بهبود حملهٔ حدس و تعیین اکتشافی به سامانه‌های رمز جریانی TIPSY و SNOW1.0

محمد صادق نعمتی‌نیا[1]، ترانه اقلیدس[2] و علی پاینده[3]

[1و3] مجتمع فن‌آوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران، ایران

[2] پژوهشکدهٔ الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

چکیده

حملات حدس و تعیین از جمله حملات عام به سامانه‌های رمز جریانی است. این حملات به دو دستهٔ حملات حدس و تعیین اقتضایی و اکتشافی تقسیم‌بندی می‌شوند. مزیت روش اکتشافی نسبت به روش اقتضایی در قدرت تحلیل و ارائهٔ الگوریتمی برای دسته بزرگی از رمزهای جریانی با فرض یکسان‌بودن اندازه متغیرها است. در این مقاله از معادلات فرعی علاوه‌بر معادلات اصلی به‌عنوان ورودی حملهٔ حدس و تعیین اکتشافی برای حمله به سامانه‌های رمز جریانی TIPSY و SNOW 1.0 استفاده شده است. بر اساس مفهوم پایهٔ حدس تعداد حدس‌ها در حمله اکتشافی و بهبودیافته به سامانهٔ TIPSY، شش مورد است؛ امّا پیچیدگی حمله حدس و تعیین اکتشافی بهبودیافته از $O(2^{102})$ به $O(2^{96})$ کاهش یافته است. این پیچیدگی با پیچیدگی حملهٔ اقتضایی برابر است؛ ولی حملهٔ پیشنهادی، اندازهٔ پایهٔ حدس را از هفت به شش بهبود داده است. همچنین، در حملهٔ حدس و تعیین به SNOW 1.0 پیچیدگی حملهٔ اکتشافی با پایهٔ حدس با اندازهٔ شش و اقتضایی با اندازهٔ هفت به‌ترتیب $O(2^{202})$ و بوده $O(2^{224})$ است که در حملهٔ پیشنهادی به پایهٔ حدس با اندازهٔ پنج و پیچیدگی از مرتبهٔ $O(2^{160})$ کاهش یافته است.

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

۱- مقدّمه

حملات حدس و تعیین از جمله حملات عام به سامانه‌های رمز جریانی است. در این حملات، هدف تعیین مقادیر اولیهٔ حافظه‌ها است. این مقادیر در مرحلهٔ بارگذاری اولیهٔ الگوریتم، به‌طورمعمول توسط کلید اصلی و در بعضی الگوریتم‌ها (هاوْکس و رُز، ۲۰۰۰) به‌صورت ترکیبی از کلید و مقدار همزمان‌کننده یا بردار نخستین بارگذاری می‌شوند. بنابراین، در این حملات متغیرها، عناصر حافظه هستند. عناصر حافظه یا به‌صورت بیت و یا به‌صورت کلمه در نظر گرفته می‌شوند (هاوْکس و رُز، ۲۰۰۰). بعد از بارگذاری نخستین، الگوریتم اجراشده، کلید اجرایی[1] به‌عنوان خروجی تولید می‌شود. به‌طورمعمول، دو معادلهٔ مهم در الگوریتم‌های رمز جریانی مورد استفادهٔ تحلیل‌گر قرار می‌گیرد: معادلهٔ بخش بروزکنندهٔ مقادیر حافظه‌ها و معادلهٔ بخش غیر خطی که از ترکیب آن دو کلید اجرایی تولید می‌شود (هاوْکس و رُز، ۲۰۰۰؛ احمدی و اقلیدس، ۲۰۰۹).

حملهٔ حدس و تعیین، شامل دو مرحله است. در مرحلهٔ نخست یا همان مرحلهٔ حدس، تعدادی از عناصر حافظه حدس زده می‌شود؛ سپس در مرحلهٔ دوم، که مرحلهٔ تعیین نامیده می‌شود، متغیرهای باقی‌مانده در معادلات اتصال پس از جای‌گذاری مقادیر حدس، تعیین می‌شوند(هاوْکس و رُز، ۲۰۰۰؛ احمدی و اقلیدس، ۲۰۰۹). بدین‌ترتیب، کلید اجرایی به‌عنوان خروجی به‌دست می‌آید و با کلید اجرایی اصلی، که به‌کمک یک جفت متن اصلی و متن رمزشدهٔ متناظر معلوم به‌دست آمده است، مقایسه می‌شود. درصورتی‌که دو کلید اجرایی یکسان باشند، حدس درست است؛ درغیراین صورت، مرحلهٔ حدس، تکرار و مقدار

[1] Keystream

پایهٔ حدس نیز نامیده می‌شود (احمدی و اقلیدس،۲۰۰۹). هرچه اندازهٔ پایهٔ حدس کوچک‌تر باشد، پیچیدگی حمله کمتر است.

با مطالعهٔ حملات حدس و تعیینی که تاکنون معرفی شده‌اند، آن‌ها را به دو دسته حملات حدس و تعیین اقتضایی[1] و حملات حدس و تعیین اکتشافی[2] می‌توان تقسیم‌بندی کرد. در حملات حدس و تعیین اقتضایی، تحلیل‌گر، بنا به تجربه و خلاقیت خود، نقاط ضعف الگوریتم رمزِ تحت بررسی را مد نظر قرار می‌دهد و در ابتدای حمله، پایهٔ حدسی را انتخاب می‌کند؛ سپس با این پایهٔ حدس و معادلات اتصال الگوریتم، سایر متغیرها را تعیین می‌کند. در این دسته از حملات به‌طورمعمول تحلیل‌گر معیار یا روشی مرحله‌به‌مرحله برای یافتن پایهٔ حدس نخستین بیان نمی‌کند. حملات حدس و تعیین اقتضایی اعمال‌شده به سامانه‌های رمزجریانی مانند A5/1 (گالیچ، ۱۹۹۷)،SOBER (دِ کانییری، ۲۰۰۱)، SNOW1.0 (هاوْکس و رُز، ۲۰۰۱؛ دو کانییر، ۲۰۰۱؛ اِکدال،۲۰۰۳) SOSEMANUK (تْسُنو و همکاران، ۲۰۰۶؛ لین و جی، ۲۰۰۹؛ فِنگ و همکاران، ۲۰۱۰) و ZUC (لین و همکاران، ۲۰۱۱) از نوع اقتضایی هستند؛ اما در حملات حدس 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 مرحله‌به‌مرحله در انواع دیگر تحلیل‌های رمز نیز صورت گرفته است. الگوریتم ارائه‌شده توسط *اِنگلَند* و همکارانش برای تحلیل آماری مقدار نخستین IV منتخب (اِنگلَند و همکاران، ۲۰۰۷) از این نمونه تلاش‌ها است.

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

در زمینهٔ حملات حدس و تعیین به رمزهای جریانی، دو نمونه از این تلاش‌ها برای یافتن یک راه حل مرحله‌به‌مرحله در(هاوْکس و رُز، ۲۰۰۰) و (احمدی و اقلیدس، ۲۰۰۹) بیان شده است. ایدهٔ *هاوْکس و رز* استفاده از معادلات مضارب چندجمله‌ای اتصال، علاوه‌بر دو معادلهٔ ثبات انتقال با پس‌خورد خطی و معادلهٔ بخش غیرخطی است (هاوْکس و رُز، ۲۰۰۰). این ایده در مرحلهٔ تعیین تأثیرگذار است. مؤلفین مقاله این حمله را به SSC-II و TIPSY اعمال کرده‌اند و به‌ترتیب به پیچیدگی از مرتبه‌های ($O(2^{41.7})$ و $O(2^{96})$) دست یافته‌اند. البته نتایج این حمله به دیگر سامانه های رمز جریانی کلمه‌گرا نتایج مناسبی را در بر نداشته است. این ایده منجر به افزایش تعداد معادلات می‌شود و چنان‌چه به روش اقتضایی صورت گیرد، ممکن است موجب افزایش پیچیدگی تحلیل حدس و تعیین شود. تلاش دیگری توسط *احمدی و اقلیدس* برای یافتن یک روش کلی برای حملهٔ حدس و تعیین انجام شده است. فکر اصلی این روش تشکیل جداول شاخص متناظر با معادلات مورد استفاده در حمله، برای الگوریتمی‌کردن حملهٔ حدس و تعیین است. حدس‌ها با جدول‌های شاخص بر اساس معیاری که در (احمدی و اقلیدس،۲۰۰۹) بیان شده است، زده می‌شود؛ سپس به‌ازای هر حدس، شاخص متناظر با آن از جدول حذف شده و الگوریتم وارد مرحلهٔ تعیین می‌شود. این روش حمله به الگوریتم TIPSY (هاوْکس و رُز، ۲۰۰۰)، SNOW1.0 (اِکدال و جُهانسن، ۲۰۰۰) و SNOW2.0 (اِکدال و جُهانسن، ۲۰۰۲) (الگوریتم‌های پیشنهاد شده به پروژهٔ اروپایی NESSIE) اعمال شده، به‌ترتیب پیچیدگی حملهٔ را به $O(2^{102})$، $O(2^{202})$ و $O(2^{256})$ کاهش داده است (احمدی و اقلیدس، ۲۰۰۹)، (احمدی و اقلیدس، ۲۰۰۵). این روش حمله همچنین به سامانهٔ رمز SOSEMANUK (بِروِین و همکاران، ۲۰۰۵) اعمال‌شده، مرتبه پیچیدگی را با مضرب 2^{-32} کاهش داده است (احمدی و اقلیدس، ۲۰۰۹)، (احمدی و همکاران، ۲۰۰۶).

ساختار مقاله به‌شرح زیر است: در بخش دوم ایدهٔ هاوْکس و رُز دربارهٔ استفاده از مضارب چندجمله‌ای اتصال در حملات حدس و تعیین معرفی شده است. بخش سوم به حملهٔ حدس و تعیین اکتشافی اختصاص داده شده است. در بخش چهارم حملهٔ حدس 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 پس‌خورد در حملات حدس و تعیین

در حملات حدس و تعیین اقتضایی، بعد از حدسِ تعدادی از متغیرهای حافظه، به‌طورمعمول از دو معادلهٔ ثبات انتقال با پس‌خورد خطی و تابع غیرخطی برای تعیین باقی متغیرهای

[1] Ad-hoc GD attacks
[2] Heuristic GD attacks

حافظه استفاده می‌شود. هاؤکس و رز بیان کردند که در حملهٔ حدس و تعیین، می‌توان از معادلات دیگری علاوه‌بر این دو معادله، بهره برد (هاؤکس و رُز، ۲۰۰۰). روش ساخت این معادلات به این صورت است که با فرض این‌که $p(x)$ چندجمله‌ای معادلهٔ بازگشتی LFSR باشد، با انتخاب یک چندجمله‌ای $q(x)$ و ضرب آن در $p(x)$، معادلات اضافی به‌صورت $r(x)=q(x)p(x)$ تولید می‌شود (هاؤکس و رُز، ۲۰۰۰). $r(x)$ مضربی از چندجمله‌ای بازگشتی LFSR است (هاؤکس و رُز، ۲۰۰۰). متأسفانه، هاؤکس و رز نتوانستند ویژگی خاصی را برای $q(x)$ به‌دست بیاورند، طوری‌که منجر به یک حملهٔ حدس و تعیین بهینه شود؛ امّا حدس می‌زنند که چندجمله‌ای‌هایی از $r(x)$ مفیدند که دارای درجه[1] و وزن[2] کمتری باشند. آنها از این ایده برای بهبود حملهٔ حدس و تعیین به TIPSY با پیچیدگی از مرتبهٔ $O(2^{96})$ استفاده کردند (هاؤکس و رُز، ۲۰۰۰).

$$p(x) = x^{13} + x^4 + x + \alpha \qquad (۱)$$

$$S_{t+13} = S_{t+4} + S_{t+1} + \alpha S_t \quad \alpha = 0\text{xEDED} \qquad (۲)$$

معادله بخش غیر خطی به‌صورت زیر است:

$$v_t = f(S_t \oplus S_{t+11}) + S_{t+5} + S_{t+10} \mod 2^{16} \qquad (۳)$$

مضارب مورد استفاده در حملهٔ حدس و تعیین *هاؤکس* و *رز* به این سامانه نیز به‌صورت زیر است:

$$p^2(x) = x^{26} + x^8 + x^2 + \alpha^2 \qquad (۴)$$

$$\begin{aligned} r_1(x) &= (x^9 + x^6 + x^3 + 1).p(x) \\ &= x^{22} + x^{19} + x^{16} + \alpha x^9 + \alpha x^6 \\ &\quad + \alpha x^3 + x + \alpha \end{aligned} \qquad (۵)$$

$$\begin{aligned} r_2(x) &= (x^{12} + \alpha x^{11} + \alpha^2 x^{10} \\ &\quad + x^6 + x^3 + \alpha x^2 + \alpha^2 x + 1).p(x) \\ &= x^{25} + \alpha x^{24} + \alpha^2 x^{23} + x^{19} \\ &\quad + (\alpha^3 + 1)x^{10} + \alpha^2 x^5 + (\alpha^3 + 1)x \\ &\quad + \alpha \end{aligned} \qquad (۶)$$

در معادلات بالا علامت $+$ بیان‌گر جمع پیمانه‌ای در میدان 2^{16} است. این حمله با استفاده از معادلات (۱) تا (۶) به TIPSY اعمال شده، تعداد حدس برابر با هفت به‌دست آمده است. حمله شامل دو مرحله است: مرحلهٔ حدس و مرحلهٔ تعیین. در مرحلهٔ نخست شش متغیر حدس زده شده است. با این حدس‌ها، مقادیر معادلهٔ بخش غیرخطی برای v_{t+23} تعیین می‌شود. بنابراین، می‌توان مقدار v_{t+23} به‌دست آمده را با مقدار v_{t+23} مشاهده‌شده مقایسه کرد. ادعا شده است که با داشتن مقدار v_{t+23} و متوازن‌بودن معادلهٔ بخش غیرخطی، فضای جستجو برای شش حدس از مرتبهٔ $O(2^{96})$ به $O(2^{80})$ کاهش می‌یابد. درمجموع پیچیدگی کل حمله از مرتبهٔ $O(2^{16\times 80}) = O(2^{96})$ است (هاؤکس و رُز، ۲۰۰۰).

۳- حمله حدس و تعیین اکتشافی

ایدهٔ دوم (احمدی و اقلیدس، ۲۰۰۹) بر اساس ارائهٔ یک الگوریتم برای اجرای حملات حدس و تعیین به سامانه‌های رمز جریانی کلمه‌گرا، با استفاده از مفهومی به نام جدول شاخص[3] تحقق می‌یابد. این الگوریتم، حملهٔ حدس و تعیین اکتشافی[4] نامیده شده است (احمدی و اقلیدس، ۲۰۰۹). تنها محدودیت حملهٔ حدس و تعیین اکتشافی، یکسان‌بودن اندازهٔ متغیرهای معادلات، معرّف رمز جریانی است.

در این روش حمله، دسته معادلات استخراج شده از رمز جریانی به‌عنوان ورودی به این الگوریتم محسوب می‌شود. برای رمزهای جریانی، می‌توان دو دسته معادلات در نظر گرفت. معادلات به‌روزکردن حالت و معادلات تولیدکنندهٔ دنبالهٔ کلید اجرایی[5]. برای جایگزینی بهتر الگوریتم با دستهٔ معادلات، می‌توان معادلات دیگری را نیز از الگوریتم رمز استخراج کرد. این معادلات خود تابعی از متغیرهای حافظه هستند. با فرض تعداد معادلات استخراج‌شده برابر rباشد، معادلات به‌صورت زیر است:

$$\begin{aligned} &f_1(S_{1,t+\Delta}, S_{2,t+\Delta}, \ldots, S_{k_1,t+\Delta}) = 0 \\ &f_2(S_{1,t+\Delta}, S_{2,t+\Delta}, \ldots, S_{k_2,t+\Delta}) = 0 \\ &\quad \vdots \\ &f_r(S_{1,t+\Delta}, S_{2,t+\Delta}, \ldots, S_{k_r,t+\Delta}) = 0 \\ &; \quad 0 \le \Delta < n \end{aligned} \qquad (۷)$$

[1] Low degree
[2] Low weight
[3] Index table
[4] Heuristic GD attack
[5] connection equation

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

$$T_i = \begin{bmatrix} S_{1,t} & S_{2,t} & \dots & S_{k_i,t} \\ S_{1,t+1} & S_{2,t+1} & \dots & S_{k_i,t+1} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & & \cdot \\ S_{1,t+n-1} & S_{2,t+n-1} & \dots & S_{k_i,t+n-1} \end{bmatrix} \quad (۸)$$

دراین‌صورت هر معادله دارای ماتریس شاخص زمانی به شکل زیر است:

$$M = \begin{bmatrix} 1 & 2 & \dots & k_i \\ 1+1 & 2+1 & \dots & k_i+1 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & & \cdot \\ 1+n-1 & 2+n-1 & \dots & k_i+n-1 \end{bmatrix} \quad (۹)$$

بر اساس ماتریس شاخص زمانی، *جدول شاخص* به‌صورت (جدول- ۱) تشکیل می‌شود:

(جدول- ۱): جدول شاخص برای معادلات(۷)

۱	۲	...	k_i
۱+۱	۲+۱	...	k_i+ ۱
...	...	...	...
۱+n-۱	۲+n-۱	...	k_i+n-۱

جدول (۱) به‌عنوان جدول شاخص در حملهٔ حدس و تعیین اکتشافی استفاده می‌شود. در این روش، متناظر با هر معادله، یک جدول شاخص تشکیل می‌شود که درایه‌های 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 بیان‌گر یک معادله در یک زمان مشخص است.جداول شاخص به تحلیل‌گر کمک می‌کند که یک برآورد از تعداد حضور یک شاخص و تعداد ترکیب‌های شاخص‌های مختلف در هر ردیف از جداول شاخص داشته باشد. همچنین، در این روش تحلیل‌گر نیازی به حل هم‌زمان معادلات اتصال در ابتدای حمله ندارد. بدین ترتیب تحلیل‌گر می‌تواند بر اساس معیارهایی خاص به‌صورت مرحله‌به‌مرحله به حدس مجموعه‌ای از متغیرها که پایهٔ حدس نامیده می‌شود، بپردازد. این معیارها که معیار "د" نامیده شده‌اند، به‌صورت زیر است (احمدی و اقلیدس، ۲۰۰۹):

معیار "د": برای یافتن یک پایهٔ 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، به‌صورت 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 مجهول کمتری در جداول شاخص است (احمدی و اقلیدس، ۲۰۰۵ و ۲۰۰۹).

انتخاب هر حدس توسط الگوریتم حملهٔ حدس و تعیین اکتشافی بر اساس معیار "د" صورت می‌گیرد. سپس این شاخص از جدول‌های شاخص حذف می‌شود. در مرحلهٔ تعیین، الگوریتم در جدول شاخص با بررسی ردیف‌ها، دسته معادلات تک مجهولی یا دو مجهولی یا بیشتر را جستجو می‌کند. اندازهٔ دستگاه معادلات را تحلیل‌گر انتخاب می‌کند. از سوی دیگر، درصورت یافتن دسته معادلات، شاخص متناظر با مجهولات را از جدول‌های شاخص حذف می‌کند. دوباره الگوریتم وارد مرحلهٔ حدس می‌شود و مراحل پیشین تکرار می‌شود تا تمامی شاخص‌های جدول حذف شوند.

حملهٔ اکتشافی بالا در (احمدی و اقلیدس، ۲۰۰۵) به‌عنوان حملهٔ حدس و تعیین پیشرفته نامیده شده است. در (احمدی و اقلیدس، ۲۰۰۹) همین الگوریتم حمله با استفاده از نمودار ترلیس و معیار شبه‌ویتربی با بیان دیگر به‌صورت الگوریتمی بیان شده و این روش به نام حملهٔ حدس و تعیین اکتشافی نامیده شده است. حملهٔ حدس و تعیین اکتشافی به رمز TIPSY با پیچیدگی از مرتبهٔ $O(2^{102})$ همراه با پایهٔ حدس با اندازهٔ شش اعمال شده است (احمدی و اقلیدس، ۲۰۰۹). بخشی از پیچیدگی به‌دست آمده مربوط به حل شش دستگاه سه معادله سه مجهول است. این حمله به رمز SNOW 1.0 نیز با پیچیدگی $O(2^{202})$ و اندازهٔ پایهٔ حدس شش اعمال شده است (احمدی، ۱۳۸۴).

۴- بهبود حملهٔ حدس و تعیین اکتشافی

در این بخش ضمن بیان یک روش برای بهبود حملهٔ حدس و تعیین اکتشافی، رمزهای TIPSY و SNOW 1.0 تحلیل شده‌اند؛ سپس، نتایج این حمله با حملات حدس و تعیین اقتضایی و اکتشافی پیشین مقایسه شده است. حملهٔ حدس و تعیین اکتشافی به دو صورت می‌تواند بهبود یابد. یکی در مرحلهٔ حدس که با بهبود معیار "د" صورت می‌گیرد. دیگری، بهبود مرحلهٔ تعیین است، به‌طوری‌که تعداد هر چه بیش‌تری از شاخص‌ها به‌ازای هر حدس تعیین شوند. در این مقاله از ایدهٔ بیان‌شده در بخش دوم برای بهبود مرحلهٔ 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، به‌عنوان معادلات کمکی، بر اساس مضارب چندجمله‌ای پس‌خورد (یکی از معادلات اصلی) به‌دست می‌آیند.

اکنون جدول‌های شاخص متناظر با معادلات فرعی را، علاوه‌بر معادلات اصلی، به‌عنوان ورودی الگوریتم حملهٔ حدس و تعیین اکتشافی به‌کار می‌گیریم. معادلات فرعی از مضارب چندجمله‌ای با وزن کمینه انتخاب می‌شوند. بنابراین تنها مضاربی که ضرایب آن‌ها یعنی $q(x)$ دارای وزن دو است، در نظر گرفته می‌شود. از طرفی برای تکرار شاخص‌های معادلات اصلی، $q(x)$ باید دارای یک جملهٔ ثابت باشد؛ یعنی، $q(x)=x^n+1$ به‌منظور کاهش وزن معادلهٔ فرعی، n را از میان تفاضل‌های دوبه‌دوی درجات جملات چندجمله‌ای پس‌خورد انتخاب می‌کنیم. دراین‌صورت 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 پس‌خورد آن‌ها در توسیع میدان $GF(2)$ باشد و همچنین جمع ضرایب جملات هم‌درجه در میدان $GF(2)$ صفر شود.

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

M3			
۲۶	۸	۲	۰
۲۷	۹	۳	۱
.	.	.	.
.	.	.	.
.	.	.	.
۵۴	۳۶	۳۰	۲۹
۵۵	۳۷	۳۱	۲۹

M2			
۱۱	۱۰	۵	۰
۱۲	۱۱	۶	۱
.	.	.	.
.	.	.	.
.	.	.	.
۳۹	۳۸	۳۳	۲۸
۴۰	۳۹	۳۴	۲۹

M1			
۱۳	۴	۱	۰
۱۴	۵	۲	۱
.	.	.	.
.	.	.	.
.	.	.	.
۴۱	۳۲	۲۹	۲۸
۴۲	۳۳	۳۰	۲۹

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

۴-۱- حملهٔ حدس و تعیین اکتشافی بهبودیافته به TIPSY

در این حمله، معادلات اصلی (۱) و (۳) و معادلهٔ فرعی (۴) به‌عنوان دسته معادلات ورودی به الگوریتم حمله استفاده می‌شود. در معادلات این بخش علامت + بیان‌گر جمع پیمانه‌ای در میدان $GF(2^{16})$ است. چندجمله‌ای به‌کاررفته در معادلهٔ فرعی، مضرب توان دوم چندجمله‌ای پس‌خورد در الگوریتم TIPSY است. جدول‌های شاخص M1، M2 و M3 به‌ترتیب متناظر با چندجمله‌ای پس‌خورد، معادلهٔ بخش غیرخطی و معادلهٔ فرعی است که در (جدول- ۲) نشان داده می‌شود.

تعداد ردیف‌های جدول‌های شاخص حداقل بایستی برابر با تعداد خانه‌های حافظهٔ الگوریتم رمز باشد (احمدی و اقلیدس، ۲۰۰۹) تا تمام شاخص‌های خانه‌های حافظهٔ 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 پایهٔ حدس برابر با شش به‌دست آمده است. مراحل

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

۴-۱-۱- پیچیدگی حمله

در جدول (۳)، با توجه به ستون حدس، پایهٔ حدس، مجموعهٔ {۲۶، ۲۷، ۲۱، ۲۲، ۱۷، ۲۳} است. در گام‌های ۱۶ و ۲۸ از جدول (۳)، دو دستگاه دو معادله و دو مجهول به‌صورت زیر تولید می‌شوند:

$$K_1 = K_2 \oplus S_{14} \oplus \alpha S_{13} \quad (۱۰)$$

$$v_{t+3} = f(K_3 \oplus S_{14}) + K_4 + S_{13} \quad (۱۱)$$

و

$$K_6 = K_7 \oplus S_{19} \oplus \alpha S_{18} \quad (۱۲)$$

$$v_{t+8} = f(K_8 \oplus S_{19}) + K_9 + S_{18} \quad (۱۳)$$

که مقادیر K_i و v_{t+j} معلوم است. با جای‌گذاری معادلات (۱۰) و (۱۲) به‌ترتیب در (۱۱) و (۱۳) معادلات یک مجهولی زیر به‌دست می‌آید:

$$f(K \oplus \alpha S_{13}) + S_{13} = K' \quad (۱۴)$$

$$f(Q \oplus \alpha S_{18}) + S_{18} = Q' \quad (۱۵)$$

که در معادلات (۱۴) و (۱۵) $K = K_1 \oplus K_2 \oplus K_3$، $K' = v_{t+23} - K_4$، $Q = K_6 \oplus K_7 \oplus K_8$ و $Q' = v_{t+8} - K_9$ است. با توجه به غیرخطی‌بودن این معادلات، برای حل هر یک از آنها نیاز به یک جدول پیش‌پردازش است که قبل از اعمال حمله به‌دست می‌آید (احمدی، ۱۳۸۴). بنابراین، با وجود این دو جدول پیش‌پردازش پیچیدگی حمله از مرتبهٔ $O(2^{6\times 16})=O(2^{96})$ است.

(جدول- ۳): مراحل اعمال حمله به TIPSY

گام	حدس	معادلات مورد استفاده	شاخص‌های مقادیر معلوم	مقادیر تعیین‌شده
۱	۲۶	-	-	-
۲	۲۷	-	-	-
۳	۲۱	-	-	-
۴	-	M2	۲۱،۲۶،۲۷	۱۶
۵	۲۲	-	-	-
۶	-	M2	۱۶،۲۱،۲۲	۱۱
۷	۱۷	-	-	-
۸	-	M2	۱۷،۲۲،۲۷	۲۸
۹	-	M2	۱۱،۱۶،۱۷	۶
۱۰	۲۳	-	-	-
۱۱	-	M1	۲۲،۲۳،۲۶	۳۵
۱۲	-	M2	۱۷،۲۲،۲۳	۱۲
۱۳	-	M2	۶،۱۱،۱۲	۱
۱۴	-	M3	۱،۳،۲۷	۹
۱۵	-	M1	۹،۱۲،۲۱	۸
۱۶	-	M1,M2	۳،۸،۱۷،۲۶	۱۳،۱۴
۱۷ الی ۲۷	-	M1,M2,M3	با استفاده از متغیرهای معلوم قبلی و حل معادلات یک مجهولی	۱۰،۲۵،۳۴،۳۳،۳۲، ۳۱،۴۰،۴۴،۴۹،۵۱،۵۲
۲۸	-	M1,M2	۸،۱۳،۲۲،۳۱	۱۸،۱۹
۲۹ تا انتها	-	M1,M2,M3	تعیین باقی‌ماندهٔ شاخص‌ها	

۴-۲- حملهٔ حدس و تعیین اکتشافی بهبودیافته به SNOW 1.0

SNOW 1.0 (اِکدال و جُهانسن، ۲۰۰۰) یک الگوریتم رمز جریانی کلمه‌گرا است. ساختار این الگوریتم از دو بخش به‌روزرسانی و بخش غیرخطی تشکیل شده است. بخش به‌روزرسانی الگوریتم مبتنی بر ثبات انتقال با پس‌خورد خطی است. این بخش دارای شانزده طبقه حافظه‌های ۳۲بیتی در میدان $GF(2^{32})$ است. معادلهٔ بازگشتی و چندجمله‌ای متناظر با آن به‌صورت زیر است:

$$S_{t+16} = \alpha(S_{t+9} \oplus S_{t+3} \oplus S_t) \quad (۱۶)$$

$$p(x) = \alpha^{-1}x^{16} + x^9 + x^3 + 1 \in F_{2^{32}}[x] \quad (۱۷)$$

علامت + در معادلات این بخش بیان‌گر جمع پیمانه‌ای در $GF(2^{32})$ است. بخش غیر خطی (FSM) الگوریتم دارای دو حافظهٔ ۳۲بیتی $R1$ و $R2$ است که با یک جعبهٔ جانشینی به یکدیگر مرتبط شده‌اند. معادلات بخش غیر خطی به‌صورت زیر است:

$$R1_t = ((W_{t-1} + R2_{t-1}) <<<_7) \oplus R1_{t-1} \quad (۱۸)$$

$$R2_t = S\_Box(R1_{t-1}) \quad (۱۹)$$

$$W_t = (S_{t+15} + R1_t) \oplus R2_t \quad (۲۰)$$

(جدول- ۴): جدول‌های شاخص M1، M2 و M3 به‌ترتیب متناظر با معادلات (۱۶)، (۲۳) و (۲۴)

M1			
۰	۳	۹	۱۶
۱	۴	۱۰	۱۷
.	.	.	.
.	.	.	.
.	.	.	.
۱۸	۲۱	۲۷	۳۴
۱۹	۲۲	۲۸	۳۵

M2			
۰	۱۵	۴۹	۵۰
۱	۱۶	۵۰	۵۱
.	.	.	.
.	.	.	.
.	.	.	.
۱۸	۳۳	۶۷	۶۸
۱۹	۳۴	۶۸	۶۹

M3					
۰	۶	۹	۱۲	۱۶	۱۹
۱	۷	۱۰	۱۳	۱۷	۲۰
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
۱۸	۲۴	۲۷	۳۰	۳۴	۳۷
۱۹	۲۵	۲۸	۳۱	۳۵	۳۸

$$Z_t = W_t \oplus S_t \quad (۲۱)$$

W خروجی بخش غیرخطی و Z خروجی الگوریتم است. با ترکیب معادلات (۱۸) ، (۱۹) و (۲۰) مقدار حافظهٔ $R1$ از رابطه زیر به‌دست می‌آید:

$$R1_t = [((S_{t+14} + R1_{t-1}) \oplus S\_Box(R1_{t-2})) + S\_Box(R1_{t-2})) <<<_7] \oplus R1_{t-1} \quad (۲۲)$$

با ترکیب روابط (۱۹)، (۲۰) و (۲۱) معادلهٔ خروجی الگوریتم به‌صورت زیر ساده می‌شود:

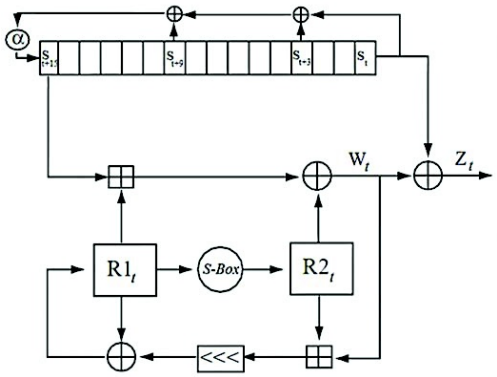
$$Z_t = [(S_{t+15} + R1_t) \oplus S\_Box(R1_{t-1})] \oplus S_t \quad (۲۳)$$

برای درک بهتر عملکرد SNOW 1.0، در (شکل- ۱) شمای رمز جریانی SNOW 1.0 نشان داده شده است.

برای اعمال حملهٔ حدس و تعیین اکتشافی از معادلات اصلی (۱۶) و (۲۳) و معادلهٔ فرعی زیر استفاده می‌شود:

$$S_{t+19} = \alpha(\alpha^{-1}S_{t+16} \oplus S_{t+12} \oplus S_{t+9} \oplus S_{t+6} \oplus S_t) \quad (۲۴)$$

معادلهٔ (۲۴) از ضرب دو جمله‌ای (x^3+1)، به‌عنوان ضریب، در چندجمله‌ای مشخصه به‌دست آمده است. درجه این دو جمله‌ای طبق روش ارائه‌شده در بخش چهار به‌دست آمده است. در جدول (۴)، جدول‌های شاخص متناظر با معادلات (۱۶)، (۲۳) و (۲۴) نمایش داده شده است. مراحل اعمال حمله حدس و تعیین اکتشافی بهبودیافته به SNOW 1.0 در جدول (۵) نشان داده می‌شود. پایهٔ حدس به‌دست آمده با اندازهٔ ۵ برابر $\{۵۰، ۲۲، ۲۵، ۱۶، ۱۹\}$ است.



(شکل- ۱): الگوریتم SNOW 1.0 (اِکدال و جُهانسن، ۲۰۰۰)

۴-۲-۱- پیچیدگی حمله

با توجه به خطی‌بودن معادلات (۱۶) و (۲۴) در حل دستگاه‌های دو معادله دومجهولی در طی مرحلهٔ تعیین، نیازی به تشکیل جدول‌های پیش پردازش نیست. معادلهٔ (۲۳) غیر خطی است، اما در طی حمله به حل این معادله نیازی نیست. بنابراین پیچیدگی محاسبات حمله تنها برابر با همان پیچیدگی محاسباتی پایهٔ حدس با اندازه ۵ است. پیچیدگی این حمله از مرتبهٔ $O(2^{5\times 32})=O(2^{160})$ است که نسبت به حملهٔ حدس و تعیین اکتشافی پیشین (احمدی و اقلیدس، ۲۰۰۹) از مرتبهٔ $O(2^{42})$ کاهش یافته است.

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

گام	حدس	معادلات مورد استفاده	شاخص‌های مقادیر معلوم	مقادیر تعیین‌شده
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 مجهول)	۰،۳،۶،۹،۱۲
۲۲		M1,M3	۱۶،۱۹،۲۲،۲۵،۳۲	۲۸،۳۵
۲۳	۵۰	-	-	-
۲۴تا انتها	-	M2	تعیین شاخص‌های باقیمانده	

۴-۳- مقایسه نتایج حملات

در جدول (۶) نتایج حملات حدس و تعیین اقتضایی و اکتشافی اعمال‌شده به الگوریتم‌های TIPSY و SNOW 1.0 با نتایج حملات حدس و تعیین اکتشافی بهبودیافته در این مقاله مقایسه شده است.

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

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

الگوریتم	حملات حدس و تعیین					
	اقتضایی		اکتشافی			
			پیشین		بهبود یافته	
	پیچیدگی مرتبه	پایهٔ حدس	پیچیدگی مرتبه	پایهٔ حدس	پیچیدگی مرتبه	پایهٔ حدس
TIPSY	$O(2^{96})$	۷	$O(2^{102})$	۶	$O(2^{96})$	۶
SNOW1.0	$O(2^{224})$	۶	$O(2^{202})$	۶	$O(2^{160})$	۵

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 پایهٔ حدس، معادلات اصلی و معادلات فرعی (کمکی) در حملات حدس و تعیین، ایدهٔ استفاده از مضارب چندجمله‌ای مشخصه به‌عنوان معادلات فرعی و روش استفاده از جدول‌های شاخص در حملهٔ حدس و تعیین اکتشافی به‌طورکامل بیان شده است. در ادامه، با استفاده از دو معادلهٔ اصلی و یک معادلهٔ فرعی حملات حدس و تعیین اکتشافی به سامانه‌های رمز جریانی TIPSY و SNOW 1.0 اعمال شده است. نتایج اعمال حملهٔ پیشنهادی حدس و تعیین اکتشافی به الگوریتم TIPSY با پیچیدگی $O(2^{96})$ نشان از بهبود این حمله نسبت به حملهٔ حدس و تعیین اکتشافی پیشین با پیچیدگی $O(2^{102})$ دارد. از سوی دیگر، پیچیدگی این حمله و حملهٔ اقتضایی پیشین به TIPSY با هم برابر و از مرتبهٔ $O(2^{96})$ است؛ درحالی‌که پایهٔ حدس از هفت به شش کاهش یافته است. همچنین، حملهٔ پیشنهادی حدس و تعیین اکتشافی به الگوریتم SNOW1.0 دارای پیچیدگی از مرتبهٔ $O(2^{160})$ است، که نسبت به حملهٔ حدس و تعیین اکتشافی پیشین از مرتبهٔ $O(2^{42})$ کاهش یافته است. از سوی دیگر، پیچیدگی این حمله نسبت به حملهٔ حدس و تعیین اقتضایی با پیچیدگی $O(2^{224})$ کاهش قابل توجهی را نشان می‌دهد.

۶- مراجع

احمدی هادی (۱۳۸۴)، بررسی حملات حدس وتعیین به سیستم‌های رمز دنباله‌ای استاندارد NESSIE و ارائهٔ یک طرح بهبودیافته برای رمزهای دنباله‌ای با انتقال کلمه‌به‌کلمه، 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.

Ahmadi H., Eghlidos T. (2009), heuristic guess-and-determine attacks on stream ciphers, IET information security, 2009, Vol. 3, lss. 2, pp. 66-73, 2009.

Bervain C., Billet O., Canteaut A (2005), "SOSE-MANUK, 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.k-uleuven.be/nessie/worksho/, 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-Verlage; LNCS 4859, 2007, pp. 268-281.

Feng Xiutao, Liu Jun, Zhou Zhaocun, 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.

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/sosemanukp3.html, accessed on 15 July 2014.

محمد صادق نعمتی‌نیا کاردانی و کارشناسی خود را در گرایش برق- الکترونیک به‌ترتیب از دانشگاه‌های بیرجند و حکیم‌سبزواری 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 علاقهٔ ایشان، رمزهای متقارن، رمزنگاری کلید عمومی است.

نشانی رایانامهٔ ایشان عبارت است از:

nemati.skh.ict@chmail.ir

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

نشانی رایانامهٔ ایشان عبارت است از:

teghlidos@sharif.edu

علی پاینده، مدرک کارشناسی ارشد و دکترای خود را به‌ترتیب در سال‌های ۱۳۷۳ و ۱۳۸۳در رشتهٔ مهندسی برق از دانشگاه تربیت مدرس و دانشگاه صنعتی خواجه نصیرالدین طوسی دریافت کرده است. ایشان از سال ۱۳۷۳ تا ۱۳۸۳ مدیریت تحقیقات در حوزهٔ امنیت ارتباطات ماهواره‌ای را در انجمن تحقیقات علوم کاربردی ایران عهده‌دار بوده‌اند. ایشان هم‌اکنون استادیار مجتمع فناوری اطلاعات و ارتباطات دانشگاه صنعتی مالک اشتر تهران هستند 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، رمزنگاری، پروتکل‌های امنیتی، امنیت رایانش ابری، ارتباطات امن و ارتباطات ماهواره‌ای است.

نشانی رایانامهٔ ایشان عبارت است از:

payandeh@mut.ac.ir