دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۰، جلد ۱۹، شماره ۱ (۲۷-۳۳)
https://monadi.isc.org.ir

ارائه‌شده در شانزدهمین کنفرانس بین المللی انجمن رمز ایران در دانشگاه فردوسی مشهد، ۶ و ۷ شهریور ۱۳۹۸

یک تمایزگر تفاضلی برای دو دور الگوریتم رمزگذاری احرازاصالت شده π-Cipher★

بهزاد سعیدی* و زهرا احمدیان

دانشکده مهندسی برق، دانشگاه شهید بهشتی، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
الگوریتم π-Cipher
رقابت CAESAR
جایگشت ARX
تمایزگر تفاضلی
احتمال مشخصه‌ی تفاضلی

dor: 10.0000/000000000

نوع مقاله: پژوهشی

چکیده

الگوریتم π-Cipher یکی از ۲۹ طرح راه یافته به دور دوم رقابت سزار می‌باشد. این الگوریتم دارای ساختاری موازی و اسفنجی است که از جایگشتی از نوع ARX بهره می‌برد و در دو نسخه و هر یک در انواع متعدد ارائه شده است. در این مقاله، الگوریتم π-Cipher با کلمات ۱۶ بیتی مورد بررسی قرار گرفته است. با تمرکز بر روی ساختار داخلی جایگشت π استفاده شده در این الگوریتم و با تحلیل تفاضلی بر روی دو دور آن، یک تمایزگر تفاضلی با احتمال 2^{-95} معرفی می شود. این نخستین تحلیل روی این الگوریتم با در نظر گرفتن جزئیات ساختار داخلی جایگشت آن می‌باشد.

۱ مقدمه

حوزه‌ی رمزگذاری احراز اصالت شده یکی از موضوعات در حال گسترش در رمزنگاری متقارن می‌باشد و در سال‌های اخیر مطالعات و تحقیقات گسترده‌ای در این زمینه انجام شده است. رقابت اروپایی سزار به منظور طراحی الگوریتم‌های رمزگذاری احراز اصالت شده از سوی جامعه‌ی رمزنگاری اروپا در سال ۲۰۱۴ اعلام عمومی شد و در پاسخ به این فراخوان ۵۷ طرح ارائه و در طی چهار مرحله طرح‌های برگزیده از دیدگاه کارایی و امنیت انتخاب شدند [۱]. الگوریتم رمزنگاری π-Cipher یکی از ۲۹ طرح راه یافته به دور دوم این رقابت است [۲]. در مقاله‌ی پیش رو، امنیت این الگوریتم در برابر تحلیل تفاضلی مورد بررسی قرار خواهد گرفت. به طور کلی الگوریتم‌های رمزنگاری متقارن را می‌توان با در نظر گرفتن عملکرد و نقاط ضعف احتمالی آن‌ها با روش‌هایی مانند حمله‌ی خطی، تفاضلی، جبری و ... تحلیل کرد.

حمله‌ی تفاضلی، یک روش تحلیل امنیتی در مدل متن اصلی منتخب می‌باشد. در این روش، تحلیل‌گر تلاش می‌کند تا رابطه‌ی محتملی میان تفاضل ورودی و خروجی در هر دور از رمز پیدا کند. با بهم پیوستن این روابط در دورهای متوالی رمز، تحلیل‌گر انتظار رابطه‌ای با احتمال به اندازه‌ی کافی بزرگ بین تفاضل ورودی و تفاضل خروجی را خواهد داشت. چنین خاصیتی می تواند در نقش تمایز الگوریتم رمز از یک جایگشت شبه تصادفی (تمایزگر)، و یا برای بازیابی اطلاعاتی از کلید الگوریتم به کار برده شود.

بنا بر ادعای طراحان الگوریتم π-Cipher [۲]، این الگوریتم به صورت موازی، افزایشی، مبتنی بر تک شمار، دارای برچسب (چکیده) مقاوم در برابر حمله‌ی پیش تصویر دوم و رمزگذاری احراز اصالت شده با داده‌های مرتبط است، که شامل ویژگی‌های رمزنگاشتی زیر است:

(۱) طراحی در دسته‌ی «رمزگذاری-سپس-کد احراز اصالت» قرار دارد.
(۲) دارای طراحی با ساختار موازی و افزایشی و مبتنی بر شمارنده است، اما برای ایجاد مقاومت برچسب‌های کد احراز اصالت در برابر پیش تصویر دوم به جای عملیات XOR برای اجزای برچسب میانی، از جمع‌های مؤلفه به مؤلفه در $(\mathbb{Z}_{2^w})^d$ استفاده شده است.

★از کمیته علمی شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: b.saeedi@mail.sbu.ac.ir (بهزاد سعیدی)، z_ahmadian@sbu.ac.ir (زهرا احمدیان)

جدول ۱. مشخصات الگوریتم π-Cipher [۲]

نسخه	نوع الگوریتم	طول کلمات به بیت	طول کلید	طول برچسب	تعداد دورها
v1,2	π16-Cipher096	۱۶	۱۲۸	۹۶	۳
v1,2	π32-Cipher128	۳۲	۲۵۶	۱۲۸	۳
v1,2	π64-Cipher128	۶۴	۵۱۲	۱۲۸	۳
v1,2	π64-Cipher256	۶۴	۵۱۲	۲۵۶	۳
v2	π16-Cipher128	۱۶	۱۲۸	۱۲۸	۴
v2	π32-Cipher256	۳۲	۲۵۶	۲۵۶	۴
سبک وزن	π16-Cipher096	۱۶	۱۲۸	۹۶	۲
سبک وزن	π16-Cipher128	۱۶	۱۲۸	۱۲۸	۲

پس از آنکه مشکلاتی در نسخه اول (version 1) این الگوریتم مشاهده شد که منجر به آسیب پذیری امنیتی در این طرح شد، طراحان نسخه دوم (version 2) آن را ارائه دادند. هر دو نسخه‌ی این الگوریتم بنا بر طول کلمات، طول کلید و همچنین قاعده‌ی لایی گذاری، دارای انواع [۱] مختلفی می‌باشد که طبقه‌بندی آن‌ها در جدول ۱ جمع‌بندی شده است.

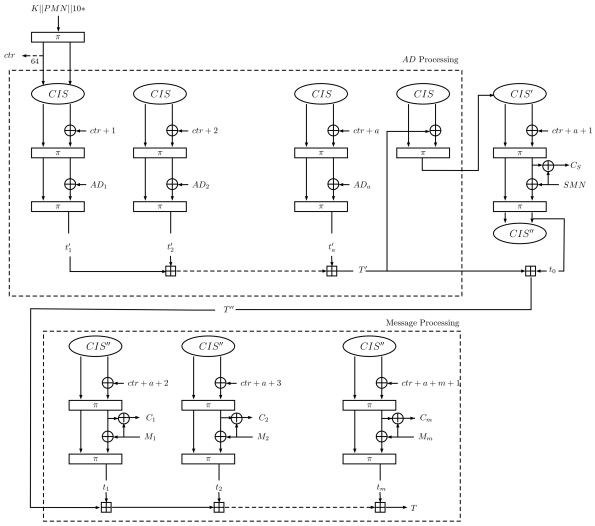
در جریان مسابقه سزار، هر دو نسخه‌ی این طرح (v1 و v2) تحلیل‌هایی بر روی الگوریتم‌های تک دوری، دو دوری، ۲/۵ دوری و سه دوری دریافت کردند. در [۳] یک تحلیل کشف حالت بر روی نسخه‌ی اول تک دوری، دو دوری، سه دوری و نسخه‌ی دوم تک دوری ارائه شده است و همچنین در [۴]، به حمله‌ی کشف کلید بر روی نسخه‌ی دوم دو دوری و ۲/۵ دوری پرداخته شده است. اساس هر دو تحلیل بر مبنای حدس و تعیین بنا شده است. بنابراین تحلیل کشف حالت در [۳] برای نسخه‌ی دوم این الگوریتم هنگامی که دارای دو دور یا بیشتر باشد ناتوان است در حالی که در مقاله‌ی پیش رو تحلیل بر روی نسخه‌ی دوم و دو دوری انجام شده است.

جایگشت استفاده شده در این الگوریتم دارای طولی برابر $16w$ می‌باشد که w طول کلمات این الگوریتم می‌باشد و می‌تواند برابر با ۱۶، ۳۲ و یا ۶۴ بیت باشد. عنصر سازنده‌ی این جایگشت که بخش عمده‌ی امنیت الگوریتم π-Cipher را تأمین می‌کند، بر عهده‌ی عملگر $*$ است که دارای ساختاری مبتنی بر ARX می باشد. هر دو تحلیل ارائه شده برای این الگوریتم، نهایتاً تا سطح عملگر $*$ عمیق شده و این عملگر را بصورت یک جعبه سیاه در نظر می گیرند.

در این مقاله تحلیل تفاضلی برای این الگوریتم، با درنظرگرفتن جزئیات ساختار داخلی عملگر $*$ ارائه می شود. با بررسی تعدادی از تفاضل‌های با وزن همینگ کم با احتمال پراکنش بالا، یک تمایزگر تفاضلی دو دوری با احتمال 2^{-95} برای طرح رمزگذاری احرازاصالت شده π-Cipher معرفی می کنیم. در جدول ۳ خلاصه‌ای از کارهای پیشین و نتایج این مقاله ارائه شده است.

ساختار این مقاله به شرح زیر است. در بخش ۲ مشخصات الگوریتم

[1] Variant



شکل ۱. ساختار کلی رمزگذاری π-Cipher [۴]

π-Cipher و مراحل آن تا حد نیاز معرفی می شود، بخش ۳ مقدماتی از تحلیل تفاضلی در ساختارهای ARX را شرح می دهد. بخش ۴ نتایج تحلیل تفاضلی روی الگوریتم π-Cipher را ارائه می‌کند و نهایتاً نتیجه‌گیری کار در بخش ۵ آورده می‌شود.

۲ مشخصات الگوریتم π-Cipher.v2

این الگوریتم در قسمت احراز اصالت خود از طرح اصالت سنجی شمارنده محور استفاده می‌کند. شکل ۱ ساختار کلی این الگوریتم را نشان می‌دهد که دارای چهار مرحله‌ی اصلی مقداردهی اولیه، پردازش داده–پیوست [۲]، پردازش عدد مخفی پیام [۳] و همچنین پردازش پیام است.

۱.۲ مرحله مقدار دهی اولیه

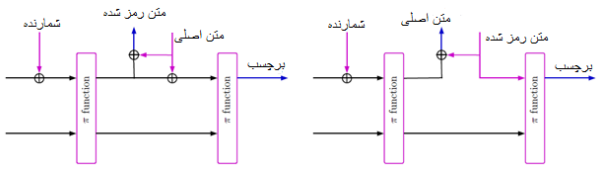
در این مرحله، کلید به همراه عدد عمومی پیام [۴] که بخشی از تک شمار این الگوریتم به حساب می‌آید و به منظور تحقق یک سیستم رمزگذاری تصادفی از آن استفاده می‌شود، به الگوریتم تزریق می‌شود. سپس با استفاده از لایی گذاری، طول حالت‌های کمتر از طول قالب را به اندازه‌ی آن قالب گسترش می‌دهد و پس از یک مرحله عبور از تابع جایگشت π، حالت داخلی مشترک تولید می‌شود. در این مرحله، شمارنده‌ی الگوریتم از ۶۴ بیت قسمت ظرفیت حالت داخلی مشترک [۵] استخراج می‌شود.

عدد عمومی پیام برای الگوریتم با کلمات ۱۶ بیتی طولی برابر ۳۲ بیت و برای الگوریتم هایی با کلمات ۳۲ و ۶۴ بیتی طولی معادل ۱۲۸ بیت خواهد داشت.

$$CIS \leftarrow \pi(K\|PMN\|10^*) \qquad (۱)$$

حالتی که در این الگوریتم به‌روز می‌شود شامل چهار بخش است که هرکدام

[2] Associated Data (AD) [3] Secret Message Number (SMN) [4] Public Message Number (PMN) [5] Common Internal State (CIS)



شکل ۲. سه‌گانه. مؤلفه‌ی سمت راست مربوط به رمزگشایی و مؤلفه‌ی سمت چپ مربوط به رمزگذاری [۲]

دارای طولی برابر با w۴ هستند و در اینجا منظور از قسمت نرخ حالت، همان کلمات فرد و منظور از قسمت ظرفیت حالت، کلمات زوج آن می‌باشد.

۲.۲ مرحله پردازش داده-پیوست

همواره بخش‌هایی از پیام وجود دارند که نیازمند احراز اصالت هستند ولی به رمزگذاری نیازی ندارند (مانند سرآیندهای بسته‌های مخابراتی). چنین بخش‌هایی از پیام باید از پیام اصلی متمایز شوند که به آن‌ها داده-پیوست گفته می‌شود. حالت‌های داخلی مشترک تولید شده بصورت موازی و با کمک قالب‌های داده-پیوست و شمارنده به عنوان ورودی‌های e-سه‌گانه [۱]، برچسب‌های جزئی داده-پیوست را تولید می‌کنند. این واحد که خود متشکل از دو جایگشت پیاپی π می باشد، در شکل ۲ نشان داده شده است. قاعده‌ی لایی گذاری بصورت زیر می‌باشد

$$Pad(AD) = AD_1 \| AD_2 \| \cdots \| AD_a \| 10^* \qquad (۲)$$

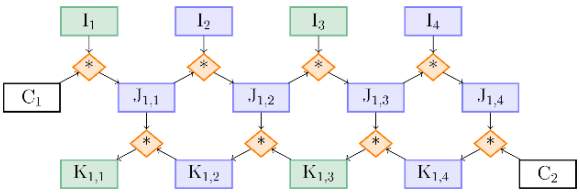
1 بیانگر بایت 0x01 و 1 بیانگر بایت 0x00 است. اگر طول داده-پیوست مضربی از طول قسمت نرخ حالت باشد، آنگاه یک قالب به تعداد قالب‌هایی که پردازش می‌شوند اضافه خواهد شد.

در نسخه‌ی اول الگوریتم π-Cipher، با فرض نبود داده-پیوست، قالب مربوط به آن نیز خالی می‌ماند، اما در نسخه‌ی دوم این الگوریتم حتی در صورت نبود داده-پیوست نیز، توسط این قاعده‌ی لایی گذاری حداقل یک قالب برای پردازش و به تبع آن حداقل یک برچسب جزئی برای این مرحله موجود خواهد بود.

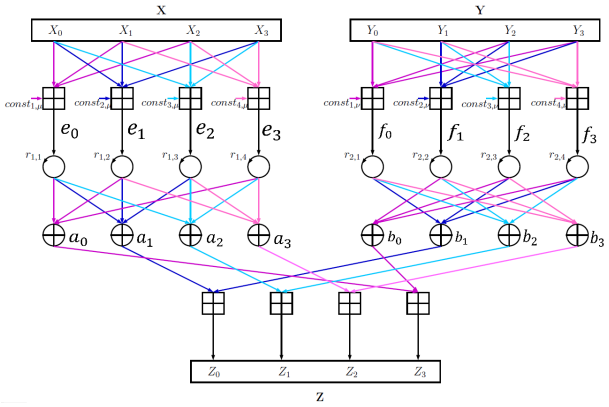
۳.۲ مرحله پردازش عدد مخفی پیام

عدد مخفی پیام نیز به همراه عدد عمومی پیام، بخش دیگری از تک شمار این الگوریتم را تشکیل می‌دهد که برای الگوریتم با کلمات ۱۶ بیتی طولی برابر ۱۲۸ بیت، برای الگوریتم با کلمات ۳۲ بیتی طولی برابر ۲۵۶ بیت و برای الگوریتم با کلمات ۶۴ بیتی طولی معادل با ۵۱۲ بیت خواهد داشت. این مرحله از رمزنگاری (در صورت خالی نبودن رشته بیت مربوط به عدد مخفی پیام) با فراخوانی e-سه‌گانه شروع می‌شود؛ به طوری که ورودی آن سه تایی $(CIS, ctr + a + 1, SMN)$ و خروجی آن زوج (c_0, t_0) خواهد بود. SMN عدد مخفی پیام و بخش محرمانه تک‌شمار است.

[1] e-triplex



شکل ۳. یک دور تابع جایگشت π [۳]



شکل ۴. ساختار ARX عملگر $*$ [۲]

۴.۲ مرحله پردازش پیام

پیام $M = M_1 \| M_2 \| \cdots \| M_m$ نیز مانند داده-پیوست بصورت موازی و قالب به قالب از طریق مؤلفه‌ی سه‌تایی پردازش می‌شود که قاعده‌ی لایی گذاری در آن همانند مرحله پردازش داده-پیوست می‌باشد. در انتها نیز برچسب نهایی احراز اصالت که تابعی از برچسب‌های مربوط به پردازش عدد مخفی، پردازش داده-پیوست و پردازش پیام هستند بصورت زیر بدست می‌آید.

$$T = T'' \boxplus t_1 \boxplus t_2 \boxplus \cdots \boxplus t_m \qquad (۳)$$

خروجی این الگوریتم، شامل متن رمز شده و برچسب، مطابق زیر خواهد بود.

$$C = C_0 \| C_1 \| \cdots \| C_m \| T \qquad (۴)$$

شکل ۳ ساختار مربوط به یک دور از تابع جایگشت π را نشان می‌دهد که شامل هشت عملگر $*$ می‌باشد. جزئیات داخلی این عملگر نیز در شکل ۴ به تصویر درآمده است. همانطور که مشخص است، عملگر $*$ ساختاری بصورت ARX دارد که با عملگرهای جمع به پیمانه‌ی 2^w، چرخش به سمت چپ و عملگر یای انحصاری (XOR) پیاده‌سازی شده است.

۳ تحلیل تفاضلی ساختار ARX

در ساختارهای ARX تنها عملگر غیرخطی، عملگر جمع پیمانه‌ای است. رفتار تفاضلی این عملگر مورد بررسی فراوان قرار گرفته است و الگوریتم‌های کارایی جهت محاسبه‌ی احتمال تفاضلی این عملگر که در زمان چندجمله‌ای قابل اجرا هستند، ارائه شده‌اند [۵، ۶].

۱.۳ خاصیت تفاضلی جمع پیمانه‌ای با دو ورودی

یک جمع پیمانه‌ای با کلمات n بیتی با دو ورودی را در نظر بگیرید. اگر α و β تفاضل های ورودی و γ تفاضل خروجی این عملگر باشد، احتمال چنین تفاضلی را با $xdp^+(\alpha,\beta\rightarrow\gamma)$ نشان می دهیم. در [۵] الگوریتم بسیار کارایی برای شناسایی تفاضل‌های ناممکن (با احتمال صفر) و نیز محاسبه احتمال تفاضل‌های ممکن، ارائه شده است که بصورت قضیه زیر است:

قضیه ۱ ([۵]). احتمال تفاضلی جمع پیمانه‌ای $xdp^+(\alpha,\beta\rightarrow\gamma)$:

- برابر صفر است، اگر و فقط اگر

$$eq\,(\alpha\ll 1,\beta\ll 1,\gamma\ll 1)\wedge(\mathrm{xor}(\alpha,\beta,\gamma)\oplus(\alpha\ll 1))\neq 0$$

- در غیر این صورت برابر است با: $2^{-w_h^*(\neg eq(\alpha,\beta,\gamma))}$.

که در روابط فوق $w_h^*(x)$ برابر با وزن همینگ کلمه x به استثنای *MSB* آن است.

تابع eq به این صورت می‌باشد که در صورتی که بیت‌های α_i، β_i و γ_i به طور همزمان برابر با صفر و یا یک باشند، آنگاه مقدار بیت متناظر $eq(\alpha_i,\beta_i,\gamma_i)$ برابر با یک و در غیر اینصورت برابر با صفر خواهد بود. تابع $\neg eq(\alpha_i,\beta_i,\gamma_i)$ نیز نقیض آن می‌باشد.

یک رویکرد متداول در تحلیل ساختارهای شامل عملگر جمع پیمانه‌ای، تقریب آن با عملگر خطی XOR است. به این ترتیب برای تفاضل‌های ورودی (α,β) تفاضل خروجی $\gamma=\alpha\oplus\gamma$ خواهد بود. این تفاضل همواره شدنی است و احتمال آن با استفاده از قضیه ۱ برابر است با:

$$xdp^+(\alpha,\beta\rightarrow\alpha\oplus\beta)=2^{-w_h^*(\alpha\wedge\beta)} \qquad (۵)$$

۲.۳ خاصیت تفاضلی جمع پیمانه‌ای با سه ورودی

برای جمع پیمانه‌ای با کلمات n بیتی با سه ورودی، و تفاضلات ورودی α، β و λ و تفاضل خروجی γ، احتمال تفاضلی را با

$$xdp^+(\alpha,\beta,\lambda\rightarrow\gamma)$$

نشان می‌دهیم. در این قسمت به بررسی رفتار تفاضلی جمع پیمانه‌ای با سه ورودی در حالت خاص $\gamma=\alpha\oplus\beta\oplus\lambda$ می‌پردازیم.

یک روش برای تخمین $xdp^+(\alpha,\beta,\lambda\rightarrow\alpha\oplus\beta\oplus\lambda)$، معادل کردن جمع پیمانه‌ای سه ورودی با دو جمع پیمانه‌ای دو ورودی متوالی، و استفاده از حاصلضرب احتمالات تفاضلی دو ورودی با فرض استقلال دو پیشامد است. به عبارت دیگر

$$xdp^+(\alpha,\beta\rightarrow\alpha\oplus\beta\oplus\lambda)=xdp^+(\alpha,\beta\rightarrow\alpha\oplus\beta)\cdot xdp^+(\alpha\oplus\beta,\lambda\rightarrow\alpha\oplus\beta\oplus\lambda) \qquad (۶)$$

رابطه فوق در واقع احتمال یک مسیر تفاضلی مشخص را محاسبه می‌کند و آن مسیری است که خروجی جمع پیمانه اول در آن لزوما دارای تفاضل با مقدار $\alpha\oplus\beta$ باشد. اما آنچه درمحاسبه

$$xdp^+(\alpha,\beta,\lambda\rightarrow\alpha\oplus\beta\oplus\lambda)$$

مهم است، تفاضل های ورودی و خروجی هستند صرف نظر از اینکه تفاضلات میانی چه مقادیری را اتخاذ می‌کنند. به این ترتیب مقدار دقیق این احتمال به صورت زیر قابل محاسبه است:

$$xdp^+(\alpha,\beta,\lambda\rightarrow\alpha\oplus\beta\oplus\lambda)=\sum_{v\in\{0,1\}^{16}}\Big(xdp^+(\alpha,\beta\rightarrow v)\cdot xdp^+(v,\lambda\rightarrow\alpha\oplus\beta\oplus\lambda)\Big) \qquad (۷)$$

بدیهی است که مقدار محاسبه شده از رابطه (۷) بایستی بزرگتر یا مساوی با مقدار محاسبه شده از رابطه (۶) باشد. برای مثال برای تفاضل‌های زیر

$$\alpha=0\text{x}0018,\quad \beta=0\text{x}0010,\quad \lambda=0\text{x}0000$$

مقدار $xdp^+(\alpha,\beta,\lambda\rightarrow\alpha\oplus\beta\oplus\lambda)$ با روش‌های اول و دوم به ترتیب برابر با 2^{-3} و $2^{-2.54}$ بدست می‌آید.

در جستجوی مشخصه‌های تفاضلی در بخش بعد از این روش محاسبه احتمال تفاضل برای عملگرهای جمع پیمانه‌ای ۳ ورودی استفاده می‌کنیم.

۴ تمایزگر تفاضلی دو دوری برای π16-Cipher

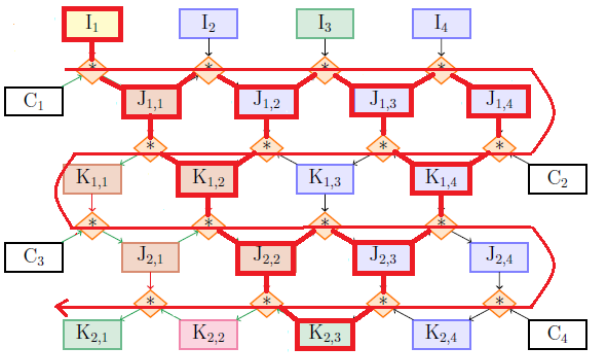
با توجه به نحوه‌ی استفاده از جایگشت π در ساختار π-Cipher، قسمت ظرفیت در حالت داخلی مشترک CIS'' بدون تغییر خواهد ماند و لذا تفاضل صفر خواهد داشت و با توجه به اینکه شمارنده‌ی ۶۴ بیتی بر روی قسمت نرخ حالت تأثیر می‌گذارد، ما نیز تنها به دنبال جستجوی مشخصه‌های تفاضلی‌ای هستیم که فقط در بخش نرخ خود مقدار ناصفر داشته و تفاضل بخش ظرفیت را صفر قرار می دهیم. از سوی دیگر با توجه به قضیه ۱، هر چه تفاضل ورودی وزن کوچکتری داشته باشد، بطور بالقوه احتمال بیشتری خواهد داشت. لذا ما نیز در جستجو برای مشخصه تفاضلی، وزن همینگ را حتی الامکان کوچک قرار می‌دهیم.

نخست برای یک دور از جایگشت π تعدادی از تفاضلات یک دوری مدنظر را با قیود فوق، بررسی می‌کنیم. این تفاضلات در جدول ۲ آورده شده‌اند. در این جدول منظور از $I_{1,m}(i)$ بیت iام از کلمه ۱۶ بیتی mام از قطعه I_1 می‌باشد. همانطور که از احتمالات تفاضلی اشاره شده در جدول ۲ مشخص است، ورودی با وزن همینگ سه نسبت به وزن یک، دو و چهار بیتی منجر به احتمالات تفاضلی مطلوب‌تری می‌شود زیرا در بیت‌های e و f (نشان داده شده در شکل ۴) امکان خنثی شدن بیت‌های بیشتری از تفاضل‌ها و حصول تفاضل صفر در ادامه می باشد که این امر به نفع احتمال مشخصه تفاضلی است.

از بین تفاضل‌های ورودی داده شده در جدول ۲، آنهایی که در دور اول رفتار نسبتاً بهتری داشته‌اند را برای یک دور بیشتر ادامه داده و از میان

جدول ۲. احتمال انتشار تفاضل ورودی‌های مختلف برای یک دور

لگاریتم احتمال	بیت‌های فعال ورودی
-۲۱۰	$I_{۱,۴}(۱۶)$
-۱۳۰	$I_{۱,۴}(۱۶);\ I_{۱,۱}(۱۶)$
-۱۴۵	$I_{۱,۲}(۱۶);\ I_{۱,۱}(۱۶)$
-۷۶	$I_{۱,۱}(۲);\ I_{۱,۲}(۲);\ I_{۱,۴}(۲)$
-۸۳	$I_{۱,۲}(۱۶);\ I_{۱,۳}(۱۶);\ I_{۱,۴}(۱۶)$
-۷۷	$I_{۱,۱}(۱۶);\ I_{۱,۲}(۱۶);\ I_{۱,۳}(۱۶)$
-۶۵	$I_{۱,۱}(۸);\ I_{۱,۲}(۸);\ I_{۱,۳}(۸)$
-۵۷	$I_{۱,۱}(۱);\ I_{۱,۲}(۱);\ I_{۱,۳}(۱)$
-۵۲	$I_{۱,۱}(۲);\ I_{۱,۲}(۲);\ I_{۱,۳}(۲)$
-۵۹	$I_{۱,۲}(۱۲);\ I_{۱,۳}(۱۲);\ I_{۱,۴}(۱۲)$



شکل ۵. مشخصه تفاضلی دو دوری

آنها بهترین مشخصه تفاضلی دو دوری را بدست آورده‌ایم. این مشخصه دارای تفاضل ورودی

$$I_{۱,۲}(۱۲) = I_{۱,۳}(۱۲) = I_{۱,۴}(۱۲) = ۱$$

می‌باشد. این ورودی پس از یک دور با احتمال $۲^{-۵۹}$ به خروجی زیر انتشار پیدا می‌کند.

$$K_{۱,۱} = \text{0x0000000000000000}$$
$$K_{۱,۲} = \text{0x0000800080008000}$$
$$K_{۱,۳} = \text{0x0000000000000000}$$
$$K_{۱,۴} = \text{0x0000002000200020}$$

در شکل ۵ نحوه‌ی انتشار این ورودی تفاضلی به ازاء دو دور از الگوریتم به تصویر کشیده شده است. بیت‌های فعال با توجه به آفست‌های چرخش در ساختار ARX طوری تنظیم شده‌اند که در موقعیت های مشابه قرار می‌گیرند و در عملگرهای ششم، هشتم، دوازدهم و پانزدهم همدیگر را خنثی می‌کنند به نحوی که باعث افزایش احتمال تفاضلی نسبت به ورودی‌های تفاضلی دیگر می‌شود.

جدول ۳. مقایسه تحلیل‌های انجام شده بر روی π-Cipher

نسخه	نوع الگوریتم	نوع تحلیل	تعداد دورها	پیچیدگی زمانی
	π16-cipher96	کشف حالت [۳]	۱	۱
	π16-cipher128			
	π32-cipher128			
	π32-cipher256			
	π64-cipher128			
	π64-cipher256			
$v۱$	π16-cipher96	کشف حالت [۳]	۲	$۲^{۶۶}$ یا $۲^{۱۳۰}$
	π16-cipher128			
	π32-cipher256			
	π32-cipher256	کشف کلید [۴]	۲٫۵	$۲^{۱۳۷}$
	π16-cipher96	کشف حالت [۳]	۳	$۲^{۶۴}$ یا $۲^{۱۲۸}$
	π16-cipher128			
	π32-cipher256			
$v۲$	π16-cipher96	کشف حالت [۳]	۱	$۲^{۶۸}$
	π16-cipher96	کشف کلید [۴]	۲٫۵	$۲^{۷۲}$
	π16-cipher128	کشف کلید [۴]	۲٫۵	$۲^{۷۲}$
	π16-cipher96	تمایزگر	۲	$۲^{۹۵}$

حال برای تامین چنین تفاضلی در ورودی جایگشت π، چه باید کرد؟ فرض کنید r معادل عددی چنین تفاضلی باشد. در مثال ما برای یک بیت تفاضل روی بیت دوازدهم هرکدام از کلمات ۱۶ بیتی دوم، سوم و چهارم قطعه‌ی اول ورودی، خواهیم داشت $r = ۲^{۴} + ۲^{۲۰} + ۲^{۳۶}$. برای تامین تفاضلی با مقدار عددی r با توجه امکان تقریب رفتار جمع پیمانه‌ای با XOR می‌توان از قالب‌های با فواصل r استفاده کرد. تفاضل ورودی بخش نرخ در دو قالب با فاصله r برابر خواهد بود با $(ctr+i+r)\oplus(ctr+i)$ است، که به شرط تقریب جمع پیمانه‌ای با XOR این تفاضل برابر با r خواهد بود. احتمال این پیشامد به وزن همینگ r وابسته است و برای تفاضل مورد بررسی ما برابر با $۲^{-۳}$ خواهد بود. بنابراین احتمال تمایزگر تفاضلی برابر با $۲^{-۹۵} = ۲^{-۳} \cdot ۲^{-۹۲}$ خواهد بود.

خلاصه‌ای از حملات انجام شده روی الگوریتم π-Cipher به همراه حمله معرفی شده در این مقاله در جدول ۳ آورده شده است.

۵ جمع‌بندی

در این مقاله به رفتار تفاضلی جایگشت π که طرحی با ساختار ARX در الگوریتم π-Cipher است پرداختیم. ابتدا رفتار تفاضلی عملگر جمع پیمانه‌ای مورد بررسی قرار گرفت و با در نظر گرفتن احتمال انتشار بیت‌های تفاضل، این عملگر به عملگر یای انحصاری تقریب زده شد. پس از آن عملگر جمع پیمانه‌ای با دو ورودی تفاضلی به عملگر جمع با سه

ورودی تفاضلی تعمیم داده شد. در نهایت، یک تمایزگر تفاضلی بر روی الگوریتم π-Cipher دو دوری و با کلمات ۱۶ بیتی معرفی شد. در تمایزگر مذکور تفاضل روی بیت‌های ورودی جایگشت π منحصرا از قسمت نرخ حالت انتخاب شده‌اند که با توجه به تزریق شمارنده در این قسمت، امکان تنظیم تفاضل‌های دلخواه برای تحلیلگر وجود دارد. به عنوان کارهای آتی می توان روی جستجوی جامع‌تر برای یافتن مشخصه‌های تفاضلی محتمل‌تر و یا بهره‌گیری از این مشخصه برای یک حمله جعل یا بازیابی حالت/کلید استفاده کرد.

مراجع

[1] Caesar: Competition for authenticated encryption: Security, applicability, and robustness. http://competitions.cr.yp.to/.

[2] Danilo Gligoroski, Hristina Mihajloska, Simona Samardjiska, Hakon Jacobsen, Mohamed El-Hadedy, Rune Erlend Jensen, and Daniel Otte. π-cipher v2. 0, submission to the caesar competition, 2015.

[3] Joseph Alley and Josef Pieprzyk. State recovery attacks against π-cipher. In *Proceedings of the Australasian Computer Science Week Multiconference*, pages 1–6, 2016.

[4] Christina Boura, Avik Chakraborti, Gaëtan Leurent, Goutam Paul, Dhiman Saha, Hadi Soleimany, and Valentin Suder. Key recovery attack against 2.5-round π-cipher. In *International Conference on Fast Software Encryption*, pages 535–553. Springer, 2016.

[5] Helger Lipmaa and Shiho Moriai. Efficient algorithms for computing differential properties of addition. In *International Workshop on Fast Software Encryption*, pages 336–350. Springer, 2001.

[6] J. Wallén. *On the differential and linear properties of addition*. PhD thesis, Helsinki University of Technology, Laboratory for Theoretical Computer Science, 2003. Master's thesis.