

بهبود حمله حدس و تعیین اکتشافی به سامانه‌های SNOW1.0 و TIPSY

محمد صادق نعمتی نیا^۱, ترانه اقلیدس^۲ و علی پاینده^۳

^۱مجتمع فن آوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران، ایران
^۲پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

چکیده

حملات حدس و تعیین از جمله حملات عام به سامانه‌های رمز جریانی است. این حملات به دو دسته حملات حدس و تعیین اقتضایی و اکتشافی تقسیم‌بندی می‌شوند. مزیت روش اکتشافی نسبت به روش اقتضایی در قدرت تحلیل و ارائه الگوریتمی برای دسته بزرگی از رمزهای جریانی با فرض یکسان بودن اندازه متغیرها است. در این مقاله از معادلات فرعی علاوه بر معادلات اصلی به عنوان ورودی حمله SNOW 1.0 استفاده شده است. بر اساس مفهوم پایه حدس تعداد حدس و تعیین اکتشافی برای حمله به سامانه‌های رمز جریانی TIPSY و SNOW 1.0 ایجاد شده است. بر اساس مفهوم پایه حدس تعیین اکتشافی بهبودیافته به سامانه TIPSY، شش مورد است: اما پیچیدگی حمله حدس و تعیین اکتشافی بهبودیافته از O(2⁹⁶) به O(2¹⁰²) کاهش یافته است. این پیچیدگی با پیچیدگی حمله اقتضایی برابر است؛ ولی حمله پیشنهادی، اندازه پایه حدس را از هفت به شش بهبود داده است. همچنین، در حمله حدس و تعیین به 1.0 SNOW پیچیدگی حمله اکتشافی با پایه حدس با اندازه شش و اقتضایی با اندازه هفت به ترتیب (O(2²⁰²) و بوده (O(2²²⁴) است که در حمله پیشنهادی به پایه حدس با اندازه پنج و پیچیدگی از مرتبه (O(2¹⁶⁰) کاهش یافته است.

واژگان کلیدی: رمز جریانی، حمله حدس و تعیین، رمز جریانی 1.0 SNOW، رمز جریانی TIPSY، پیچیدگی محاسباتی حمله.

۱- مقدمه

حملات حدس و تعیین از جمله حملات عام به سامانه‌های رمز جریانی است. در این حملات، هدف تعیین مقادیر اولیه حافظه‌ها است. این مقادیر در مرحله بارگذاری اولیه الگوریتم، به طور معمول توسط کلید اصلی و در بعضی الگوریتم‌ها (هاوکس و رز، ۲۰۰۰) به صورت ترکیبی از کلید و مقدار همزمان‌کننده یا بردار نخستین بارگذاری می‌شوند. بنابراین، در این حملات متغیرها، عناصر حافظه هستند. عناصر حافظه یا به صورت بیت و یا به صورت کلمه در نظر گرفته می‌شوند (هاوکس و رز، ۲۰۰۰). بعد از بارگذاری نخستین، الگوریتم اجراسده، کلید اجرایی^۱ به عنوان خروجی تولید می‌شود. به طور معمول، دو معادله مهم در الگوریتم‌های رمز جریانی مورد استفاده تحلیل گر قرار می‌گیرد: معادله

¹ Keystream

است. مؤلفین مقاله این حمله را به SSC-II و TIPSY اعمال کرده‌اند و بهتریب به پیچیدگی از مرتبه‌های $O(2^{41.7})$ و $O(2^{96})$ دست یافته‌اند. البته نتایج این حمله به دیگر سامانه‌های رمز جریانی کلمه‌گرا نتایج مناسبی را در بر نداشته است. این ایده منجر به افزایش تعداد معادلات می‌شود و چنان‌چه به روش اقتصایی صورت گیرد، ممکن است موجب افزایش پیچیدگی تحلیل حمله و تعیین شود. تلاش دیگری توسط احمدی و اقلیدس برای یافتن یک روش کلی برای حمله حمله و تعیین انجام شده است. فکر اصلی این روش تشکیل جداول شاخص متناظر با معادلات مورد استفاده در حمله، برای الگوریتمی کردن حمله حمله و تعیین است. حمله‌ها با جدول‌های شاخص بر اساس معیاری که در (احمدی و اقلیدس، ۲۰۰۹) بیان شده است، زده می‌شود؛ سپس بهزاری هر حمله، شاخص متناظر با آن از جدول حذف شده و الگوریتم وارد مرحله تعیین می‌شود. این روش حمله به الگوریتم TIPSY (هاوکس و رز، ۲۰۰۰) و SNOW2.0 (اکدال و جهانسن، ۲۰۰۰) و SNOW1.0 (اکدال و جهانسن، ۲۰۰۲) (الگوریتم‌های پیشنهاد شده به پروژه اروپایی NESSIE) اعمال شده، بهتریب پیچیدگی حمله را به $O(2^{102})$ و $O(2^{256})$ کاهش داده است (احمدی و اقلیدس، ۲۰۰۹). این روش حمله همچنین به سامانه رمز SOSEMANUK (برون و همکاران، ۲۰۰۵) اعمال شده، مرتبه پیچیدگی را با ضرب 3^{-3} کاهش داده است (احمدی و اقلیدس، ۲۰۰۹) (احمدی و همکاران، ۲۰۰۶).

ساختر مقاله به شرح زیر است: در بخش دوم ایده هاوکس و رز درباره استفاده از مضارب چندجمله‌ای اتصال در حملات حمله و تعیین معرفی شده است. بخش سوم به حمله حمله و تعیین اکتشافی اختصاص داده شده است. در بخش چهارم حمله حمله و تعیین اکتشافی بهبود یافته به سامانه‌های TIPSY و SNOW1.0 شرح داده شده است. در بخش پنجم نتایج حاصل از کار پژوهشی و کارهای آینده بیان می‌شود.

۲- بهره‌گیری از مضارب چندجمله‌ای پس خورد در حملات حمله و تعیین

در حملات حمله و تعیین اقتصایی، بعد از حمله تعدادی از متغیرهای حافظه، به طور معمول از دو معادله ثبات انتقال با پس خورد خطی و تابع غیرخطی برای تعیین باقی متغیرهای

پایه حمله نیز نامیده می‌شود (احمدی و اقلیدس، ۲۰۰۹). هرچه اندازه پایه حمله کوچک‌تر باشد، پیچیدگی حمله کمتر است.

با مطالعه حملات حمله و تعیین که تاکنون معرفی شده‌اند، آن‌ها را به دو دسته حملات حمله و تعیین اقتصایی^۱ و حملات حمله و تعیین اکتشافی^۲ می‌توان تقسیم‌بندی کرد. در حملات حمله و تعیین اقتصایی، تحلیل‌گر، بنا به تجربه و خلاقیت خود، نقاط ضعف الگوریتم رمز تحت بررسی را مد نظر قرار می‌دهد و در ابتدای حمله، پایه حمله را انتخاب می‌کند؛ سپس با این پایه حمله و معادلات اتصال الگوریتم، سایر متغیرها را تعیین می‌کند. در این دسته از حملات به طور معمول تحلیل‌گر معیار یا روشنی مرحله به مرحله برای یافتن پایه حمله نخستین بیان نمی‌کند. حملات حمله و تعیین اقتصایی اعمال شده به سامانه‌های رمز جریانی مانند A5/1 (گالیج، ۱۹۹۷)، SOBER (کانییری، ۲۰۰۱)، SNOW1.0 (هاوکس و رز، ۲۰۰۱) و SNOW2.0 (کانییر، ۲۰۰۱؛ اکدال، ۲۰۰۳)

SOSEMANUK (تسنون و همکاران، ۲۰۰۶؛ لین و جی، ۲۰۰۹؛ فنگ و همکاران، ۲۰۱۰) و ZUC (لین و همکاران، ۲۰۱۱) از نوع اقتصایی هستند؛ اما در حملات حمله و تعیین اکتشافی (احمدی و اقلیدس، ۲۰۰۹)، تحلیل‌گر سعی در یافتن یک روش کلی برای تمامی الگوریتم‌های رمز جریانی یا بعضی از انواع آن‌ها دارد. تلاش برای یافتن یک روش مرحله به مرحله در انواع دیگر تحلیل‌های رمز نیز صورت گرفته است. الگوریتم ارائه شده توسعه اینکنند و همکارانش برای تحلیل آماری مقدار نخستین IV منتخب (إنگلند و همکاران، ۲۰۰۷) از این نمونه تلاش‌ها است.

حملاتی که در آنها یک روش مرحله به مرحله را برای تحلیل یک سامانه رمز ارائه می‌دهند، از دو جهت اهمیت دارد: از دیدگاه طراحی الگوریتم و همچنین ارزیابی آن توسط طراح یا تحلیل‌گر.

در زمینه حملات حمله و تعیین به رمزهای جریانی، دو نمونه از این تلاش‌ها برای یافتن یک راه حل مرحله به مرحله در (هاوکس و رز، ۲۰۰۰) و (احمدی و اقلیدس، ۲۰۰۹) بیان شده است. ایده هاوکس و رز استفاده از معادلات مضارب چندجمله‌ای اتصال، علاوه بر دو معادله ثبات انتقال با پس خورد خطی و معادله بخش غیرخطی است (هاوکس و رز، ۲۰۰۰). این ایده در مرحله تعیین تأثیرگذار

¹ Ad-hoc GD attacks

² Heuristic GD attacks



TIPSY اعمال شده، تعداد حدس برابر با هفت به دست آمده است. حمله شامل دو مرحله است: مرحله حدس و مرحله تعیین. در مرحله نخست شش متغیر حدس زده است. با این حدس ها، مقادیر معادله بخش غیرخطی برای v_{t+23} تعیین می شود. بنابراین، می توان مقدار v_{t+23} به دست آمده را با مقدار v_{t+23} مشاهده شده مقایسه کرد. ادعا شده است که با داشتن مقدار v_{t+23} و متوازن بودن معادله بخش غیرخطی، فضای جستجو برای شش حدس از مرتبه $O(2^{96})$ به $O(2^{80})$ کاهش می یابد. در مجموع پیچیدگی کل حمله از مرتبه $O(2^{16} \times 80) = O(2^{96})$ است (هاوکس و رز، ۲۰۰۰).

۳- حمله حدس و تعیین اکتشافی

ایده دوم (احمدی و اقلیدس، ۲۰۰۹) بر اساس ارائه یک الگوریتم برای اجرای حملات حدس و تعیین به سامانه های رمز جریانی کلمه گرا، با استفاده از مفهومی به نام جدول شاخص^۳ تحقق می یابد. این الگوریتم، حمله حدس و تعیین اکتشافی^۴ نامیده شده است (احمدی و اقلیدس، ۲۰۰۹). تنها محدودیت حمله حدس و تعیین اکتشافی، یکسان بودن اندازه متغیرهای معادلات، معرف رمز جریانی است.

در این روش حمله، دسته معادلات استخراج شده از رمز جریانی به عنوان ورودی به این الگوریتم محسوب می شود. برای رمزهای جریانی، می توان دو دسته معادلات در نظر گرفت. معادلات به روز کردن حالت و معادلات تولید کننده دنباله کلید اجرایی^۵. برای جایگزینی بهتر الگوریتم با دسته معادلات، می توان معادلات دیگری را نیز از الگوریتم رمز استخراج کرد. این معادلات خود تابعی از متغیرهای حافظه هستند. با فرض تعداد معادلات استخراج شده برابر باشد، معادلات به صورت زیر است:

$$\begin{aligned} f_1(S_{1,t+\Delta}, S_{2,t+\Delta}, \dots, S_{k_1,t+\Delta}) &= 0 \\ f_2(S_{1,t+\Delta}, S_{2,t+\Delta}, \dots, S_{k_2,t+\Delta}) &= 0 \\ &\vdots \\ f_r(S_{1,t+\Delta}, S_{2,t+\Delta}, \dots, S_{k_r,t+\Delta}) &= 0 \end{aligned} \quad (7)$$

؛ $0 \leq \Delta < n$

³Index table⁴Heuristic GD attack⁵connection equation

حافظه استفاده می شود. هاوکس و رز بیان کردند که در حمله حدس و تعیین، می توان از معادلات دیگری علاوه بر این دو معادله، بهره برد (هاوکس و رز، ۲۰۰۰). روش ساخت این معادلات به این صورت است که با فرض این که $p(x)$ چندجمله ای معادله بازگشتی LFSR باشد، با انتخاب یک چندجمله ای $q(x)$ و ضرب آن در $p(x)$ معادلات اضافی به صورت $r(x) = q(x)p(x)$ تولید می شود (هاوکس و رز، ۲۰۰۰). $r(x)$ مضری از چندجمله ای بازگشتی LFSR است (هاوکس و رز، ۲۰۰۰). متأسفانه، هاوکس و رز نتوانستند ویژگی خاصی را برای $q(x)$ به دست بیاورند، طوری که منجر به یک حمله حدس و تعیین بهینه شود؛ اما حدس می زند که چندجمله ای هایی از $r(x)$ مفیدند که دارای درجه^۱ و وزن^۲ کمتری باشند. آنها از این ایده برای بهبود حمله حدس و تعیین به TIPSY با پیچیدگی از مرتبه $O(2^{96})$ استفاده کردند (هاوکس و رز، ۲۰۰۰).

$$p(x) = x^{13} + x^4 + x + \alpha \quad (1)$$

$$S_{t+13} = S_{t+4} + S_{t+1} + \alpha S_t \quad \alpha = 0x EDED \quad (2)$$

معادله بخش غیر خطی به صورت زیر است:

$$v_t = f(S_t \oplus S_{t+11}) + S_{t+5} + S_{t+10} \bmod 2^{16} \quad (3)$$

مضارب مورد استفاده در حمله حدس و تعیین هاوکس و رز به این سامانه نیز به صورت زیر است:

$$p^2(x) = x^{26} + x^8 + x^2 + \alpha^2 \quad (4)$$

$$\begin{aligned} r_1(x) &= (x^9 + x^6 + x^3 + 1) \cdot p(x) \\ &= x^{22} + x^{19} + x^{16} + \alpha x^9 + \alpha x^6 \\ &\quad + \alpha x^3 + x + \alpha \end{aligned} \quad (5)$$

$$\begin{aligned} r_2(x) &= (x^{12} + \alpha x^{11} + \alpha^2 x^{10} \\ &\quad + x^6 + x^3 + \alpha x^2 + \alpha^2 x + 1) \cdot p(x) \\ &= x^{25} + \alpha x^{24} + \alpha^2 x^{23} + x^{19} \\ &\quad + (\alpha^3 + 1)x^{10} + \alpha^2 x^5 + (\alpha^3 + 1)x \\ &\quad + \alpha \end{aligned} \quad (6)$$

در معادلات بالا علامت^۶ بیان گر جمع پیمانه ای در میدان ۲^{۱۶} است. این حمله با استفاده از معادلات (۱) تا (۶) به

¹Low degree²Low weight

باشد. همچنین، در این روش تحلیل گر نیازی به حل هم‌زمان معادلات اتصال در ابتدای حمله ندارد. بدین ترتیب تحلیل گر می‌تواند بر اساس معیارهایی خاص به صورت مرحله‌به‌مرحله به حدس مجموعه‌ای از متغیرها که پایه حدس نامیده می‌شود، پردازد. این معیارها که معیار "د" نامیده شده‌اند،

به صورت زیر است (احمدی و اقلیدس، ۲۰۰۹):

معیار "د": برای یافتن یک پایه حدس مناسب، می‌بایست یک معیار مناسب وجود داشته باشد تا عمل جستجوی الگوریتم در جداول شاخص بر اساس آن انجام شود. این معیار که به معیار "د" مشهور است، به صورت زیر است:

(الف) متغیری که قادر به بیشترین حذف شاخص از ماتریس‌ها باشد؛

(ب) متغیری که قادر به ایجاد ردیف‌ها با تعداد شاخص‌های متناظر با متغیرهای مجھول کمتری در جداول شاخص است (احمدی و اقلیدس، ۲۰۰۵ و ۲۰۰۹).

انتخاب هر حدس توسط الگوریتم حمله حدس و تعیین اکتشافی بر اساس معیار "د" صورت می‌گیرد. سپس این شاخص از جدول‌های شاخص حذف می‌شود. در مرحله تعیین، الگوریتم در جدول شاخص با بررسی ردیف‌ها، دسته معادلات تک مجھولی یا دو مجھولی یا بیشتر را جستجو می‌کند. اندازه دستگاه معادلات را تحلیل گر انتخاب می‌کند. از سوی دیگر، در صورت یافتن دسته معادلات، شاخص متناظر با مجھولات را از جدول‌های شاخص حذف می‌کند. دوباره الگوریتم وارد مرحله حدس می‌شود و مراحل پیشین تکرار می‌شود تا تمامی شاخص‌های جدول حذف شوند.

حمله اکتشافی بالا در (احمدی و اقلیدس، ۲۰۰۵) به عنوان حمله حدس و تعیین پیشرفته نامیده شده است. در (احمدی و اقلیدس، ۲۰۰۹) همین الگوریتم حمله با استفاده از نمودار تریس و معیار شبیه‌وتربی با بیان دیگر به صورت الگوریتمی بیان شده و این روش به نام حمله حدس و تعیین اکتشافی نامیده شده است. حمله حدس و تعیین اکتشافی به رمز TIPSY با پیچیدگی از مرتبه $O(2^{10^2})$ همراه با پایه حدس با اندازه شش اعمال شده است (احمدی و اقلیدس، ۲۰۰۹). بخشی از پیچیدگی به دست آمده مربوط به حل شش دستگاه سه معادله سه مجھول است. این حمله به رمز SNOW 1.0 نیز با پیچیدگی $O(2^{20^2})$ و اندازه پایه حدس شش اعمال شده است (احمدی، ۱۳۸۴).

در معادلات (۷) $t + \Delta$ بیان گر زمان است. یعنی معادلات در n فرمان ساعت در نظر گرفته می‌شوند. مقدار n باید حداقل برابر با تعداد متغیرهای حافظه باشد. در این صورت برای هر یک از معادلات (۷)، ماتریس گسترش زمانی، یا ماتریس اتصال به صورت زیر تشکیل می‌شود:

$$T_i = \begin{bmatrix} S_{1,t} & S_{2,t} & \dots & S_{k_i,t} \\ S_{1,t+1} & S_{2,t+1} & \dots & S_{k_i,t+1} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ S_{1,t+n-1} & S_{2,t+n-1} & \dots & S_{k_i,t+n-1} \end{bmatrix} \quad (8)$$

در این صورت هر معادله دارای ماتریس شاخص زمانی به شکل زیر است:

$$M = \begin{bmatrix} 1 & 2 & \dots & k_i \\ 1+1 & 2+1 & \dots & k_i+1 \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 1+n-1 & 2+n-1 & \dots & k_i+n-1 \end{bmatrix} \quad (9)$$

بر اساس ماتریس شاخص زمانی، جدول شاخص به صورت (جدول - ۱) تشکیل می‌شود:

(جدول - ۱): جدول شاخص برای معادلات (۷)

۱	۲	...	k_i
$1+1$	$2+1$...	k_i+1
...
$1+n-1$	$2+n-1$...	k_i+n-1

جدول (۱) به عنوان جدول شاخص در حمله حدس و تعیین اکتشافی استفاده می‌شود. در این روش، متناظر با هر معادله، یک جدول شاخص تشکیل می‌شود که در این‌های جدول متناظر با متغیرهای حافظه در فرمان‌های ساعت متفاوت است. شاخص‌های یکسان در جداول شاخص متناظر با یک متغیر در زمان خاص است. هر ردیف از جداول شاخص نیز بیان گر یک معادله در یک زمان مشخص است. جداول شاخص به تحلیل گر کمک می‌کند که یک برآورد از تعداد حضور یک شاخص و تعداد ترکیب‌های شاخص‌های مختلف در هر ردیف از جداول شاخص داشته

فصل نهم



اکنون جدول‌های شاخص متناظر با معادلات فرعی را، علاوه‌بر معادلات اصلی، به عنوان ورودی الگوریتم حمله حدس و تعیین اکتشافی به کار می‌گیریم. معادلات فرعی از مضارب چندجمله‌ای با وزن کمینه انتخاب می‌شوند. بنابراین تنها مضاربی که ضرایب آن‌ها یعنی $(x)^q$ دارای وزن دو است، در نظر گرفته می‌شود. از طرفی برای تکرار شاخص‌های معادلات اصلی، $(x)^q$ باید دارای یک جمله ثابت باشد؛ یعنی، $x^q = x^{q+1}$. به منظور کاهش وزن معادله فرعی، n را از میان تفاضل‌های دوبعدی درجات جملات چندجمله‌ای پس خورد انتخاب می‌کنیم. در این صورت وزن چندجمله‌ای فرعی نسبت به حالتی که n را هر عدد طبیعی دیگری انتخاب کنیم، یک واحد کاهش می‌یابد. این کاهش وزن مربوط به الگوریتم‌های رمزی است که چندجمله‌ای پس خورد آن‌ها در توسعی میدان GF(2) باشد و همچنین جمع ضرایب جملات هم درجه در میدان GF(2) صفر شود.

۴- بهبود حمله حدس و تعیین اکتشافی

در این بخش ضمن بیان یک روش برای بهبود حمله حدس و تعیین اکتشافی، رمزهای SNOW 1.0 و TIPSY تحلیل شده‌اند؛ سپس، نتایج این حمله با حملات حدس و تعیین اقتضایی و اکتشافی پیشین مقایسه شده است. حمله حدس و تعیین اکتشافی به دو صورت می‌تواند بهبود یابد. یکی در مرحله حدس که با بهبود معیار "D" صورت می‌گیرد. دیگری، بهبود مرحله تعیین است، به‌طوری که تعداد هر چه بیشتری از شاخص‌ها به‌ازای هر حدس تعیین شوند. در این مقاله از ایده بیان شده در بخش دوم برای بهبود مرحله تعیین استفاده می‌شود. به این ترتیب دو دسته معادلات تعریف می‌کنیم:

الف- معادلات اصلی: این معادلات به‌طور مستقیم از الگوریتم استخراج می‌شوند.

ب- معادلات فرعی: این معادلات، به عنوان معادلات کمکی، بر اساس مضارب چندجمله‌ای پس خورد (یکی از معادلات اصلی) به دست می‌آیند.

(جدول-۲): جدول‌های شاخص M1 و M2 و M3 متناظر با معادلات (۱) و (۳) و (۴)

M1				M2				M3			
0	1	4	13	0	5	10	11	0	2	8	26
1	2	5	14	1	6	11	12	1	3	9	27
.
.
28	29	32	41	28	33	38	39	29	30	36	54
29	30	33	42	29	34	39	40	29	31	37	55

پیمانه‌ای در میدان GF(2¹⁶) است. چندجمله‌ای به کار رفته در معادله فرعی، مضرب توان دوم چندجمله‌ای پس خورد در الگوریتم TIPSY است. جدول‌های شاخص M1، M2 و M3 به ترتیب متناظر با چندجمله‌ای پس خورد، معادله بخش غیرخطی و معادله فرعی است که در

(جدول-۲) نشان داده می‌شود.

تعداد ردیف‌های جدول‌های شاخص حداقل بایستی برابر با تعداد خانه‌های حافظه الگوریتم رمز باشد (احمدی و اقلیدس، ۲۰۰۹) تا تمام شاخص‌های خانه‌های حافظه الگوریتم رمز حداقل یکبار در جدول‌های شاخص ظاهر شوند. در این حمله تعداد ردیف‌ها برابر با سی در نظر گرفته شده است؛ زیرا با به ازای تعداد سی ردیف از جدول شاخص، کمترین پایه حدس برابر با شش به دست آمده است. مراحل

البته در الگوریتم‌های رمزی که چندجمله‌ای LFSR آنها در توسعی میدان GF(2) تعریف شده است، توان دوم این چندجمله‌ای دارای وزن یکسانی با خود چندجمله‌ای LFSR است؛ اما درجه این چندجمله‌ای دو برابر درجه چندجمله‌ای LFSR است. از ایده این معادلات فرعی برای بهبود حمله حدس SNOW 1.0 و TIPSY و تعیین اکتشافی به سامانه‌های رمز SNOW 1.0 و TIPSY به عنوان رمزهای نمونه استفاده می‌شود. در ادامه حملات اکتشافی بهبود یافته به رمزهای مذکور را شرح خواهیم داد.

۴- حمله حدس و تعیین اکتشافی

بهبود یافته به TIPSY

در این حمله، معادلات اصلی (۱) و (۳) و معادله فرعی (۴) به عنوان دسته معادلات ورودی به الگوریتم حمله استفاده می‌شود. در معادلات این بخش علامت + بیان گر جمع

که مقادیر K_i و v_{t+j} معلوم است. با جایگذاری معادلات (۱۰) و (۱۲) به ترتیب در (۱۱) و (۱۳) معادلات یک مجھولی زیر به دست می‌آید:

$$f(K \oplus \alpha S_{13}) + S_{13} = K' \quad (14)$$

$$f(Q \oplus \alpha S_{18}) + S_{18} = Q' \quad (15)$$

$K = K_1 \oplus K_2 \oplus K_3$ (۱۵) که در معادلات (۱۴) و

$$Q' = v_{t+8} - K_9 \quad Q = K_6 \oplus K_7 \oplus K_8, \quad K' = v_{t+23} - K_4$$

است. با توجه به غیرخطی بودن این معادلات، برای حل هر یک از آنها نیاز به یک جدول پیش‌پردازش است که قبل از اعمال حمله به دست می‌آید (احمدی، ۱۳۸۴). بنابراین، با وجود این دو جدول پیش‌پردازش پیچیدگی حمله از مرتبه $O(2^{6 \times 16}) = O(2^{96})$ است.

حمله حدس و تعیین اکتشافی در جدول (۳) نشان داده شده است.

۱-۱-۴- پیچیدگی حمله

در جدول (۳)، با توجه به ستون حدس، پایه حدس، مجموعه $\{26, 27, 21, 22, 23, 17\}$ است. در گام‌های ۱۶ و ۲۸ از جدول (۳)، دو دستگاه دو معادله و دو مجھول به صورت زیر تولید می‌شوند:

$$K_1 = K_2 \oplus S_{14} \oplus \alpha S_{13} \quad (10)$$

$$v_{t+3} = f(K_3 \oplus S_{14}) + K_4 + S_{13} \quad (11)$$

و

$$K_6 = K_7 \oplus S_{19} \oplus \alpha S_{18} \quad (12)$$

$$v_{t+8} = f(K_8 \oplus S_{19}) + K_9 + S_{18} \quad (13)$$

(جدول-۳): مراحل اعمال حمله به TIPSY

گام	حدس	معادلات مورد استفاده	شاخص‌های مقادیر معلوم	مقادیر تعیین شده
۱	۲۶	-	-	-
۲	۲۷	-	-	-
۳	۲۱	-	-	-
۴	۲۲	M2	۲۱, ۲۶, ۲۷	۱۶
۵	۲۲	-	-	-
۶	۲۱	M2	۱۶, ۲۱, ۲۲	۱۱
۷	۱۷	-	-	-
۸	۱۷	M2	۱۷, ۲۲, ۲۷	۲۸
۹	۱۷	M2	۱۱, ۱۶, ۱۷	۶
۱۰	۲۳	-	-	-
۱۱	۱۱	M1	۲۲, ۲۳, ۲۶	۳۵
۱۲	۱۲	M2	۱۷, ۲۲, ۲۳	۱۲
۱۳	۱۳	M2	۶, ۱۱, ۱۲	۱
۱۴	۱۴	M3	۱, ۲, ۲۷	۹
۱۵	۱۵	M1	۹, ۱۲, ۲۱	۸
۱۶	۱۶	M1, M2	۳, ۸, ۱۷, ۲۶	۱۳, ۱۴
۱۷	۱۷	M1, M2, M3	با استفاده از متغیرهای معلوم قبلی و حل معادلات یک مجھولی	۱۰, ۰۲۵, ۰۳۴, ۰۳۰, ۰۳۲ ۳۱, ۰۴۰, ۰۴۴, ۰۴۹, ۰۵۱, ۰۵۲
۱۷	۲۷	-	-	الی
۲۸	۲۸	M1, M2	۸, ۱۳, ۲۲, ۳۱	۱۸, ۱۹
۲۹	۲۹	M1, M2, M3	تعیین باقی‌مانده شاخص‌ها	۲۹ تا انتها

به روزرسانی الگوریتم مبتنی بر ثبات انتقال با پس‌خورد خطی است. این بخش دارای شانزده طبقه حافظه‌های ۳۲ بیتی در میدان $GF(2^32)$ است. معادله بازگشتی و چندجمله‌ای متناظر با آن به صورت زیر است:

$$S_{t+16} = \alpha(S_{t+9} \oplus S_{t+3} \oplus S_t) \quad (16)$$

۲-۴- حمله حدس و تعیین اکتشافی

بهبود یافته به SNOW 1.0

SNOW 1.0 (اکدال و جهانسن، ۲۰۰۰) یک الگوریتم رمز جربانی کلمه‌گرا است. ساختار این الگوریتم از دو بخش به‌روزرسانی و بخش غیرخطی تشکیل شده است. بخش

فصل نهم



$$R1_t = ((W_{t-1} + R2_{t-1}) \lll 7) \oplus R1_{t-1} \quad (18)$$

$$R2_t = S_Box(R1_{t-1}) \quad (19)$$

$$W_t = (S_{t+15} + R1_t) \oplus R2_t \quad (20)$$

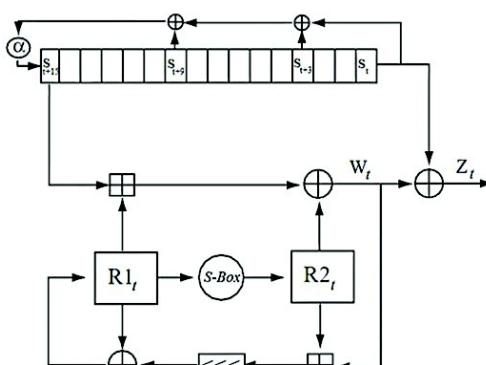
$$p(x) = \alpha^{-1}x^{16} + x^9 + x^3 + 1 \in F_{2^{32}}[x] \quad (17)$$

علامت + در معادلات این بخش بیان گر جمع پیمانه ای در GF(2³²) است. بخش غیر خطی (FSM) الگوریتم دارای دو حافظه ۳۲ بیتی R1 و R2 است که با یک جعبه جانشینی به یکدیگر مرتبط شده اند. معادلات بخش غیر خطی به صورت زیر است:

(جدول - ۴): جدول های شاخص M1، M2 و M3 به ترتیب متناظر با معادلات (۱۶)، (۲۰) و (۲۴)

M1				M2				M3					
.	۳	۹	۱۶	.	۱۵	۴۹	۵۰	.	۶	۹	۱۲	۱۶	۱۹
۱	۴	۱۰	۱۷	۱	۱۶	۵۰	۵۱	۱	۷	۱۰	۱۳	۱۷	۲۰
.
.	۱۸	۲۴	۲۷	۳۰	۳۴	۳۷
.	۱۹	۲۵	۲۸	۳۱	۳۵	۳۸
۱۸	۲۱	۲۷	۳۴	۱۸	۳۳	۶۷	۶۸	۱۹	۳۴	۶۸	۶۹		
۱۹	۲۲	۲۸	۳۵	۱۹	۳۴	۶۸	۶۹						

در جدول (۵) نشان داده می شود. پایه حدس به دست آمده با اندازه ۵ برابر {۵۰، ۲۵، ۲۲، ۱۶، ۱۹} است.



(شکل - ۱): الگوریتم SNOW 1.0 (اکمال و جهانسون، ۲۰۰۰)

۱-۲-۱- پیچیدگی حمله
با توجه به خطی بودن معادلات (۱۶) و (۲۴) در حل دستگاه های دو معادله دومجهولی در طی مرحله تعیین، نیازی به تشکیل جدول های پیش پردازش نیست. معادله (۲۳) غیر خطی است، اما در طی حمله به حل این معادله نیازی نیست. بنابراین پیچیدگی محاسبات حمله تنها برابر با همان پیچیدگی محاسباتی پایه حدس با اندازه ۵ است. پیچیدگی این حمله از مرتبه O(2¹⁶⁰) = O(2⁵ × 3²) است که نسبت به حمله حدس و تعیین آکتشافی پیشین (احمدی و اقلیدس، ۲۰۰۹) از مرتبه O(2⁴²) کاهش یافته است.

$$Z_t = W_t \oplus S_t \quad (21)$$

خروجی بخش غیر خطی و Z خروجی الگوریتم است. با ترکیب معادلات (۱۸)، (۱۹) و (۲۰) مقدار حافظه از رابطه زیر به دست می آید:

$$\begin{aligned} R1_t = & (((S_{t+14} + R1_{t-1}) \oplus S_Box(R1_{t-2})) \\ & + S_Box(R1_{t-2})) \lll 7] \oplus R1_{t-1} \end{aligned} \quad (22)$$

با ترکیب روابط (۱۹)، (۲۰) و (۲۱) معادله خروجی الگوریتم به صورت زیر ساده می شود:

$$Z_t = [(S_{t+15} + R1_t) \oplus S_Box(R1_{t-1})] \oplus S_t \quad (23)$$

برای درک بهتر عملکرد SNOW 1.0 (شکل - ۱) شما رمز جریانی 1.0 نشان داده شده است. برای اعمال حمله حدس و تعیین آکتشافی از معادلات اصلی (۱۶) و (۲۳) و معادله فرعی زیر استفاده می شود:

$$\begin{aligned} S_{t+19} = & \alpha(\alpha^{-1}S_{t+16} \oplus S_{t+12} \oplus S_{t+9} \\ & \oplus S_{t+6} \oplus S_t) \end{aligned} \quad (24)$$

معادله (۲۴) از ضرب دو جمله ای (x³+1)، به عنوان ضرب، در چند جمله ای مشخصه به دست آمده است. درجه این دو جمله ای طبق روش ارائه شده در بخش چهار به دست آمده است. در جدول (۴)، جدول های شاخص متناظر با معادلات (۱۶)، (۲۳) و (۲۴) نمایش داده شده است. مراحل اعمال حمله حدس و تعیین آکتشافی بهمودیافته به SNOW

(جدول-۵): مراحل حمله حدس و تعیین اکتشافی به الگوریتم SNOW 1.0

گام	حدس	معادلات مورد استفاده	شاخص‌های مقادیر معلوم	مقادیر تعیین شده
۱	۱۹	-	-	-
۲	۱۶	-	-	-
۳	۲۵	-	-	-
۴	-	M1	۱۶,۱۹,۲۵	۳۲
۵	۲۲	-	-	-
۶	-	M1,M3	۱۶,۱۹,۲۲,۲۵	۱۳,۲۹
۷	-	M1,M3	۱۳,۱۶,۱۹,۲۲,۲۹	۱۰,۲۶
۸	-	M1,M3	۱۰,۱۳,۱۶,۱۹	۷,۲۳
۹	-	M1,M3	۷,۱۰,۱۳,۱۶	۴,۲۰
۱۰	-	M1,M3	۴,۷,۱۰,۱۳,۲۰	۱,۱۷
۱۱	-	M1	۱۷,۲۰,۲۶	۳۳
۱۲	-	M3	۱۷,۲۳,۲۶,۲۹,۳۳	۳۶
۱۳	-	M1,M3	۱۷,۲۰,۲۳,۲۶,۳۳	۱۴,۳۰
۱۴	-	M1,M3	۱۴,۱۷,۲۰,۲۳,۳۰	۱۱,۲۷
۱۵	-	M1,M3	۱۱,۱۴,۱۷,۲۰,۲۷	۸,۲۴
۱۶	-	M1,M3	۸,۱۱,۱۴,۱۷,۲۴	۵,۲۱
۱۷	-	M1,M3	۵,۸,۱۱,۱۴,۲۱	۲,۱۸
۱۸	-	M1	۱۸,۲۱,۲۷	۳۴
۱۹	-	M3	۱۸,۲۴,۲۷,۳۰,۳۴	۳۷
۲۰	-	M1,M3	۱۸,۲۱,۲۴,۲۷,۳۴	۱۵,۳۱
۲۱	-	M1,M3	متغیرهای معلوم (دستگاه چهارمعادله و چهار مجھول)	۰,۳,۶,۹,۱۲
۲۲	-	M1,M3	۱۶,۱۹,۲۲,۲۵,۳۲	۲۸,۳۵
۲۳	۵۰	-	-	-
۲۴	۱۱۰	M2	تعیین شاخص‌های باقیمانده	تاتا انتها

(جدول-۶): مقایسه نتایج حملات حدس و تعیین

اکتشافی و اقتصابی

حملات حدس و تعیین								الگوریتم	
اکتشافی				اقتصابی					
بهبود یافته		پیشین							
۵	۶	۷	۸	۹	۱۰	۱۱	۱۲		
۶	O(۲ ^{۱۶})	۶	O(۲ ^{۱۷})	۷	O(۲ ^{۱۸})	TIPSY			
۵	O(۲ ^{۱۶})	۶	O(۲ ^{۱۷})	۶	O(۲ ^{۱۸})	SNOW1.0			

۳-۴- مقایسه نتایج حملات

در جدول (۶) نتایج حملات حدس و تعیین اقتصابی و اکتشافی اعمال شده به الگوریتم‌های SNOW 1.0 و TIPSY با نتایج حملات حدس و تعیین اکتشافی بهبود یافته در این مقاله مقایسه شده است.

در حمله حدس و تعیین اکتشافی به الگوریتم SNOW1.0 پیچیدگی $O(2^{160})$ به دست آمده است که نسبت به حمله حدس و تعیین اکتشافی پیشین (احمدی و اقلیدس، ۲۰۰۹) پیچیدگی را به اندازه $O(2^{42})$ کاهش داده است. این حمله نسبت به حمله حدس و تعیین اقتصابی هاؤکس و رُز (هاوکس و رُز، ۲۰۰۲) با پیچیدگی $O(2^{224})$ کاهش از مرتبه $O(2^{64})$ را نشان می‌دهد.

فصل نهم





- Ahmadi H., Eghlidos T. (2009), heuristic guess-and-determine attacks on stream ciphers, IET information security, 2009, Vol. 3, Iss. 2, pp. 66-73, 2009.
- Bervain C., Billet O., Canteaut A (2005), "SOSEMANUK, a fast software-oriented stream cipher", eSTREAM, ECRYPT Stream Cipher Project Report 2005/027, 2005, <http://www.ecrypt.eu.org/stream/>, accessed on June 2013.
- DE CANNIERE C. (2001), Guess and determine attack on SOBER'.NESSIE Public Document, NES/DOC/KUL/WP5/010/a, 2001, <http://www-cryptonessie.org>, accessed on June 2013.
- DE CANNIERE C. (2001), Guess and determine attack on SNOW, NESSIE Public Document, NES/DOC/KUL/WP5/011/a, 2001, <http://www-cryptonessie.org>, accessed on June 2013.
- EKDAHL P., JOHANSSON T. (2000), SNOW – a new stream cipher, Proc. First NESSIE Workshop, 2000, Heverlee, Belgium, <https://www.cosic.esat.kuleuven.be/nessie/workshop/>, accessed on June 2013.
- EKDAHL P., JOHANSSON T. (2002), "A new version of the stream cipher SNOW". SAC 2002, 2002, (LNCS, 2595), pp. 47–61. New European Schemes for Signature, Integrity and Encryption, <https://www.cosic.esat.kuleuven.be/nessie/>, accessed June 2013.
- EKDAHL P. (2003), 'On LFSR based stream ciphers analysis and design', PhD Thesis, Department of Information Technology, Lund University, Sweden, 2003.
- England H., Johansson T., Turan M.S. (2007), A Framework for Chosen IV Statistical Analysis of Stream Cipher"; INDOCRYPT 2007; Springer-Verlag; LNCS 4859, 2007, pp. 268-281.
- Feng Xiutao, Liu Jun, Zhou Zhaojun, Wu Chuankun, Feng Dengguo (2010), A Byte-Based Guess and Determine Attack on SOSEMANUK, In Proceedings of Asiacrypt '10, LNCS 6477, PP.146-157, Springer-Verlage, 2010.
- GOLIC' J. (1997), Cryptanalysis of alleged A5 stream cipher, Proc. EUROCRYPT'97, 1997, (LNCS, 1233), pp. 239–255.
- Hawkes, P., Rose, G. (2000). Exploiting multiplies of the connection polynomial in word-oriented stream ciphers, ASIACRYPT2000, LNCS1976, pp.302-316.
- Hawkes P., Rose G. (2002), Guess and determine attacks on SNOW, In Selected Area of Cryptography—SAC2002, LNCS 2595, pp.37-46.
- Lin D., Jie G. (2009), Guess and Determine Attack on SOSEMANUK', 2009 Fifth International Conference on Information Assurance and Security, vol.1, pp.658-661.
- Lin D., Liu Shu-kai, Zhang Zhong-ya, Jie G. (2011), Guess and Determine Attack on ZUC Based on Solving Nonlinear Equations"; First Workshop on ZUC; 2011. Accessed on 2012.

۵- جمع‌بندی و نتیجه‌گیری

در این مقاله دو دسته از حملات حدس و تعیین، حملات حدس و تعیین اقتضایی و اکتشافی معرفی و تفاوت‌های این دو روش بیان شده است. پس از معرفی مفهوم پایه حدس، معادلات اصلی و معادلات فرعی (کمکی) در حملات حدس و تعیین، ایده استفاده از مضارب چندجمله‌ای مشخصه به عنوان معادلات فرعی و روش استفاده از جدول‌های شاخص در حمله حدس و تعیین اکتشافی به طور کامل بیان شده است. در ادامه، با استفاده از دو معادله اصلی و یک معادله فرعی حملات حدس و تعیین اکتشافی به سامانه‌های رمز جریانی TIPSY و SNOW 1.0 اعمال شده است. نتایج اعمال حمله پیشنهادی حدس و تعیین اکتشافی به الگوریتم TIPSY با پیچیدگی $O(2^{96})$ نشان از بهبود این حمله نسبت به حمله حدس و تعیین اکتشافی پیشین با پیچیدگی $O(2^{102})$ دارد. از سوی دیگر، پیچیدگی این حمله و حمله اقتضایی پیشین به TIPSY با هم برابر و از مرتبه $O(2^{96})$ است؛ در حالی که پایه حدس از هفت به شش کاهش یافته است. همچنین، حمله پیشنهادی حدس و تعیین اکتشافی به الگوریتم SNOW1.0 دارای پیچیدگی از مرتبه $O(2^{160})$ است، که نسبت به حمله حدس و تعیین اکتشافی پیشین از مرتبه $O(2^{42})$ کاهش یافته است. از سوی دیگر، پیچیدگی این حمله نسبت به حمله حدس و تعیین اقتضایی با پیچیدگی $O(2^{224})$ کاهش قابل توجهی را نشان می‌دهد.

۶- مراجع

احمدی هادی (۱۳۸۴)، بررسی حملات حدس و تعیین به سیستم‌های رمز دنباله‌ای استاندارد NESSIE و ارائه یک طرح بهبودیافته برای رمزهای دنباله‌ای با انتقال کلمه به کلمه، پایان‌نامه کارشناسی ارشد، دانشگاه صنعتی شریف، آبان ماه ۱۳۸۴.

Ahmadi H., Eghlidos T. (2005), "Advanced Guess and Determine Attacks on Stream Ciphers" International Symposium on Telecommunications (IST 2005), pp. 87-91, Sept. 10-12, 2005, Shiraz, Iran.

Ahmadi H., Eghlidos T., Khazaei S. (2006), Improved guess and determine Attack on SOS-EMANUK, SASC 2006- Stream Cipher Revisited, Special Workshop hosted by the ECRYPT Network of Excellence, Leuven, Belgium, Feb. 2-3, 2006. www.ecrypt.eu.org/stream/sosemanukp3.html. Accessed on 15June 2014.

ماهواره‌ای را در انجمن تحقیقات علوم کاربردی ایران
عهدهدار بوده‌اند. ایشان هم‌اکنون استادیار مجتمع فناوری
اطلاعات و ارتباطات دانشگاه صنعتی مالک اشتر تهران
همستند و تاکنون بیش از ۱۰۰ مقاله در مجلات و
کنفرانس‌های بین‌المللی ارائه و به چاپ رسانده‌اند. زمینه‌های
علمی مورد علاقه ایشان نظریه اطلاعات، نظریه کدگذاری،
رمزگاری، پروتکل‌های امنیتی، امنیت رایانش ابری،
ارتباطات امن و ارتباطات ماهواره‌ای است.

نشانی رایانامه ایشان عبارت است از:

payandeh@mut.ac.ir

Tsunoo Y., Saito T., Shigeri M., Suzaki T., Ahmadi H., Eghlidos T., Khazaei S. (2006), ‘Evaluation of SOSEMANUK with regard to guess-and-determine attacks’, In Proceedings of SASC 2006, <http://www.ecrypt.eu.org/stream/osemanukp3.html>, accessed on 15 July 2014.



محمد صادق نعمتی‌نیا کاردانی و
کارشناسی خود را در گرایش برق -
الکترونیک بهتریب از دانشگاه‌های
بیرجند و حکیم‌سیبزواری در سال‌های
۱۳۸۶ و ۱۳۸۸ دریافت کرده است.
ایشان در سال ۱۳۹۳ از پایان‌نامه

کارشناسی ارشد خود در گرایش مخابرات رمز در دانشگاه
مالک اشتر تهران دفاع کرده است. زمینه‌های پژوهشی مورد
عالقه ایشان، رمزهای متقارن، رمزگاری کلید عمومی است.
نشانی رایانامه ایشان عبارت است از:

nemati.skh.ict@chmail.ir

خانم دکتر ترانه اقلیدس دانشیار پژوهشکده الکترونیک در
دانشگاه صنعتی شریف، مدارک کارشناسی و کارشناسی
ارشد خود را در رشته ریاضی از دانشگاه‌های شهید بهشتی و
کایزرسلاترن (آلمان) بهتریب در سال‌های ۱۳۶۴ شمسی و
۱۹۹۱ میلادی و مدرک دکتراخود را در رشته ریاضی از
دانشگاه گیسن آلمان در سال ۲۰۰۰ میلادی دریافت کرد.
ایشان از بهمن ۱۳۸۰ تاکنون عضو هیئت علمی پژوهشکده
الکترونیک در دانشگاه صنعتی شریف است. زمینه‌های علمی
پژوهشی مورد علاقه ایشان شامل مبانی رمزگاری متقارن و
نماتقارن، نظریه کدگذاری و کاربردهای آن در رمزگاری،
نظریه مشبکه و کاربردهای آن در رمزگاری و به طور کلی
مدل‌سازی ریاضی برای مسائل برخاسته از پدیده‌های دنیای
واقعی است.

نشانی رایانامه ایشان عبارت است از:

teghlidos@sharif.edu



علی پاینده، مدرک کارشناسی
ارشد و دکتراخود را بهتریب در
سال‌های ۱۳۷۳ و ۱۳۸۳ در رشته
مهندسی برق از دانشگاه تربیت
مدرس و دانشگاه صنعتی خواجه
نصیرالدین طوسی دریافت کرده است. ایشان از سال

۱۳۷۳ تا ۱۳۸۳ مدیریت تحقیقات در حوزه امنیت ارتباطات

فصل نهم



سال ۱۳۹۴ شماره ۴ پیاپی ۲۶