مجله‌ی علمی و پژوهشی شریف
اسفند ۱۳۸۸، شماره‌ی پنجاه و دوم، ص. ۵۷-۶۱

حمله‌ی تمایز بر نوع ساده‌شده‌ی رمز دنباله‌یی WG-۱۲۸

اعظم شادمان (کارشناس ارشد)
دانشکده‌ی مهندسی برق، دانشگاه صنعتی شریف
جواد مهاجری (کارشناس ارشد)
محمود سلماسی‌زاده (دانشیار)
پژوهشکده‌ی الکترونیک، دانشگاه صنعتی شریف

الگوریتم رمز دنباله‌یی WG (Welch-Gong)، یک الگوریتم رمز با کلیدی با طول متغیر ۸۰، ۹۶، ۱۱۲ و ۱۲۸ بیت است که با هدف شرکت در گروه ۲ پروژه‌ی eSTREAM طراحی شده است. در این نوشتار به تحلیل الگوریتم رمز دنباله‌یی WG-۱۲۸، و بررسی میزان مقاومت آن دربرابر حمله‌ی تمایز مبتنی بر تقریب خطی پرداخته‌ایم. با یافتن یک نقاب خطی مناسب برای بخش غیرخطی WG-۱۲۸، حمله‌ی تمایز به الگوریتم WG-۱۲۸ ساده‌شده (بدون در نظر گرفتن «تابع اثر[۱]») اعمال و نشان داده می‌شود که اعمال این حمله در صورت دسترسی به 2^{32} کلمه‌ی خروجی منجر به تمایز دنباله‌ی کلمات خروجی الگوریتم WG-۱۲۸ ساده‌شده از دنباله‌ی خروجی یک منبع تصادفی می‌شود.

واژگان کلیدی: حمله تمایز، رمزهای دنباله‌یی، تقریب خطی.

shademan@ee.sharif.edu
mohajer@sharif.edu
salmasi@sharif.edu

۱. مقدمه

نیاز به الگوریتم‌های رمز سریع، با پیچیدگی سخت‌افزاری کم‌تر از رمزهای قالبی، باعث پیشرفت‌های چشم‌گیری در زمینه‌ی طراحی رمزهای دنباله‌یی در چند سال اخیر شده است. ازجمله اقدامات تأثیرگذار درخصوص طراحی و تحلیل الگوریتم‌های رمز دنباله‌یی امن و کارآمد، می‌توان به اقدام قطب علمی رمزنگاری اروپا (ECRYPT[۲]) در نوامبر سال ۲۰۰۴، مبنی بر انتشار فراخوانی تحت عنوان eSTREAM به‌منظور مدیریت و هماهنگ‌سازی تلاش‌های چندین‌ساله برای طراحی رمزهای دنباله‌یی مناسب اشاره کرد.[۱] الگوریتم‌های ارائه‌شده به eSTREAM در دو گروه تقسیم‌بندی می‌شوند:

۱. الگوریتم‌های رمز دنباله‌یی مناسب برای پیاده‌سازی نرم‌افزاری؛

۲. الگوریتم‌های رمز دنباله‌یی مناسب برای پیاده‌سازی سخت‌افزاری با منابع محدود (از قبیل حافظه، تعداد دروازه‌ها[۳] یا توان مصرفی).

در ابتدا عملکرد بسیاری از الگوریتم‌های رمز دنباله‌یی مبتنی بر بیت بود که با توجه به فنّاوری آن دوره، هزینه‌ی پیاده‌سازی سخت‌افزاری آنها (تعداد دروازه‌های مورد نیاز) بسیار پایین بود. پیشرفت در فنّاوری ساخت تراشه‌های الکترونیکی و افزایش کاربردهای نرم‌افزاری، امکان طراحی الگوریتم‌هایی با ساختار مبتنی برکلمه را فراهم ساخت. الگوریتم‌های رمز دنباله‌یی SNOW، PANAMA و SEAL،[۲-۴] ازجمله الگوریتم‌هایی هستند که ساختار آنها مبتنی برکلمه است. ساختار اصلیِ بسیاری از الگوریتم‌های رمز دنباله‌یی، ثبات انتقال با پسخورد خطی (LFSR[۴]) است که خروجی آنها، از نظر آماری ویژگی‌های خوبی دارد.

تاریخ: دریافت ۱۳۸۸/۳/۱۸، داوری ۱۳۸۸/۹/۸، پذیرش ۱۳۸۸/۱۲/۲.

الگوریتم رمز دنباله‌یی WG یکی از الگوریتم‌های ارائه‌شده به eSTREAM است که به‌منظور رقابت با الگوریتم‌های گروه ۲ (مناسب برای پیاده‌سازی سخت‌افزاری) طراحی شده است. این الگوریتم به فاز دوم eSTREAM راه یافت ولی به‌دلیل پیچیدگی خطیِ کمِ دنباله‌ی کلید اجرایی و پیچیدگی زیاد پیاده‌سازی سخت‌افزاری، جزء ۸ الگوریتم راه‌یافته از گروه ۲ به فاز سوم قرار نگرفت. الگوریتم رمز دنباله‌یی WG ازجمله الگوریتم‌های مبتنی برکلمه با ساختاری براساس LFSR است که خروجی آن از توابع غیر خطی عبور می‌کند و دنباله‌ی کلید اجرایی تولید می‌شود.[۵]

۱.۱. کارهای مرتبط

تاکنون حمله‌ی تمایزی[۵] بر خانواده‌ی WG اعمال نشده است. تنها حمله‌ی صورت گرفته بر این خانواده، حمله‌یی از نوع حملات مقدار اولیه‌ی منتخب[۶] است که بر WG-۸۰ اعمال شده است.[۶] اعمال این حمله بر نسخه‌ی WG-۸۰ با مقدار اولیه‌ی ۸۰ بیتی، با حدود $2^{31.3}$ مقدار اولیه‌ی منتخب متفاوت، منجر به بازیابی ۴۸ بیت ازکلید با احتمال $2^{-8.7}$ می‌شود. همچنین با اعمال این حمله بر نسخه‌ی WG-۸۰ با مقدار اولیه‌ی ۶۴ بیتی، با حدود $2^{25.1}$ مقدار اولیه‌ی منتخب متفاوت، ۲۹ بیت ازکلید با احتمال 2^{-5} قابل بازیابی است.[۶و۷]

پس از معرفی این حمله، طراحان WG تنها با افزایش تعداد مراحل بارگذاری کلید و مقدار اولیه، از ۲۲ دور به ۴۴ دور و بدون هرگونه تغییر دیگری در ساختار الگوریتم، تلاش کردند امکان اعمال حمله‌ی مقدار اولیه‌ی منتخب به WG را از میان ببرند.[۸]

۲.۱. نوآوری

در این نوشتار میزان مقاومت الگوریتم WG-۱۲۸ با طول بارگذاری ۴۴ دور، در برابر حمله‌ی تمایز مبتنی بر تحلیل خطی بررسی و نشان داده شده است که می‌توان با یافتن یک نقاب[۷] خطی مناسب برای بخش غیرخطی WG-۱۲۸ با اریبی[۸] (فاصله‌ی احتمال رویداد رابطه‌ی خطی یافت‌شده از $\frac{1}{2}$) 2^{-1}، حمله‌ی تمایز به الگوریتم WG-۱۲۸ ساده‌شده (بدون در نظرگرفتن «تابع اثر») را با موفقیت اعمال کرد. این حمله منجر به تمایز بین دنباله‌ی کلمات خروجی الگوریتم WG-۱۲۸ و دنباله‌ی خروجی یک منبع تصادفی می‌شود. در ادامه‌ی این نوشتار، در بخش ۲ به معرفی حملات مختلف بر الگوریتم‌های رمز دنباله‌یی، به‌ویژه حمله‌ی تمایز، می‌پردازیم. در بخش ۳ نیز خانواده‌ی WGمعرفی خواهد شد. سپس حمله‌ی تمایز اعمال‌شده به الگوریتم WG-۱۲۸ را در بخش ۴ تشریح کرده و نهایتاً نتایج حاصل از اعمال حمله در بخش ۵ ارائه می‌شود.

۲. انواع حملات

حملات علیه رمزهای دنباله‌یی براساس میزان اطلاعات در دسترس، هدف حمله و یا روش حمله تقسیم‌بندی می‌شوند. معمولاً فرض بر این است که حمله‌کننده الگوریتم رمز را می‌داند اما به کلید دسترسی ندارد. حملات براساس هدف حمله با فرض متن اصلی معلوم به سه دسته تقسیم می‌شوند:

۱. بازیابی کلید[۹]: حملاتی که هدف از آنها استخراج کلید یا بخشی از آن است.

۲. پیش‌گویی[۱۰]: حملاتی که در آنها سعی می‌شود یک بیت یا دنباله‌یی از بیت‌های کلید با احتمال زیاد پیش‌گویی شود.

۳. تمایز: حملاتی که براساس روش‌های آماری برای تمایز دنباله‌ی کلید اجرایی از یک دنباله‌ی تصادفی به کار می‌روند. در این نوشتار تمرکز روی این حمله است.

۱.۲. حمله‌ی تمایز

یکی از حملاتی که به الگوریتم‌های رمز دنباله‌یی اعمال می‌شود «حمله‌ی تمایز» است. حمله‌ی تمایز حمله‌یی است که در آن دنباله‌ی خروجی یک الگوریتم رمز از یک دنباله‌ی تصادفی با احتمال غیر قابل چشم‌پوشی تمیز داده می‌شود. لازم به ذکر است که به‌لحاظ نظری اعمال حمله‌ی تمایز به هر الگوریتم رمز با طول کلید محدود امکان‌پذیر است زیرا به هر الگوریتم رمز با طول کلید k بیت، می‌توان با پیچیدگی 2^k و جست‌وجوی فراگیرِ فضای کلید مشخص کرد که دنباله‌ی در دسترس، خروجیِ الگوریتمِ رمزِ مورد نظر هست یا خیر.

درمورد حمله‌ی تمایز این نکته قابل ذکر است که اعمال حمله‌ی تمایز، بستگی به طول دنباله‌ی خروجیِ در دسترس از الگوریتم مورد نظر دارد و به طول کلید الگوریتم وابسته نیست. در واقع در این حمله با تحلیل آماریِ دنباله‌ی خروجی، مشخص می‌شود که دنباله‌ی در دسترس، خروجی یک منبع کاملاً تصادفی است یا خروجی الگوریتم رمز مورد نظر. توجه به این نکته ضروری است که هدف از حمله‌ی تمایز بازیابی کلید یا حالت اولیه‌ی الگوریتم رمز دنباله‌ای نیست. بلکه تنها ویژگی‌های دنباله‌ی تولیدشده از نظر تطابق با ویژگی‌های مورد انتظار برای یک دنباله‌ی کاملاً تصادفی سنجیده می‌شود؛ لذا اعمال این حمله به طول زیادی از دنباله‌ی کلید ـ بسته به قدرت الگوریتم ـ نیاز دارد. توجه به این نکته ضروری است که با وجود آن که به‌دلیل عدم ارتباط مشخص بین طول دنباله‌ی خروجی و مقدار کلید، اعمال موفق این حمله لزوماً منجر به کسب اطلاعاتی درمورد کلید نمی‌شود، ولی نشان‌گر وجود یک نقطه ضعف در الگوریتم و عدم ارضای یکی از شرایط لازم برای الگوریتم‌های رمز بوده که در شرایطی می‌تواند موجب نشت اطلاعات ناخواسته برای دشمن شود و استفاده از الگوریتم تحلیل‌شده را با تردید مواجه سازد.[۹] تاکنون حمله‌ی تمایز به الگوریتم‌های رمز دنباله‌یی متعددی مانند SNOW۱، SNOW۲، SOBER-۱۲۸ و DRAGON اعمال شده است.[۱۰-۱۳]

۳. خانواده‌ی WG

الگوریتم WG، الگوریتمی مبتنی بر کلمه است که در میدان متناهی با 2^{29} عنصر تعریف شده است. نمادهای استفاده شده در این مقاله در بخش ۱.۳. ارائه می‌شود.

۱.۳. نمادگذاری و تعاریف اولیه

در این بخش از تعاریف و نمادهای زیر استفاده شده است:

$F_2 = GF(2)$: یک میدان متناهی با دو عنصر صفر و یک؛

$F_{2^n} = GF(2^n)$: بسط میدان $GF(2)$ با 2^n عنصر؛

F_2^n: یک فضای برداری n بعدی روی میدان $GF(2)$؛

تابع اثر: برای مقادیر صحیح مثبت n و m، که در آن $m|n$، تابع اثر $Tr_n^m(x)$ از F_{2^n} به F_{2^m} مطابق رابطه‌ی ۱ تعریف می‌شود:

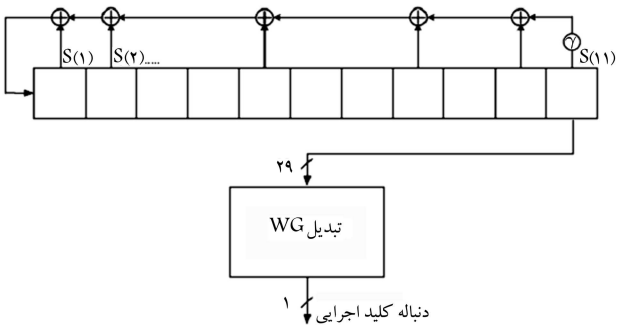
$$Tr_n^m(x) = \sum_{i=0}^{(n/m)-1} x^{2^{mi}}, x \in F_{2^n} \qquad (1)$$

پایه‌های چندجمله‌یی: اگر F_{2^m} میدانی متناهی و α یک ریشه از چندجمله‌یی اولیه[۱۱]یی باشد که F_{2^m} را تولید می‌کند، آنگاه $\{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$ پایه‌ی چندجمله‌یی F_{2^m} روی F_2 نامیده می‌شود.

پایه‌ی نرمال: اگر F_{2^m} یک میدان متناهی و γ یک عنصر از F_{2^m} باشد به‌طوری که $\{\gamma, \gamma^{2^1}, \gamma^{2^2}, ..., \gamma^{2^{m-1}}\}$ یک پایه از F_{2^m} روی میدان F_2 باشد، آنگاه $\{\gamma, \gamma^{2^1}, \gamma^{2^2}, ..., \gamma^{2^{m-1}}\}$ پایه‌ی نرمال F_{2^m} روی F_2 نامیده می‌شود.

۲.۳. ساختار خانواده‌ی WG

هر الگوریتم رمز دنباله‌یی از خانواده‌ی WG، شامل یک مولد دنباله‌ی شبه‌تصادفی (دنباله‌ی کلید) است. این دنباله‌ی کلید با متن اصلی در پیمانه ۲ جمع شده و متن رمزشده را ایجاد می‌کند. مولد دنباله‌ی کلید WG از یک ثبات انتقال با پسخورد خطی به‌طول L با چندجمله‌یی پسخورد اولیه روی F_{2^n} و از یک تبدیل Welch-Gong (WG) به‌عنوان تابع فیلتر تشکیل شده است. تبدیل WG برگرفته از تبدیل معرفی‌شده توسط محققین در سال ۱۹۹۸ است.[۱۴] این مولد، یک دنباله‌ی کلید با دوره‌ی تناوب $2^m - 1$ تولید می‌کند که در آن $m = nL$ است. این دنباله متوازن است و خودهم‌بستگی[۱۲] دوسطحی دارد. پیچیدگی خطی دنباله‌ی WG به‌صورت نمایی با n افزایش می‌یابد و هم‌بستگی متقابل[۱۳] آن سه سطح دارد. به‌علاوه اگر پایه‌های به کار رفته در محاسبات F_{2^n} به‌درستی انتخاب شوند، دنباله‌ی خروجی تبدیل WG، هیچ هم‌بستگی با ورودی آن نخواهد داشت.[۱۵]



شکل ۱. نمودار قالبی مولد دنباله‌ی کلید WG.[۵]

۳.۳. ساختار الگوریتم WG-۱۲۸

WG یک رمز دنباله‌یی با کلیدهایی به طول‌های ۸۰، ۹۶، ۱۱۲ و یا ۱۲۸ بیت است. همچنین یک بردار اولیه (IV) ۳۲ یا ۶۴ بیتی نیز به‌همراه هریک از کلیدهای یادشده به‌منظور افزایش امنیت استفاده می‌شود. شمای کلی الگوریتم‌های خانواده‌ی WG در شکل ۱ نشان داده شده است. الگوریتم WG- ۱۲۸ شامل یک ثبات انتقال خطی (LFSR) روی میدان $F_{۲^{۲۹}}$ است. دنباله‌ی تولیدشده توسط ثبات انتقال، به‌وسیله‌ی تبدیل غیرخطی WG فیلتر می‌شود. همه‌ی عناصر $F_{۲^{۲۹}}$ و محاسبات میدان برحسب پایه‌های نرمال نمایش داده می‌شوند.[۱۵،۵] چندجمله‌یی پسخورد LFSR در رابطه‌ی ۲ تعریف شده است:

$$p(x) = x^{۱۱} + x^{۱۰} + x^{۹} + x^{۶} + x^{۳} + x + \gamma \qquad (۲)$$

که در آن $\gamma = \beta^{۴۶۴۷۳۰۰۷۷}$ و β ریشه‌ی چندجمله‌یی اولیه $g(x)$ به‌عنوان چندجمله‌یی مولد $F_{۲^{۲۹}}$ روی $F_۲$ بوده که در رابطه‌ی ۳ تعریف شده است:

$$g(x) = x^{۲۹} + x^{۲۸} + x^{۲۴} + x^{۲۱} + x^{۲۰} + x^{۱۹} + x^{۱۸} + x^{۱۷} + x^{۱۴} + x^{۱۲} + x^{۱۱} + x^{۱۰} + x^{۷} + x^{۶} + x^{۴} + x + ۱ \qquad (۳)$$

اگر $t(x)$ یک چندجمله‌یی روی میدان $F_{۲^{۲۹}}$ باشد که در رابطه‌ی ۴ تعریف شده است:

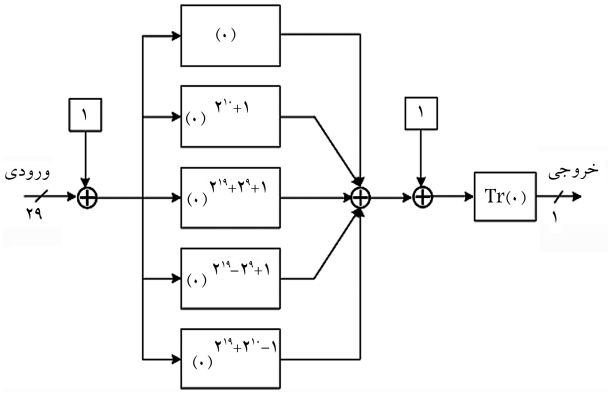
$$t(x) = x + x^{۲^{۱۰}+۱} + x^{۲^{۱۹}+۲^{۹}+۱} + x^{۲^{۱۹}-۲^{۹}+۱} + x^{۲^{۱۹}+۲^{۱۰}-۱}, \quad x \in F_{۲^{۲۹}} \qquad (۴)$$

آنگاه تابع غیر خطی اعمال‌شده بر دنباله‌ی خروجی LFSR الگوریتم WG، به‌صورت رابطه‌ی ۵ تعریف می‌شود:

$$f(x) = Tr(t(x+۱)+۱), \qquad x \in F_{۲^{۲۹}} \qquad (۵)$$

که در آن $Tr(\alpha) = \sum_{i=۰}^{۲۸} \alpha^{۲^i}$، یک تبدیل از $F_{۲^{۲۹}}$ به $F_۲$ است. تابع $f(x)$ در شکل ۲ نشان داده شده است. ۲۹ بیت ورودی WG به‌عنوان عنصری در $F_{۲^{۲۹}}$ در نظرگرفته شده و برحسب پایه‌ی نرمال نشان داده می‌شود. عناصر پایه‌ی نرمال $F_{۲^{۲۹}}$ که توسط $g(x)$ تعریف و به‌وسیله‌ی عنصر $\gamma \in F_{۲^{۲۹}}$ تولید می‌شوند عبارت‌اند از: $\{\gamma, \gamma^{۲}, \gamma^{۲^۲}, ..., \gamma^{۲^{۲۸}}\}$. با استفاده از پایه‌ی نرمال می‌توان محاسبات WG را چنین ساده کرد:

- اگر عناصر برحسب پایه‌های نرمال نشان داده شوند، توان‌رسانی با انتقال چرخشی به سمت راست انجام می‌شود. به‌عبارت دیگر، اگر $x \in F_{۲^{۲۹}}$ به‌صورت یک بردار ۲۹ بیتی نمایش داده شود، آنگاه $x^{۲^i}$ با i بیت انتقال چرخشی بیت‌های x به سمت راست به‌دست می‌آید.
- اگر γ مولد پایه‌ی نرمال باشد، آنگاه $\sum_{i=۰}^{۲۸} \gamma^{۲^i} = ۱$، یک بردار ۲۹ بیتی تمام یک است. بنابراین حاصل جمع هر عنصر میدان با یک، برحسب پایه‌های نرمال، به‌آسانی با معکوس‌کردن بیت‌های آن عنصر به‌دست می‌آید.
- مقدار تابع اثر همه‌ی عناصر پایه‌ی نرمال برابر ۱ است، یعنی $Tr(\gamma^{۲^i}) = ۱$، $۰ \le i \le ۲۸$. درنتیجه تابع اثر هر عنصر میدان که به‌صورت یک بردار ۲۹ بیتی است، با جمع بیت‌های آن عنصر در $F_۲$، XOR، محاسبه می‌شود.[۵]



شکل ۲. نمودار قالبی تبدیل WG: $F_{۲^{۲۹}} \to F_۲$.[۵]

۴.۳. امنیت الگوریتم WG-۱۲۸

دنباله‌ی تولیدشده به‌وسیله‌ی الگوریتم WG-۱۲۸ متوازن بوده و دوره‌ی تناوب آن $۲^{۳۱۹} - ۱$ است. خودهم‌بستگی آن دو سطح دارد و پیچیدگی خطیِ دنباله‌ی کلید $۲^{۴۵٫۰۴۱۵}$ است. مرتبه‌ی غیرخطی تبدیل WG برابر $۲^{۱۴} - ۲^{۲۸}$ است. اندازه‌ی حالت داخلی WG، ۳۱۹ بیت است که از دو برابر طول کلید بیشتر و درنتیجه در برابر حمله‌ی بده ـ بستان زمان/حافظه/داده مقاوم است. همچنین طراحان این الگوریتم مدعی‌اند که این الگوریتم در برابر حمله‌ی جبری و هم‌بستگی نیز امن است.[۱۵]

۴. اعمال حمله‌ی تمایز به الگوریتم رمز دنباله‌یی WG-۱۲۸

در این بخش به تشریح یک حمله‌ی تمایز جدید به نسخه‌ی ساده‌شده‌یی از الگوریتم WG-۱۲۸ می‌پردازیم. برای اعمال این حمله، تابع اثر را حذف، و فرض می‌کنیم حمله‌کننده به دنباله‌ی کلمات ۲۹ بیتی قبل از تابع اثر، دسترسی دارد. لازم به ذکر است که تابع اثر، ۲۹ بیت هر کلمه را با یکدیگر در پیمانه ۲ جمع کرده و درنتیجه خروجی الگوریتم، بیت‌به‌بیت تولید می‌شود که منجر به کاهش سرعت تولید دنباله‌ی کلید اجرایی خواهد شد.

در بسیاری از موارد، حمله‌ی تمایز به الگوریتم‌های رمز دنباله‌یی ساده‌شده اعمال شده است. در این حملات با در نظرگرفتن برخی فرضیات، امکان اعمال حمله‌ی تمایز با اریبی مناسب، افزایش یافته است. به‌عنوان مثال، در سال ۲۰۰۲ حمله‌ی تمایز مبتنی بر خطی‌سازی، صرف‌نظر از تابع stuttering که باعث توزیع غیریکنواخت دنباله‌ی خروجی می‌شود، بر SOBER۳۲ اعمال شد.[۸] ما نیز در این حمله فرض می‌کنیم به دنباله‌ی‌بیت قبل از تابع اثر دسترسی داریم.

۱.۴. ویژگی های آماری الگوریتم ساده‌شده در مقایسه با الگوریتم اصلی

چنان‌که پیش‌ترگفته شد، در الگوریتم ساده‌شده دنباله‌ی بیت‌های خروجی را قبل از تابع اثر در نظر می‌گیرند. لازم به ذکر است که حذف تابع اثر بر دوره‌ی تناوب دنباله‌ی خروجی تأثیری ندارد و باعث تخریب خواص تصادفی‌بودن دنباله‌ی خروجی نیز نمی‌شود. به‌منظور بررسی این ادعا، دنباله‌ی خروجی الگوریتم WG-۱۲۸ قبل از تابع اثر را از تعدادی از آزمون‌های آماری عبور می‌دهیم تا مطمئن شویم که با حذف تابع اثر نمی‌توان با اعمال آزمون‌های آماری رایج، بین دنباله‌ی بیت حاصل از الگوریتم ساده‌شده‌ی WG-۱۲۸ و دنباله‌ی بیت تصادفی تمایز قائل شد. در این بررسی آزمون‌های سریال، فرکانس، روها[14]، پوکر و هم‌بستگی روی دنباله‌ی خروجی اعمال شد. چنان‌که در جدول ۱ مشاهده می‌شود، بیت‌های خروجی با موفقیت از آزمون‌های آماری عبورکرده و درنتیجه اعمال حمله‌ی تمایز از طریق اعمال آزمون‌های آماری متداول ممکن نیست.

۲.۴. روش حمله

دراین بخش روش ساخت تمایزگر[15] برای اعمال حمله‌ی تمایز برالگوریتم WG-۱۲۸ بررسی می‌شود.

۱.۲.۴. تحلیل LSFR

چندجمله‌یی پسخورد LFSR به‌کار رفته در WG-۱۲۸ در رابطه‌ی ۲ معرفی شد. برای تسهیل در اعمال حمله‌ی تمایز به WG-۱۲۸ باید همه‌ی ضرایب این چندجمله‌یی ۰ و ۱ باشد. به‌منظور حذف $\gamma \in F_{۲^{۲۹}}$ از رابطه‌ی مزبور، می‌توان $P(x)$ را به توان $۲^{۲۹}$ رساند. توان‌رسانی‌های مکرر تأثیری در رابطه‌ی بازگشتی WG-۱۲۸ ندارد و این رابطه همچنان معتبر باقی خواهد ماند.

$$p(x)^{۲^{۲۹}} = x^{۱۱\times ۲^{۲۹}} + x^{۱۰\times ۲^{۲۹}} + x^{۹\times ۲^{۲۹}} + x^{۶\times ۲^{۲۹}} + x^{۳\times ۲^{۲۹}} + x^{۲^{۲۹}} + \gamma^{۲^{۲۹}} \quad (۶)$$

از آنجا که $\gamma \in F_{۲^{۲۹}}$ آنگاه $\gamma = \gamma^{۲^{۲۹}}$. از جمع روابط ۲ و ۶، رابطه‌ی ۷ حاصل می‌شود:

$$p(x) + p(x)^{۲^{۲۹}} = x^{۱۱\times ۲^{۲۹}} + x^{۱۰\times ۲^{۲۹}} + x^{۹\times ۲^{۲۹}} + x^{۶\times ۲^{۲۹}} + x^{۳\times ۲^{۲۹}} + x^{۲^{۲۹}} + x^{۱۱} + x^{۱۰} + x^{۹} + x^{۶} + x^{۳} + x \quad (۷)$$

که در آن پس از حذف γ، یک رابطه‌ی خطی با ۱۲ جمله باقی می‌ماند. با تقسیم رابطه‌ی ۷ به x، رابطه‌ی بازگشتی ۸ حاصل می‌شود:

$$S_{t+\tau_۱} + S_{t+\tau_۲} + S_{t+\tau_۳} + S_{t+\tau_۴} + S_{t+\tau_۵} + S_{t+\tau_۶} + S_{t+\tau_۷} + S_{t+\tau_۸} + S_{t+\tau_۹} + S_{t+\tau_{۱۰}} + S_{t+\tau_{۱۱}} + S_{t+\tau_{۱۲}} = ۰ \quad (۸)$$

که در آن $\tau_۱ = ۰$ ، $\tau_۲ = ۲$، $\tau_۳ = ۵$، $\tau_۴ = ۸$، $\tau_۵ = ۹$، $\tau_۶ = ۱۰$، $\tau_۷ = ۲^{۲۹} - ۱$، $\tau_۸ = ۳\times ۲^{۲۹} - ۱$، $\tau_۹ = ۶\times ۲^{۲۹} - ۱$، $\tau_{۱۰} = ۹\times ۲^{۲۹} - ۱$، $\tau_{۱۱} = ۱۰\times ۲^{۲۹} - ۱$، $\tau_{۱۲} = ۱۱\times ۲^{۲۹} - ۱$ است. رابطه‌ی خطی ۸ برای هر بیت ازکلمه‌ی خروجی به طور جداگانه برقرار است.

۲.۲.۴. تقریب خطی WG-۱۲۸ ساده‌شده

برای تقریب بخش غیرخطی، از روش نقاب‌گذاری استفاده می‌کنیم. اولین قدم در روش نقاب‌گذاری، انتخاب چندین بیت از ورودی، خروجی، کلید ثابت و سپس ترکیب خطی آنها به‌گونه‌یی است که اریبی ترکیب خطی که تنها شامل بیت‌های خروجی است به‌اندازه‌ی کافی بزرگ باشد. اگر ترکیب خطی به‌دست آمده با اریبی ε برقرار باشد، حدود $\varepsilon^{-۲}$ کلمه‌ی خروجی برای تمایز بین خروجی الگوریتم از یک دنباله‌ی بیت کاملاً تصادفی مورد نیاز است. این مقدار باید از فضای جست‌وجوی کامل کلید کم‌تر باشد تا حمله‌ی تمایز موفق تلقی شود. بنابراین مسئله‌ی مهم، یافتن تقریب خطی با بالاترین اریبی ممکن است.

بخش غیرخطی الگوریتم رمزی WG-۱۲۸ بدون احتساب تابع رد با رابطه‌ی ۹ قابل توصیف است:

$$h(x) = t(x+۱) + ۱, \qquad x \in F_{۲^{۲۹}} \quad (۹)$$

برای خطی‌سازی رابطه‌ی ۹ باید نقاب λ چنان باشد که رابطه‌ی $\lambda.h(x) = \lambda.x$ با بالاترین اریبی ممکن برقرار باشد که در آن $\lambda.x$ مبین ضرب داخلی λ و x است. از آنجا که $\lambda \in F_{۲^{۲۹}}$، امکان جست‌وجوی همه‌ی حالت‌های موجود امکان‌پذیر نیست. بنابراین حالت‌های مختلف با وزن همینگهای متفاوت شبیه‌سازی شد. جدول ۲ نمونه‌یی از نقاب‌های مختلف و اریبی مربوط به آنها را نشان می‌دهد.

همان‌طور که در جدول ۲ مشاهده می‌شود، تابع $h(x)$ در بیت‌های کم‌ارزش (LSB) بسیار ضعیف عمل می‌کند، به‌طوری که با قرار دادن $\lambda = ۰۰۰۰۰۰۰۷$ رابطه‌ی $\lambda.h(x) = \lambda.x$ با اریبی بسیار خوبی برقرار است. بنابراین اگر خروجی تابع $h(x)$ را z بنامیم، با توجه به این‌که ورودی $h(x)$، $S(۱۱)$ است، رابطه‌ی ۱۰ به دست می‌آید:

$$S(۱۱)_۰ \oplus S(۱۱)_۱ \oplus S(۱۱)_۲ = z_۰ \oplus z_۱ \oplus z_۲ \quad (۱۰)$$

اندیس i در z_i و $S(۱۱)_i$ بیان‌گر موقعیت بیت است. با توجه به رابطه‌ی $p = \frac{۱}{۲} + \varepsilon$ رابطه‌ی ۱۰ با اریبی $۲^{-۱}$ برقرار است. با جایگذاری رابطه‌ی ۱۰ در رابطه‌ی خطی

جدول ۱. نتایج آزمون‌های آماری استاندارد اعمال شده بر الگوریتم WG-۱۲۸ ساده شده.

نام آزمون	آزمون فرکانس	آزمون سریال	آزمون پوکر	آزمون روها	آزمون هم بستگی
درصد موفقیت	٪۹۵	٪۹۵	٪۹۵	٪۱۰۰	٪۹۸

جدول ۲. نقاب‌های اعمال شده به تابع $h(x)$.

نقاب	احتمال
۰۰۰۳۰۰۰۳	$۱/۲ - ۶/۴۸E-۰۵$
۰۰۰۸۳۰۰۰	$۱/۲ - ۱/۹۱E-۰۵$
۰۰۰۱۸۰۰۱	$۱/۲ - ۲/۲۹E-۰۵$
۰۳۰۳۶۰۰c	$۱/۲ - ۳/۴۳E-۰۵$
۰۰۰a۰۱۰۱	$۱/۲ - ۲/۲۹E-۰۵$
۰۰۵۰۰۰۰	$۱/۲ + ۱/۵۳E-۰۵$
۰۰۰۰۰۰۰f	$۱/۲ + ۷/۶۳E-۰۶$
۰۸۰۸۰۰۰۳	$۱/۲ - ۱/۵۳E-۰۵$
۰ffffff۰	$۱/۲ - ۲/۶۷E-۰۵$
۰۰۰۰۰۰۰۷	$۱/۲ + ۰/۵$

۸، به رابطه‌ی ۱۱ براساس بیت‌های خروجی دست می‌یابیم:

$$S(11+\tau_1)_0 \oplus S(11+\tau_2)_0 \oplus S(11+\tau_3)_0 \oplus ... \oplus S(11+\tau_{12})_0$$
$$\oplus S(11+\tau_1)_1 \oplus S(11+\tau_2)_1 \oplus S(11+\tau_3)_1 \oplus ... \oplus S(11+\tau_{12})_1$$
$$\oplus S(11+\tau_1)_2 \oplus S(11+\tau_2)_2 \oplus S(11+\tau_3)_2 \oplus ... \oplus S(11+\tau_{12})_2$$
$$= z(\tau_1)_0 \oplus z(\tau_1)_1 \oplus z(\tau_1)_2 \oplus ... \oplus z(\tau_{12})_0 \oplus z(\tau_{12})_1 \oplus z(\tau_{12})_2 = 0 \quad (11)$$

هر سطر از سمت چپ رابطه‌ی ۱۱، معادل با یک رابطه‌ی بازگشتی از ثبات انتقال خطی است. بنابراین می‌توان نتیجه گرفت که حاصل هر سطر از سمت چپ رابطه‌ی ۱۱ طبق رابطه‌ی ۸ برابر صفر است. بنابراین سمت چپ رابطه‌ی ۱۱ مساوی صفر می‌شود و تنها سمت راست آن که براساس کلمات خروجی بیان شده است، باقی می‌ماند. درنتیجه تمایزگر $\oplus_{t=\tau_1}^{\tau_{12}} (z_0 \oplus z_1 \oplus z_2)$ با اریبی $2^{-1} = (2^{-1})^{12} \cdot 2^{12-1}$ (و به‌عبارت دیگر با احتمال $p = \frac{1}{2} + \varepsilon = \frac{1}{2} + \frac{1}{2}$) برقرار است. بنابراین به‌منظور اعمال این حمله با توجه به رابطه‌ی ۸ فقط حدود $11 \times 2^{29} - 1 = 2^{32}$ کلمه خروجی لازم است تا رابطه‌ی مزبور برآورده شود؛ این مقدار بسیار کوچک‌تر از فضای جست‌وجوی کلید (یعنی 2^{64} کلمه) است. از طرفی با توجه به این که احتمال برقراری رابطه‌ی ۱۱، با توجه به نقاب تعریف‌شده در جدول ۲ و اریبی 2^{-1}، برابر با ۱ است، امکان یافتن نقاب با اریبی بالاتر وجود ندارد و درنتیجه این نقاب، بهترین نقاب ممکن برای اعمال حمله‌ی تمایز بر الگوریتم WG-128 ساده‌شده است.

۵. نتیجه گیری

در این مقاله، با یافتن یک نقاب خطی مناسب برای بخش غیرخطی WG-128، حمله‌ی تمایز به الگوریتم WG-128 ساده شده (بدون در نظرگرفتن تابع اثر) اعمال شد که درصورت دسترسی به 2^{32} کلمه خروجی منجر به ساخت تمایزگری با احتمال ۱ می‌شود. لازم به ذکر است که اعمال آزمون‌های آماری متداول بر دنباله‌های خروجی الگوریتم ساده‌شده‌ی WG-128 نشان می‌دهد که حذف تابع اثر موجب پیدایش رفتار غیرتصادفی در دنباله‌ی بیت‌های حاصل از الگوریتم ساده‌شده WG-128 نمی‌شود.

پانوشت

1. trace function
2. european network of excellence for cryptology
3. gate
4. linear feadback shift register
5. distinguishing attack
6. chosen IV
7. mask
8. bias
9. key recovery
10. prediction
11. primitive polynomial
12. autocorrelation
13. cross correlation
14. run
15. elistinyuisher

منابع

1. Available at http.//www.ecrypt.eu.org/2009.
2. Ekdahl, P., and Johansson, T. "SNOW-a new stream cipher", First Open NESSIE Workshop, (2000); Available at http.// www.it.lth.se / cryptology/snow/2008.
3. Daemen, J., and Clapp, C. "Fast hashing and stream encryption with panama", Fast Software Encryption-FSE'1998, LNCS 1372, pp. 60-74, Springer-Verlag (1998).
4. Rogaway, P., and Coppersmith, D. "A software-optimized encryption algorithm", Fast Software Encryption-FSE'1994, LNCS 809, pp. 56-63, Springer-Verlag (1994).
5. Nawaz, Y., Gong, G. "WG, a family of stream ciphers with designed randomness properties", *Information Sciences*, **178**(7), pp. 1903-1916 (2008).
6. Wu, H., and Preneel, B. "Resynchronization attacks on WG and LEX", Fast Software Encryption-FSE'2006, LNCS 4047, PP. 422-432, Springer-Verlag (2006).
7. Wu, H. "Cryptanalysis and design of stream ciphers", A PhD thesis of Katholieke Universiteit Leuven, Belgium (2008).
8. Nawaz, Y., and Gong, G. "Preventing chosen IV attack on WG cipher by increasing the length of key/IV setup", ECRYPT Stream Cipher Project Report 2005/033; Available at http.//www.ecrypt.eu.org/stream/2008.
9. Rose, G., and Hawkes, P. "On the applicability of distinguishing attacks against stream ciphers", Third Nessie Workshop, Technical report, QUALCOMM Australia (2002).
10. Coppersmith, D.; Halevi, S., and Julta, C. "Cryptanalysis of stream ciphers with linear masking", Advances in Cryptology-Crypto'2002, LNCS 2442, pp. 515-532, Springer-Verlag (2002).
11. Nyberg, K., and Wallen, J. "Improved linear distinguishers for SNOW 2.0", Fast Software Encryption-FSE'2006, LNCS 4047, pp. 144-162, Springer-Verlag (2006).
12. Yeon Cho, J., and Pieprzyk, J. "Distinguishing attack on SOBER-128 with linear masking", Information Security and Privacy, LNCS 4058, pp. 29-39, Springer-Verlag (2006).
13. Englund, H., and Maximov, A. "Attack the DRAGON", Progress in Cryptology INDOCRYPT'2005, LNCS 3797, pp. 130–142, Springer-Verlag (2005).
14. No, J.S.; Golomb, S.W.; Gong, G.; Lee, H.K., and Gaal, P. "Binary pseudorandom sequences of period $2^n - 1$ with ideal correlation properties", *IEEE Transactions on Information Theory*, **44**(2), pp. 814-817 (1998).
15. Nawaz, Y. "Design of stream ciphers and cryptographic properties of nonlinear functions", A PhD Thesis of University of Waterloo, Ontario, Canada (2007).