 9-round impossible differential characteristic

۷- با توجه به این که فقط یک جعبه جانشینی فعال در ابتدای دور هفتم داریم، با توجه به قضیه ۱، $2^{42} \times 2^{7} = 2^{49}$ حالت ممکن در انتهای دور ششم خواهیم داشت.

۸- بنابر قضایای ۱و ۲، هر یک از 2^{49} حالت ممکن در انتهای دور ششم می‌توانند به $2^{3\times7} \times 2^{8} = 2^{29}$ مقدار تفاضل، در انتهای دور پنجم تبدیل شوند؛ بنابراین با فرض این‌که مقدار تفاضل خروجی در دور نهم یکی از مقادیر $\boldsymbol{\delta_{out}^{i}}$ است، کل تعداد مقادیر ممکن برای مقدار تفاضل خروجی در انتهای دور پنجم برابر است با $2^{49} \times 2^{29} = 2^{78}$ مقدار. این مقادیر را محاسبه کرده و در یک مجموعه مانند $\boldsymbol{D_2}$ ذخیره می‌کنیم.

اگر مجموعه‌های $\boldsymbol{D_1}$ و $\boldsymbol{D_2}$ دارای هیچ اشتراکی نباشند در واقع یک مشخصه تفاضل ناممکن به‌دست آورده‌ایم. احتمال

[DOI: 10.29252/jsdp.16.4.17]

اینکه دو مجموعه D_1 و D_2 با یک دیگر اشتراک نداشته باشند براساس آنچه در بخش ۴-۲ توضیح داده شد برابر است با $\frac{\binom{N-d_1}{d_2}}{\binom{N}{d_2}} = \frac{\binom{2^{128}-2^{78}}{2^{36}}}{\binom{2^{128}}{2^{36}}} = \frac{(2^{128}-2^{78})!\times(2^{128}-2^{36})!}{(2^{128})!\times(2^{128}-2^{78}-2^{36})!} \approx 1$.

بنابراین با احتمال حدودا برابر ۱، روش بالا منجر به یافتن یک مشخصه تفاضل ناممکن می‌شود. مشخصه تفاضل ناممکن به‌دست‌آمده به این شکل خواهد بود که یک مقدار تفاضلی خاصی δ_{in} (با شرایطی که توصیف شد) نمی‌تواند پس از نُه‌دور به یکی از تفاضل‌های δ_{out}^{i} با مشخصات یادشده برود که $1 \le i \le 2^{42}$.

۶- اعمال حمله به ده دور از الگوریتم Zorro

2^n زوج متن (P_j, P'_j) که $1 \le j \le 2^n$ را انتخاب می‌کنیم به‌گونه‌ای که $P_j = P'_j \oplus \delta_{in}$ است و منظور از δ_{in} همان تفاضلی است که توصیفش در بخش ۵ ارائه شده است. متن‌های اصلی را با استفاده از الگوریتم Zorro ده‌دوری رمز کرده و زوج متن‌های معادل آن‌ها (C_i, C'_i) را به‌دست می‌آوریم (شکل (۶)).

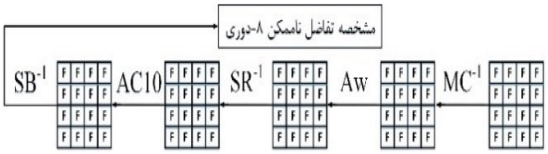
همان‌طورکه در بخش ۲ توضیح داده شد، به‌دلیل خطی‌بودن دو تبدیل مخلوط‌ساز ستونی و جمع با کلید، می‌توانیم این دو تبدیل را با یکدیگر جابه‌جا کنیم با این تفاوت که در عمل جمع با کلید، به‌جای استفاده از کلید k باید از زیرکلید معادل آن یعنی $w = MC^{-1}(k)$ استفاده کنیم. بنابراین در مرحله بعد برای هر یک از جفت متن‌های رمزشده به‌دست آمده، چهار بایت سطر نخست از کلید معادل دور آخر ($w = MC^{-1}(k)$) را حدس می‌زنیم و به‌ازای آن، تفاضل انتهای دور نهم را محاسبه می‌کنیم. این کار امکان‌پذیر است چون جعبه‌های جانشینی تنها به بایت‌های سطر نخست اعمال می‌شوند و تأثیری بر مقادیر تفاضلی سطرهای دیگر در دور آخر ندارند. اگر مقدار تفاضل به‌دست‌آمده برابر یکی از مقادیر δ_{out}^{i}ها به ازای $1 \le i \le 2^{42}$ شود، در آن صورت کلید حدس‌زده‌شده غلط است و باید از فهرست نامزدهای ممکن حذف شود.

پیچیدگی

احتمال آن‌که تفاضل محاسبه‌شده در انتهای دور هشتم، یکی از مقادیر γ_{out}^{i}ها ($1 \le i \le 2^{42}$) شود برابر با $\frac{2^{42}}{2^{128}} = 2^{-86}$ است. بنابراین احتمال این‌که بعد از رمزگشایی یک زوج به‌ازای یک کلید حدس‌زده‌شده، کلید غلط حذف شود، برابر 2^{-86} است. اگر تعداد کلیدهای غلط باقی‌مانده N باشد، پس از امتحان‌کردن یک زوج انتظار داریم که تعداد کلیدهای غلط باقی‌مانده برابر با $N - N \times 2^{-86} = N(1 - 2^{-86})$ شود. با توجه به آنکه 2^{32} نامزد برای چهار بایت کلید معادل وجود دارد، بنابراین پس از تکرار رویه بالا برای 2^n زوج، انتظار داریم که $2^{32}(1 - 2^{-86})^{2^n}$ کلید در فهرست باقی بماند. در این‌صورت اگر $n = 90.5$ انتخاب شود، تعداد کلیدهای نادرست باقی‌مانده برابر خواهد شد با:

$$2^{32}(1 - 2^{-86})^{2^{86}\times 2^{4.5}} \approx 2^{32} * e^{-22.6} < 1$$

بنابراین انتظار می‌رود که هیچ کلید غلطی باقی نماند و کلید صحیح به‌صورت یکتا در چهار بایت مورد هدف به‌دست آید.



(شکل-۶): حمله تفاضل ناممکن ۱۰-دوری
(Figure-6): 10-round impossible differential attack

پیچیدگی دادهٔ حملهٔ ارائه‌شده برابر است با $2^{90.5}$ زوج و معادل $2^{91.5}$ متن منتخب است. پیچیدگی زمانی اجرای حمله برای به‌دست‌آوردن چهار بایت کلید معادل برابر $2 \times 2^n \times 2^{32} = 2^{123.5}$ عمل رمزنگاری یک‌دوری است که معادل $\frac{2^{123.5}}{10} \approx 2^{120.2}$ عمل رمزنگاری ده‌دوری است. دوازده بایت باقیمانده را نیز می‌توان با استفاده از جستجوی جامع و پیچیدگی 2^{96} عمل رمزنگاری به‌دست آورد. درنهایت پیچیدگی زمانی کل حمله، حدودا برابر با $2^{120.2} + 2^{96} \approx 2^{120.2}$ خواهد بود.

۷- نتیجه‌گیری

در این مقاله روشی نوین به منظور یافتن مشخصه‌های تفاضل ناممکن در الگوریتم Zorro را ارائه کردیم. برمبنای روش ارائه‌شده می‌توان برای نُه‌دور از الگوریتم‌هایی با ساختار شبیه Zorro و بدون درنظرگرفتن خصوصیات لایهٔ خطی، مشخصهٔ تفاضل ناممکن پیدا کرد. همچنین حمله بازیابی کلید را برای ده‌دور الگوریتم اجرا کرد. بنابراین فارغ از ویژگی‌های عناصر به‌کاررفته می‌توان نشان داد که این تعداد دور از الگوریتم حتی با تغییر لایه خطی نمی‌تواند به امنیت لازم برسد.

[DOI: 10.29252/jsdp.16.4.17]

8- References ۸- مراجع

[1] S. Mangard, E. Oswald, and T. Popp, Power analysis attacks: Revealing the secrets of smart cards vol. 31: Springer Science & Business Media, 2008.

[۲] ج. شیخزادگان، ا. ویزندان، ع. میرقدری. "تحلیل الگوریتم رمز جریانی HC-256' بر اساس حمله تمایز". پردازش علائم و داده‌ها. ۷ (۲): ۱۳-۲۲. ۱۳۸۹.

[۲] j.Sheikhzadegan, A.Vizandan,E.Mirqadri, "Cryptanalysis of the stream cipher HC-256' based on distinguishing attack", *Signal and data processing*, Vol. 7(2), pp.13-22, 1389.

[3] H. Soleimany, "Probabilistic slide cryptanalysis and its applications to LED-64 and Zorro," *in International Workshop on Fast Software Encryption*, pp. 373-389, 2014.

[4] J. Guo, I. Nikolic, T. Peyrin, and L. Wang, "Cryptanalysis of Zorro," *IACR Cryptology ePrint Archive*, vol. 2013, p. 713, 2013.

[5] S. Rasoolzadeh, Z. Ahmadian, M. Salmasizadeh, and M. R .Aref, "Total break of Zorro using linear and differential attacks," *The ISC International Journal of Information Security*, vol. 6, pp. 23-34, 2014

[6] Y. Wang, W. Wu, Z. Guo, and X. Yu, "Differential cryptanalysis and linear distinguisher of full-round Zorro," i*n International Conference on Applied Cryptography and Network Security* , pp. 308-323, 2014.

[7] G. Leander, B. Minaud, and S. Rønjom, "A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro," *EUROCRYPT* (1), vol. 9056, 2015, pp. 254-283.

[8] A. Bar-On, I. Dinur, O. Dunkelman, V. Lallemand, N. Keller, and B. Tsaban, "Cryptanalysis of SP Networks with Partial Non-Linear Layers," *in EUROCRYPT* (1) , pp. 315-342, 2015.

[9] N. F. Pub, "197: Advanced encryption standard (AES)," Federal information processing standards publication, vol. 197, p. 0311, 2001.

[10] B. Gérard, V. Grosso, M. Naya-Plasencia, and F.-X. Standaert, "Block ciphers that are easier to mask: How far can we go?," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 383-399, 2013.

[11] B. Bahrak and M. R. Aref, "Impossible differential attack on seven-round AES-128," *IET Information Security*, vol. 2 ,pp. 28-32, 2008.

[12] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 12-23,1999.

[13] E. Biham, A. Biryukov, and A. Shamir, "Miss in the Middle Attacks on IDEA and Khufu," in FSE, pp. 124-138, 1999

[14] P. Derbez, P.-A. Fouque, and J. Jean, "Improved key recovery attacks on reduced-round AES in the single-key setting," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* ,pp. 371-387, 2013.

[15] M. Shakiba, M. Dakhilalian, H. Mala, "Impossible Differential Cryptanalysis of 3D Block Cipher," in *The Modares Journal of Electrical Engineering*, vol.16(3), pp.24-8, 2016 Oct 1

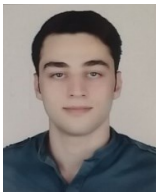
[16] A. R. Shahmirzadi, S. A. Azimi, M. Salmasizadeh, J. Mohajeri, M. R. Aref, "Impossible Differential Cryptanalysis of Reduced-Round Midori64 Block Cipher," in ISeCure. 2018 Jan 1;10(1).

هادی سلیمانی: وی در سال ۱۳۸۷ در مقطع کارشناسی مخابرات از دانشگاه علم و صنعت ایران فارغ‌التحصیل شد و تحصیلات خود را در مقطع کارشناسی‌ارشد در دانشگاه امام حسین (ع) در گرایش مخابرات رمز در سال ۱۳۸۹ و سپس در مقطع دکترا در دانشکده علوم کامپیوتر دانشگاه آلتو فنلاند درسال ۱۳۹۴ به پایان رساند. همچنین طی یک دوره کوتاه‌مدت پسادکترا در گروه رمزنگاری دانشگاه DTU دانمارک درخصوص تحلیل و طراحی رمزهای قالبی نوین مشغول به پژوهش شد. وی هم‌اکنون، ضمن همکاری با پژوهشکده‌ها و مراکز پژوهشی مختلف در حوزه رمزنگاری و امنیت اطلاعات، به‌عنوان استادیار گروه امنیت شبکه و رمزنگاری پژوهشکده فضای مجازی دانشگاه شهید بهشتی مشغول به کار است. زمینه‌های پژوهشی مورد علاقه ایشان تحلیل و طراحی اولیه‌های رمزنگاری متقارن و همچنین پیاده‌سازی امن است.

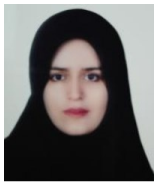
نشانی رایانامه ایشان عبارت است از:

h_soleimany@sbu.ac.ir

[DOI: 10.29252/jsdp.16.4.17]



علیرضا مهرداد: وی تحصیلات کارشناسی خود را در رشته مهندسی برق گرایش مخابرات در سال ۱۳۹۴ در دانشگاه نوشیروانی بابل به پایان رساند. ایشان مدرک کارشناسی ارشد خود را در رشته برق گرایش مخابرات امن و رمزنگاری از دانشگاه شهید بهشتی در سال ۱۳۹۶ اخذ کردند. زمینه‌های پژوهشی مورد علاقه ایشان تحلیل و طراحی اولیه‌های رمزنگاری متقارن است.
نشانی رایانامه ایشان عبارت است از:
a.mehrdad@mail.sbu.ac.ir



سعیده صادقی: وی تحصیلات کارشناسی خود را در رشته مهندسی برق گرایش الکترونیک در سال ۱۳۹۲ در دانشگاه شریعتی به پایان رساند. ایشان مدرک کارشناسی ارشد خود را در رشته برق گرایش مخابرات امن و رمزنگاری از دانشگاه شهید بهشتی در سال ۱۳۹۶ اخذ کردند. زمینه‌های پژوهشی مورد علاقه ایشان تحلیل سامانه‌های رمز نگاری متقارن و امنیت در حوزه وب است.
نشانی رایانامه ایشان عبارت است از:
saei.sadeghi@mail.sbu.ac.ir

فرخ لقا معظمی: وی در سال ۱۳۸۳ در مقطع کارشناسی ریاضی از دانشگاه الزهرا فارغ‌التحصیل شد و تحصیلات خود در مقطع کارشناسی‌ارشد را در دانشگاه صنعتی شریف در سال ۱۳۸۵ و سپس در مقطع دکترا در دانشکده ریاضی دانشگاه الزهرا درسال ۱۳۹۲ به پایان رساند. همچنین طی یک دوره پسادکترا در دانشکده ریاضی دانشگاه شریف درخصوص تحلیل سامانه‌های رمزنگاری مشغول به پژوهش شد. وی هم‌اکنون، به عنوان استادیار گروه امنیت شبکه و رمزنگاری پژوهشکده فضای مجازی دانشگاه شهید بهشتی مشغول به کار است. زمینه‌های پژوهشی مورد علاقه ایشان پروتکل‌های رمزنگاری، سامانه‌های رمزنگاری مشبکه مبنا و تحلیل و طراحی اولیه‌های رمزنگاری متقارن است.
نشانی رایانامه ایشان عبارت است از:
f_moazemi@mail.sbu.ac.ir

[DOI: 10.29252/jsdp.16.4.17]