

تحلیل الگوریتم رمز جریانی 'HC-256'

بر اساس حمله تمایز

احمدرضا ویزندان^۱، جواد شیخ زادگان^۲ و عبدالرسول میرقدری^۱
^۱ دانشگاه امام حسین علیه السلام، ^۲ پژوهشکده پردازش هوشمند علائم

چکیده:

رمزهای جریانی یکی از مهم‌ترین انواع الگوریتم‌های رمزنگاری متقارن است که به لحاظ قابلیت‌های ویژه و مناسب در برخی از کاربردهایی مانند امنیت شبکه‌ها و ارتباطات مخابراتی، ارزیابی امنیتی آن‌ها در حوزه شبکه‌های ارتباطی از اهمیت به‌سزایی برخوردارند و پروژه بین‌المللی eSTREAM در راستای افزایش فعالیت در این شاخه رمزنگاری نقش به‌سزایی ایفا نمود. در این مقاله یکی از الگوریتم‌های رمز جریانی پایه‌آرایه‌ای با استفاده از حمله تمایز، مورد ارزیابی تحلیلی قرار می‌گیرد. در واقع ایده اصلی این مقاله در معرفی دو دسته تمایزگر، تمایزگر پایه و بهبودیافته بر روی الگوریتم رمز جریانی 'HC-256' می‌باشد که در حمله پایه، نیاز به $2^{56/3}$ رشته کلید خروجی می‌باشد، در حالی که در حمله بهبودیافته نیاز به $2^{55/4}$ رشته کلید خروجی می‌باشد. بنابراین در حمله بهبودیافته به‌طور تقریبی سی مرتبه کمتر از حمله پایه، نیاز به رشته کلید خروجی از الگوریتم رمز داریم.

واژگان کلیدی: حمله تمایز، تحلیل الگوریتم، eSTREAM، 'HC-256'

۱- مقدمه

امروزه با افزایش پیچیدگی شبکه‌های مخابراتی و رایانه‌ای، کنترل آسیب‌پذیری‌ها و تهدیدها یکی از مسایل جدی می‌باشد. لذا یکی از راه‌های ایجاد امنیت اطلاعات در برابر حمله و سایر خرابی‌ها، در سامانه‌های ارتباطی آتی، توسعه جدی در نظریه و مدل‌سازی ارزیابی‌های امنیتی سیستم‌های رمزکننده می‌باشد. شانون بنیان‌گذار نظریه اطلاعات، سیستم رمز امن کاملی را پیشنهاد کرد که در آن هر حرف از پیام اصلی با حرفی از یک دنباله کاملاً تصادفی ترکیب می‌شود و پیام رمزی را تشکیل می‌دهد (Menezes, 1965). از آنجایی که این دنباله ترکیب‌شده با پیام اصلی، به‌طور کامل تصادفی است، امنیت سیستم را تضمین می‌کند. رمزهای جریانی که یکی از مهم‌ترین شیوه‌های رمزنگاری متقارن است، به‌طور منحصربه‌فرد تک‌تک حروف متن پیام آشکار را رمز می‌کند که این تبدیل، با زمان تغییر می‌کند؛ که در مقایسه با شیوه دوم رمزهای متقارن، رمزهای قالبی، یک

قالب از حروف متن پیام آشکار را رمز می‌کند و این تبدیل رمزنگاری، متغیر با زمان نمی‌باشد (Menezes, 1965). به‌طور معمول رمزهای جریانی نسبت به رمزهای قالبی در کاربردهای سخت‌افزاری سریع‌تر بوده و پیچیدگی مدارات سخت‌افزاری کمتری دارند. همچنین آن‌ها قابلیت‌های ویژه و مناسب‌تری در برخی از کاربردها (به‌طور نمونه در کاربردهای مخابراتی) مانند کاربردهایی که با حافظه‌های میانی^۱ محدود و انتشار خطای محدود سرو کار دارند، از خود نشان می‌دهند (Rijmen, 2010). شاپان ذکر است، بعضی از رمزهای جریانی در کاربردهای نرم‌افزاری در مقایسه با رمزهای قالبی مانند AES، چهار الی پنج برابر سریع‌تر می‌باشند. در حال حاضر دانش نظری زیادی بر روی رمزهای جریانی وجود دارد و اصول طراحی و تحلیل‌های گوناگونی بر روی این‌گونه رمزها ارائه گردیده است. در این اواخر، پیشنهادها زیادی برای رمزهای جریانی مشخصی مشاهده گردید (ECRYPT, 2008 and NESSIE, 1999). هم‌چنین بسیاری از رمزهای جریانی

¹ Buffer

انتقال کلمه به کلمه و مبتنی بر چرخش آرایه‌ها و جمع‌کننده‌ها بوده و در دسته‌بندی رمزهای جریانی از گروه رمزهای هم‌زمان محسوب می‌شوند. تحلیل‌های اولیه طراح بر روی این رمز، نشان می‌دهد که به‌دست آوردن کلید در این رمز بسیار سخت، و لازمه آن جستجوی کامل فضای کلید است. با توجه به این که اغلب ساختار رمزهای جریانی از یک مولد رشته‌کلید شبه‌تصادفی برای تولید یک رشته طولانی از علائم دودویی استفاده می‌کنند، لذا امنیت یک رمز جریانی، به‌طور دقیق وابسته به چگونگی شباهت این رشته تولیدشده به یک رشته تصادفی واقعی می‌باشد. در حمله تمایز، تحلیل‌گر تلاش می‌نماید که نشان دهد رفتار رشته تولیدشده، مانند یک رشته تصادفی واقعی نمی‌باشد (Hell, et al, 2009). در بخش حمله تمایز پایه بر روی این الگوریتم، نشان داده شده که این حمله نیاز به 2^{56} خروجی الگوریتم رمز دارد و در نهایت این مقدار در حمله بهبودیافته کاهش می‌یابد.

پردازش الگوریتم رمز 'HC-256' به‌صورت کلمه‌ای⁴ است و طول هر کلمه ۳۲ بیت می‌باشد و الگوریتم از یک کلید اصلی و بردار حالت اولیه⁵ به‌طول ۲۵۶ بیت برای تولید رشته‌کلید خروجی بهره می‌جوید. از آن جایی که این الگوریتم به شکل ممتازی طراحی گردیده و تاکنون مورد تحلیل قرار نگرفته است، بنابراین دستیابی به نتایج تحلیل، جذاب به‌نظر می‌رسد. در واقع هدف از این مقاله ارزیابی تحلیلی الگوریتم رمز 'HC-256' مبتنی بر حمله تمایز می‌باشد که در ادامه به‌دقت یک گروه از تمایزگرها مورد بررسی قرار خواهد گرفت که نیاز به آزمایش تقریباً $2^{55.6}$ معادله خطی دارد. هر کدام از اجزای این معادلات شامل خروجی رشته‌کلید شبه تصادفی الگوریتم می‌باشد که با توجه به این موضوع، تعداد رشته‌کلیدهای مورد نیاز از خروجی الگوریتم در این حمله برابر $2^{55.4}$ خواهد شد و نسبت به حمله پایه به‌طور تقریبی سی برابر بهبودی مشاهده می‌گردد.

این مقاله از بخش‌هایی به شرح ذیل تشکیل شده است. در بخش بعدی نمادهایمان را تعریف می‌کنیم. در بخش سه به‌طور مختصر الگوریتم 'HC-256' معرفی می‌گردد. حمله تمایز پایه در بخش چهار ارائه می‌گردد. در بخش پنج حمله تمایز بهبودیافته بیان شده و آخرین بخش به نتیجه‌گیری اختصاص پیدا خواهد کرد.

اختصاصی شده، در عمل استفاده می‌گردد که برخی از آن‌ها در ابتدا به‌صورت محرمانه استفاده می‌شد که بعدها با انتشار آن‌ها ضعف‌هایی در رد آن‌ها مشاهده گردید، به‌عنوان مثال الگوریتم A5 مورد استفاده در شبکه تلفن همراه GSM و RC4 (Wikipedia, 2008). در کل می‌توان الگوریتم‌های رمز جریانی را به دو گروه رمز جریانی هم‌زمان¹ و غیرهم‌زمان² تقسیم کرد. در رمزهای جریانی هم‌زمان، مولد رشته‌کلید شبه‌تصادفی، غیر وابسته به متن رمزی و متن آشکار می‌باشد؛ در صورتی که در رمز جریانی غیرهم‌زمان رشته‌کلید رمز وابسته به متن رمزی و متن آشکار علاوه بر کلید اصلی می‌باشد. امروزه الگوریتم‌های رمز جریانی پیشرفته در چندین ساختار طراحی می‌گردند که یکی از آن‌ها استفاده از آرایه‌های بزرگ در حالت داخلی³ می‌باشد که رشته‌کلید تولیدشده، تابعی از محتویات این آرایه است (Paul and Preeel, 2005). گفتنی است که پس از اتمام فرآیند انتخاب استاندارد رمزگذاری پیشرفته (AES)، رمزهای قالبی کانون توجه جامعه رمزنگاری گردید. برخی از افراد بیان داشتند که آیا هنوز هم، برنامه عملی برای رمزهای جریانی می‌تواند وجود داشته باشد؟ و یا دلیلی برای انجام تحقیقات روی این دسته از الگوریتم‌ها وجود دارد؟

شبکه ECRYPT پروژه چندمرحله‌ای eSTREAM را جهت شناسایی و بررسی رمزهای جریانی جدید در سال ۲۰۰۴ شروع کرد و در سال ۲۰۰۸ به اتمام رسانید. این پروژه در دو دسته مجزا اجرا گردید: رمزهای جریانی جهت کاربردهای نرم‌افزاری با سرعت بالا و رمزهای جریانی جهت کاربردهای سخت‌افزاری با محدودیت‌های منابع. در اولین مرحله از این پروژه در سال ۲۰۰۵، ۳۴ الگوریتم با توجه به شرایط اعلام شده در مسابقه شرکت کردند (Babbage, et al, 2005). یکی از الگوریتم‌های معرفی شده در مرحله نهایی پروژه eSTREAM، الگوریتم رمز جریانی HC-128 می‌باشد که توسط وو ارائه گردید (Wu, 2008). قابل توجه است که وو، قبل از ارائه این الگوریتم، الگوریتم HC-256 (Wu, 2004) را در کنفرانس FSE در سال ۲۰۰۴ ارائه نمود و هم‌چنین شکل تغییر یافته الگوریتم HC-256، رمز جریانی 'HC-256' را ارائه کرد (Wu, 2004) که در این مقاله مورد تحلیل قرار می‌گیرد. رمزهای خانواده HC از نوع رمزهای با

¹ Synchronous

² Asynchronous

³ Internal state

⁴ word-oriented

⁵ Initial Value

جدول P و Q تشکیل شده که هر کدام دارای ۱۰۲۴ عنصر ۳۲ بیتی می‌باشند (Wu, 2004).

۳-۱- فرآیند پیش محاسبات: الگوریتم برپایی و اجرای کلید و مقداردهی اولیه

- آرایه $R[0, \dots, 2559]$ توسط توسیع K و IV به صورت ذیل به دست می‌آید:

$$R_i = \begin{cases} K_i & 0 \leq i \leq 7 \\ IV_{i-8} & 8 \leq i \leq 15 \\ f_2(R_{i-2}) + R_{i-7} + f_1(R_{i-15}) + R_{i-16} + i & 16 \leq i \leq 2559 \end{cases}$$

که توابع f_1 و f_2 به صورت زیر تعریف می‌گردند:

$$f_1(x) = (x \ggg 7) \oplus (x \ggg 18) \oplus (x \gg 3)$$

$$f_2(x) = (x \ggg 17) \oplus (x \ggg 19) \oplus (x \gg 10)$$

- جدول‌های P و Q با استفاده از آرایه R به صورت زیر به روز رسانی می‌گردند:

$$P[i] = R_{i+512} \quad \text{for } 0 \leq i \leq 1023$$

$$Q[i] = R_{i+1536} \quad \text{for } 0 \leq i \leq 1023$$

- الگوریتم، ۴۰۹۶ مرتبه اجرا می‌شود و مقادیر خروجی با عناصر جدول‌ها، به صورت زیر تعویض می‌گردند:

$$P[i] = P[i] + P[i \boxminus 10] + g_1(P[i \boxminus 3], P[i \boxminus 1023]) \oplus h_1(P[i \boxminus 12]) \quad \text{for } 0 \leq i \leq 1023$$

$$Q[i] = Q[i] + Q[i \boxminus 10] + g_2(Q[i \boxminus 3], Q[i \boxminus 1023]) \oplus h_2(P[i \boxminus 12]) \quad \text{for } 0 \leq i \leq 1023$$

در اینجا توابع g_1 و g_2 به شکل زیر تعریف می‌گردند:

$$g_1(x, y) = ((x \ggg 10) \oplus (y \ggg 23)) + Q[(x \oplus y) \bmod 1024]$$

$$g_2(x, y) = ((x \ggg 10) \oplus (y \ggg 23)) + P[(x \oplus y) \bmod 1024]$$

بعد از مراحل بالا، فرآیند پیش پردازش و مقداردهی اولیه به اتمام رسیده و الگوریتم رمز جهت تولید رشته کلید رمز آماده می‌باشد.

۳-۲- الگوریتم مولد رشته کلید

مولد رشته کلید شبه تصادفی، عناصر هر کدام از جدول‌ها را در هر مرحله به روز رسانی و یک رشته کلید خروجی ۳۲ بیتی (کلمه) تولید می‌کند.

$i = 0$
Repeat until (enough keystream bits are generated)
{

سال ۱۳۸۹ شماره ۲ پیاپی ۱۴

۲- نمادها و عملگرها

نمادها و عملگرهای مورد استفاده در این نوشتار به شرح ذیل می‌باشد.

$+$: یعنی $x + y \bmod 2^{32}$ که $0 \leq y < 2^{32}$ و $0 \leq x < 2^{32}$

\boxminus : یعنی $x - y \bmod 1024$

\oplus : یای انحصاری

||: الحاق^۱

\gg : انتقال به راست x به اندازه y بیت

\ll : انتقال به چپ x به اندازه y بیت

\ggg : یعنی $(x \ll (32 - n)) \oplus (x \gg n)$ که $0 \leq x < 2^{32}$ و $0 \leq n < 32$

\lll : یعنی $(x \ll n) \oplus (x \gg (32 - n))$ که $0 \leq x < 2^{32}$ و $0 \leq n < 32$

s_i : رشته کلید تولیدشده در مرحله i (یعنی $i + 1$ امین تکرار از مولد رشته کلید شبه تصادفی^۲)

عبارت‌های s_i^j , $h_1(x)$, $h_2(x)$ و $Q[x]$ به ترتیب بیان‌گر j امین بیت از عبارت‌های s_i , $h_1(x)$, $h_2(x)$, $Q[x]$ می‌باشند.

اگر x یک کلمه باشد، سپس $x^{(i)}$ عبارت است از i امین بایت از x که $x^{(0)}$ بایت پایین رتبه و $x^{(3)}$ بایت بالا رتبه خواهد بود.

P و Q به عنوان جعبه‌های جانشینی^۳ در الگوریتم HC-256 به کار می‌رود که هر کدام از جدول‌ها، ۱۰۲۴ عنصر ۳۲ بیتی دارند.

K بیان‌گر یک کلید به اندازه ۲۵۶ بیت می‌باشد.

IV بیان‌گر یک مقدار اولیه به اندازه ۲۵۶ بیت می‌باشد.

۳- تشریح الگوریتم HC-256

در این بخش الگوریتم HC-256 به طور خلاصه معرفی می‌گردد. این الگوریتم از یک کلید، K و یک مقدار اولیه، IV به اندازه ۲۵۶ بیت استفاده می‌نماید.

می‌توان $IV = IV_0 || \dots || IV_7$, $K = K_0 || \dots || K_7$ را تعریف نمود که هر کدام از K_i و IV_i ($i = 0, \dots, 7$) به اندازه ۳۲ بیت می‌باشند. حالت داخلی^۴ الگوریتم HC-256 از دو

¹ Concatenation

² PRGB: pseudo random bit generation

³ S-BOX

⁴ Internal State

و

$$s_{2i+1} \oplus h_2(Y_i) = (s_{2(i-2048)+1} \oplus h'_2(Y_{i-2048})) + (s_{2(i-10)+1} \oplus h_2(Y_{i-10})) + g_2(s_{2(i-3)+1} \oplus h_2(Z_{i-3}), s_{2(i-2047)+1} \oplus h'_2(Y_{i-2047})) \quad (2)$$

شایان ذکر است که توابع $h_2(x)$, $h'_1(x)$, $h_1(x)$ به جهت این که از جعبه‌های جانسنی متفاوتی هستند، با هم فرق دارند. در این جا Z_i و Y_i به ترتیب $P[i \boxminus 12]$ و $Q[i \boxminus 12]$ در i آمین مرحله می‌باشند. همان طوری که مشاهده می‌گردد، عملگرهای \oplus و \boxplus در بیت پایین‌رتبه^۲ مانند هم عمل می‌نمایند؛ بنابراین معادله‌های (۱) و (۲) را می‌توان به شکل زیر مجدد نوشت.

$$s_{2i}^0 \oplus s_{2(i-2048)}^0 \oplus s_{2(i-10)}^0 \oplus s_{2(i-3)}^{10} \oplus s_{2(i-2047)}^{23} = (h_1(Z_i))^0 \oplus (h'_1(Z_{i-2048}))^0 \oplus (h_1(Z_{i-10}))^0 \oplus (h_1(Z_{i-3}))^{10} \oplus (h'_1(Z_{i-2047}))^{23} \oplus (Q[r_i])^0 \quad (3)$$

و

$$s_{2i+1}^0 \oplus s_{2(i-2048)+1}^0 \oplus s_{2(i-10)+1}^0 \oplus s_{2(i-3)+1}^{10} \oplus s_{2(i-2047)+1}^{23} = (h_2(Y_i))^0 \oplus (h'_2(Y_{i-2048}))^0 \oplus (h_2(Y_{i-10}))^0 \oplus (h_2(Y_{i-3}))^{10} \oplus (h'_2(Y_{i-2047}))^{23} \oplus (P[s_i])^0 \quad (4)$$

که

$$r_i = s_{2(i-3)} \oplus h_1(Z_{i-3}) \oplus s_{2(i-2047)} \oplus h'_1(Z_{i-2047}) \\ s_i = s_{2(i-3)+1} \oplus h_2(Z_{i-3}) \oplus s_{2(i-2047)+1} \oplus h'_2(Y_{i-2047})$$

از طرفی هنگامی که $10 \leq i \leq 1024$ باشد الگوریتم مولد رشته کلید، به طور دائم جدول‌های P و Q را به روزرسانی می‌نماید؛ لذا می‌توان تابع بازخورد را به صورت زیر نمایش داد.

$$s_{2i}^0 \oplus s_{2(i-2048)}^0 \oplus s_{2(i-10)}^0 \oplus s_{2(i-3)}^{10} \oplus s_{2(i-2047)}^{23} \oplus s_{2i+1}^0 \oplus s_{2(i-2048)+1}^0 \oplus s_{2(i-10)+1}^0 \oplus s_{2(i-3)+1}^{10} \oplus s_{2(i-2047)+1}^{23} = (h_1(Z_i))^0 \oplus (h'_1(Z_{i-2048}))^0 \oplus (h_1(Z_{i-10}))^0 \oplus (h_1(Z_{i-3}))^{10} \oplus (h'_1(Z_{i-2047}))^{23} \oplus (Q[r_i])^0 \oplus (h_2(Y_i))^0 \oplus (h'_2(Y_{i-2048}))^0 \oplus (h_2(Y_{i-10}))^0 \oplus (h_2(Y_{i-3}))^{10} \oplus (h'_2(Y_{i-2047}))^{23} \oplus (P[s_i])^0 \quad (5)$$

² Least Significant Bit (LSB)

$$j = i \bmod 1024;$$

$$P[j] = P[j] + P[j \boxminus 10] + g_1(P[j \boxminus 3], P[j \boxminus 1023]) \\ ; \\ s_{2i} = h_1(P[j \boxminus 12]) \oplus P[j];$$

$$Q[j] = Q[j] + Q[j \boxminus 10] + g_2(Q[j \boxminus 3], Q[j \boxminus 1023]);$$

$$s_{2i+1} = h_2(Q[j \boxminus 12]) \oplus Q[j];$$

$i = i + 1$; each increment of i corresponds to 2 steps.

در روابط بالا h_1 و h_2 به صورت زیر بیان می‌گردند.

$$h_1(x) = Q[x^{(0)}] + Q[256 + x^{(1)}] + Q[512 + x^{(2)}] + Q[768 + x^{(3)}]$$

$$h_2(x) = P[x^{(0)}] + P[256 + x^{(1)}] +$$

$$P[512 + x^{(2)}] + P[768 + x^{(3)}]$$

۴- حمله تمایز پایه

در این بخش حمله تمایز پایه به الگوریتم رمز جریانی 'HC-256' مورد بررسی قرار می‌گیرد با این فرض که فرآیند پیش پردازش و مقداردهی اولیه کامل^۱ باشد. در واقع در این مرحله شیوه کار نزدیک به کار وو می‌باشد (Wu, 2004, 2008 and Hell, et al, 2009). در i آمین مرحله، جدول‌های P و Q به صورت زیر به روزرسانی می‌شوند:

$$P[i] = P[i] + P[i \boxminus 10] + g_1(P[i \boxminus 3], P[i \boxminus 1023]) \\ Q[i] = Q[i] + Q[i \boxminus 10] + g_2(Q[i \boxminus 3], Q[i \boxminus 1023])$$

و هم چنین

$$s_{2i} = h_1(P[i \boxminus 12]) \oplus P[i \bmod 1024] \\ s_{2i+1} = h_2(Q[i \boxminus 12]) \oplus Q[i \bmod 1024]$$

اگر $10 \leq i < 1024$ و با استفاده از این حقیقت $Q[i \bmod 1024] = P[i \bmod 1024] \oplus s_{2i} \oplus h_1(Z_i)$ و $s_{2i+1} \oplus h_2(Y_i)$ تابع بازخورد را می‌توان به صورت زیر نوشت:

$$s_{2i} \oplus h_1(Z_i) = (s_{2(i-2048)} \oplus h'_1(Z_{i-2048})) + (s_{2(i-10)} \oplus h_1(Z_{i-10})) + g_1(s_{2(i-3)} \oplus h_1(Z_{i-3}), s_{2(i-2047)} \oplus h'_1(Z_{i-2047})) \quad (1)$$

¹ Perfect

می توان معادله (۸) را به صورت زیر تقریب زد:

$$H(x_1) = H(x_2) \quad (1)$$

H یک جعبه جانشینی ۲۷۶ بیت به یک بیت می باشد.

x_1 و x_2 دو ورودی تصادفی ۲۷۶ بیتی می باشد.

$$x_1 = z_{i-3} \parallel z_{i-10} \parallel z_{i-2047} \parallel z_{i-2048} \parallel Y_{i-3} \parallel Y_{i-10} \parallel$$

$$Y_{i-2047} \parallel Y_{i-2048} \parallel r_i \parallel s_i$$

$$x_2 = z_{j-3} \parallel z_{j-10} \parallel z_{j-2047} \parallel z_{j-2048} \parallel Y_{j-3} \parallel$$

$$Y_{j-10} \parallel Y_{j-2047} \parallel Y_{j-2048} \parallel r_j \parallel s_j$$

برای به دست آوردن نرخ تصادم^۱ می توان از قضیه زیر

استفاده نمود:

قضیه: اگر s یک جعبه جانشینی m بیت به n بیت

باشد و تمام عناصر n بیتی به طور تصادفی تولید شده و

$m \geq n$ باشد. حال x_1 و x_2 دو ورودی تصادفی به s باشند

سپس $s(x_1) = s(x_2)$ با احتمال $2^{-m} + 2^{-n} - 2^{-m-n}$

می باشد (Wu, 2008).

اثبات. اگر $x_1 = x_2$ ، در این صورت $s(x_1) = s(x_2)$

می گردد. اگر $x_1 \neq x_2$ در این صورت $s(x_1) = s(x_2)$ با

احتمال 2^{-n} . چون $x_1 = x_2$ با احتمال 2^{-m} می باشد و

$x_1 \neq x_2$ با احتمال $1 - 2^{-m}$ صورت می پذیرد احتمال

$$\square. 2^{-m} + (1 - 2^{-m})2^{-n} \text{ با } s(x_1) = s(x_2) \text{ برابر}$$

با استفاده از این قضیه، احتمال معادله (۱۰) برابر

$$2^{-277} + \frac{1}{2} \text{ می باشد. بنابراین احتمال معادله (Y) هم با همین}$$

$$\text{احتمال یعنی } 2^{-277} + \frac{1}{2} \text{ می باشد.}$$

حال تمام اجزا، به منظور بنا کردن حمله تمایز به

HC-256 مهیا می باشد. برای انجام این کار فرض کنید N

تعداد تمام معادله های (Y) می باشد. هم چنین فرض کنید که

به ترتیب D و D' توزیع جمع انحصاری^۲ ۲۰ خروجی از

معادله (Y) برای الگوریتم رمز HC-256 و یک الگوریتم رمز

ایده آل باشد.

میانگین و انحراف استاندارد این توزیع با

$$\mu = Np \text{ و } \sigma = \sqrt{Np(1-p)} \text{ برای } D \text{ و } \mu' = Np' \text{ و}$$

$$\sigma' = \sqrt{Np'(1-p')} \text{ برای } D' \text{ به دست می آید.}$$

یادآوری می گردد که از نتایج بالا داریم

$$p = \frac{1}{2} + 2^{-277} \text{ و } p' = \frac{1}{2} \text{ و هنگامی که } N \text{ بزرگ باشد هر}$$

دو توزیع دو جمله ای^۳ را با توزیع نرمال می توان تقریب زد.

حال اگر $|\mu - \mu'| > 2(\sigma + \sigma')$ یعنی برای $N > 2^{556}$,

با در نظر گرفتن سمت چپ معادله (۵) می توان حمله

پایه را به صورت زیر اعمال نمود:

$$\text{برای } 2048 \times \alpha + 10 \leq i, j < 2048 \times \alpha + 1023$$

که α عضو مجموعه اعداد طبیعی می باشد و $i \neq j$

می توان معادله (۵) را به صورت زیر نوشت:

$$s_{2j}^0 \oplus s_{2(j-2048)}^0 \oplus s_{2(j-10)}^0 \oplus s_{2(j-3)}^{10} \oplus$$

$$s_{2(j-2047)}^{23} \oplus s_{2i+1}^0 \oplus s_{2(j-2048)+1}^0 \oplus s_{2(j-10)+1}^0 \oplus \quad (6)$$

$$s_{2(j-3)+1}^{10} \oplus s_{2(j-2047)+1}^{23}$$

$$= (h_1(z_j))^0 \oplus (h'_1(z_{j-2048}))^0 \oplus (h_1(z_{j-10}))^0 \oplus$$

$$(h_1(z_{j-3}))^{10} \oplus (h'_1(z_{j-2047}))^{23} \oplus (Q[r_j])^0 \oplus$$

$$(h_2(Y_j))^0 \oplus (h'_2(Y_{j-2048}))^0 \oplus (h_2(Y_{j-10}))^0 \oplus$$

$$(h_2(Y_{j-3}))^{10} \oplus (h'_2(Y_{j-2047}))^{23} \oplus (P[s_j])^0$$

به عبارتی اگر سمت چپ معادله های (۵) و (۶) برابر

باشد داریم:

$$s_{2i}^0 \oplus s_{2(i-2048)}^0 \oplus s_{2(i-10)}^0 \oplus s_{2(i-3)}^{10} \oplus$$

$$s_{2(i-2047)}^{23} \oplus s_{2i+1}^0 \oplus s_{2(i-2048)+1}^0 \oplus s_{2(i-10)+1}^0 \oplus$$

$$s_{2(i-3)+1}^{10} \oplus s_{2(i-2047)+1}^{23} = s_{2j}^0 \oplus s_{2(j-2048)}^0 \oplus \quad (7)$$

$$s_{2(j-10)}^0 \oplus s_{2(j-3)}^{10} \oplus s_{2(j-2047)}^{23} \oplus s_{2i+1}^0 \oplus$$

$$s_{2(j-2048)+1}^0 \oplus s_{2(j-10)+1}^0 \oplus s_{2(j-3)+1}^{10} \oplus$$

$$s_{2(j-2047)+1}^{23}$$

سپس طرف راست معادله های (۵) و (۶) نیز برابر خواهند بود:

$$(h_1(z_i))^0 \oplus (h'_1(z_{i-2048}))^0 \oplus (h_1(z_{i-10}))^0 \oplus$$

$$(h_1(z_{i-3}))^{10} \oplus (h'_1(z_{i-2047}))^{23} \oplus (Q[r_i])^0 \oplus$$

$$(h_2(Y_i))^0 \oplus (h'_2(Y_{i-2048}))^0 \oplus (h_2(Y_{i-10}))^0 \oplus$$

$$(h_2(Y_{i-3}))^{10} \oplus (h'_2(Y_{i-2047}))^{23} \oplus (P[s_i])^0$$

$$= (h_1(z_j))^0 \oplus (h'_1(z_{j-2048}))^0 \oplus (h_1(z_{j-10}))^0 \oplus \quad (8)$$

$$(h_1(z_{j-3}))^{10} \oplus (h'_1(z_{j-2047}))^{23} \oplus (Q[r_j])^0 \oplus$$

$$(h_2(Y_j))^0 \oplus (h'_2(Y_{j-2048}))^0 \oplus (h_2(Y_{j-10}))^0 \oplus$$

$$(h_2(Y_{j-3}))^{10} \oplus (h'_2(Y_{j-2047}))^{23} \oplus (P[s_j])^0.$$

یادآوری می گردد:

$$z_i = z_{i-2048} + z_{i-10} + g_1(z_{i-3}, z_{i-2047})$$

$$z_j = z_{j-2048} + z_{j-10} + g_1(z_{j-3}, z_{j-2047}) \quad (9)$$

$$Y_j = Y_{j-2048} + Y_{j-10} + g_2(Y_{j-3}, Y_{j-2047})$$

$$Y_i = Y_{i-2048} + Y_{i-10} + g_2(Y_{i-3}, Y_{i-2047})$$

¹ Collision Rate

² XOR

³ Binomial



می‌توانیم وضعیت‌های متفاوتی را به‌صورت زیر در نظر بگیریم:

۵-۲- وضعیت یک

فرض کنید E رویداد

$$Z_{j-2038} \parallel Z_{j+7} \parallel Z_{j-2037} = Z_{j-2048} \parallel Z_{j-3} \parallel Z_{j-2047}$$

$$Y_{j-2038} \parallel Y_{j+7} \parallel Y_{j-2037} = Y_{j-2048} \parallel Y_{j-3}$$

$$\parallel Y_{j-2047}$$

باشد. در این جا z و Y دو متغیر تصادفی با توزیع یکنواخت می‌باشند. حال وقتی رویداد E با احتمال

$$\Pr[E] = 2^{-96} \cdot 2^{-96} = 2^{-192}$$

به معادله (۱۳) کاهش پیدا می‌نماید.

$$\begin{aligned} & (h_1(z_{j+10}))^0 \oplus (Q[r_{j+10}])^0 \\ & \oplus (h_2(Y_{j+10}))^0 \oplus (P[s_{j+10}])^0 \\ & = (h_1(z_{j-10}))^0 \oplus (Q[r_j])^0 \oplus (h_2(Y_{j-10}))^0 \\ & \oplus (P[s_j])^0 \end{aligned} \quad (13)$$

یادآوری می‌گردد:

$$\begin{aligned} (h_1(z_{j+10}))^0 &= (Q[z_{(j+10)}^{(0)}])^0 \oplus (Q[256 + \\ & z_{(j+10)}^{(1)}])^0 \oplus (Q[512 + z_{(j+10)}^{(2)}])^0 \oplus (Q[768 + \\ & z_{(j+10)}^{(3)}])^0 \end{aligned}$$

$$\begin{aligned} (h_1(z_{j-10}))^0 &= (Q[z_{(j-10)}^{(0)}])^0 \oplus (Q[256 + \\ & z_{(j-10)}^{(1)}])^0 \oplus (Q[512 + z_{(j-10)}^{(2)}])^0 \oplus (Q[768 + \\ & z_{(j-10)}^{(3)}])^0 \end{aligned}$$

$$\begin{aligned} (h_2(Y_{j+10}))^0 &= (P[Y_{(j+10)}^{(0)}])^0 \oplus (P[256 + \\ & Y_{(j+10)}^{(1)}])^0 \oplus (P[512 + Y_{(j+10)}^{(2)}])^0 \oplus (P[768 + \\ & Y_{(j+10)}^{(3)}])^0 \end{aligned}$$

$$\begin{aligned} (h_2(Y_{j-10}))^0 &= (P[Y_{(j-10)}^{(0)}])^0 \oplus (P[256 + \\ & Y_{(j-10)}^{(1)}])^0 \oplus (P[512 + Y_{(j-10)}^{(2)}])^0 \oplus (P[768 + \\ & Y_{(j-10)}^{(3)}])^0 \end{aligned}$$

خروجی الگوریتم رمز را با احتمال ۰/۹۷۷۲ می‌توان از یک رشته تمام تصادفی تمایز داده شود.

۵- حملۀ تمایز بهبود یافته

در این بخش حملۀ تمایز بهبودیافته به الگوریتم رمز جریانی HC-256' ارائه خواهد شد. نشان خواهیم داد که معادله (۷) وقتی که $i = j + 10$ می‌تواند با احتمال بیشتری نگه داشته شود.

۵-۱- فرآیند بهبود حمله

در این بخش ارزیابی تحلیلی الگوریتم، شبیه به حملۀ پایه می‌باشد که در بخش قبل مورد بررسی قرار گرفت.

با شرط $2048 \times \alpha + 10 \leq i, j < 2048 \times \alpha + 10$

و $i = j + 10$ معادله‌های (۷) و (۸) را می‌توان به شکل زیر کاهش داد:

$$\begin{aligned} & s_{2(j+10)}^0 \oplus s_{2(j-2038)}^0 \oplus s_{2(j+7)}^{10} \oplus \\ & s_{2(j-2037)}^{23} \oplus s_{2(j+10)+1}^0 \oplus s_{2(j-2038)+1}^0 \oplus \\ & s_{2(j+7)+1}^{10} \oplus s_{2(j-2037)+1}^{23} = s_{2(j-2048)}^0 \oplus \\ & s_{2(j-10)}^0 \oplus s_{2(j-3)}^{10} \oplus s_{2(j-2047)}^{23} \oplus \\ & s_{2(j-2048)+1}^0 \oplus s_{2(j-10)+1}^0 \oplus s_{2(j-3)+1}^{10} \oplus \\ & s_{2(j-2047)+1}^{23} \end{aligned} \quad (11)$$

بنابراین

$$\begin{aligned} & (h_1(z_{j+10}))^0 \oplus (h'_1(z_{j-2038}))^0 \oplus \\ & (h_1(z_{j+7}))^{10} \oplus (h'_1(z_{j-2037}))^{23} \oplus \\ & (Q[r_{j+10}])^0 \oplus (h_2(Y_{j+10}))^0 \oplus \end{aligned} \quad (12)$$

$$\begin{aligned} & (h'_1(Y_{j-2038}))^0 \oplus (h_2(Y_{j+7}))^{10} \oplus \\ & (h'_2(Y_{j-2037}))^{23} \oplus (P[s_{j+10}])^0 \\ & = (h'_1(z_{j-2048}))^0 \oplus (h_1(z_{j-10}))^0 \oplus (h_1(z_{j-3}))^{10} \oplus \\ & (h'_1(z_{j-2047}))^{23} \oplus (Q[r_j])^0 \oplus (h'_2(Y_{j-2048}))^0 \oplus \\ & (h_2(Y_{j-10}))^0 \oplus (h_2(Y_{j-3}))^{10} \oplus (h'_2(Y_{j-2047}))^{23} \oplus \\ & (P[s_j])^0 \end{aligned}$$

فرض کنید هنگامی که معادله (۱۲) برقرار باشد، بیان می‌داریم که رویداد L اتفاق افتاده است. با فرض این‌که الگوریتم پیش‌پردازش و مقدردهی اولیه کامل باشد

وقتی F رخ دهد، معادله (۱۳) به معادله زیر کاهش پیدا می‌کند.

$$\begin{aligned} & (Q[768 + z_{j+10}^{(3)}])^0 \oplus (Q[r_{j+10}])^0 \oplus \\ & (P[768 + Y_{j+10}^{(3)}])^0 \oplus (P[s_{j+10}])^0 = \\ & (Q[768 + z_{j-10}^{(3)}])^0 \oplus (Q[r_j])^0 \oplus (P[768 + \\ & Y_{j-10}^{(3)}])^0 \oplus (P[s_j])^0 \end{aligned} \quad (۱۵)$$

حال اگر معادله (۱۶)

$$r_{j+10} \parallel r_j \parallel s_{j+10} \parallel s_j = 768 + z_{j+10}^{(3)} \parallel 768 + z_{j-10}^{(3)} \parallel 768 + Y_{j+10}^{(3)} \parallel 768 + Y_{j-10}^{(3)} \quad (۱۶)$$

یا معادله (۱۷)

$$r_{j+10} \parallel r_j \parallel s_{j+10} \parallel s_j = 768 + z_{j-10}^{(3)} \parallel 768 + z_{j+10}^{(3)} \parallel 768 + Y_{j-10}^{(3)} \parallel 768 + Y_{j+10}^{(3)} \quad (۱۷)$$

را داشته باشیم سپس معادله (۱۵) برقرار می‌باشد. از قبل اشاره کردیم که r_j و s_j دو متغیر ده‌بیتی می‌باشند؛ بنابراین احتمال عبارت $r_{j+10} \parallel r_j \parallel s_{j+10} \parallel s_j$ برابر است با 2^{-40} . از طرفی معادله‌های (۱۶) و (۱۷) به‌طور هم‌زمان رخ نمی‌دهند با فرض این‌که: $(z_{j-10}^{(3)})^7 \parallel (Y_{j-10}^{(3)})^7 \neq (z_{j+10}^{(3)})^7 \parallel (Y_{j+10}^{(3)})^7$ ، یعنی $z_{j-10}^{31} \parallel Y_{j-10}^{31} \neq z_{j+10}^{31} \parallel Y_{j+10}^{31}$ در نتیجه عبارت $z_{j-10}^{31} \parallel Y_{j-10}^{31} \neq z_{j+10}^{31} \parallel Y_{j+10}^{31}$ را خواهیم داشت.

• رویداد L تحت شرایط زیر که از آن به‌عنوان S_1 یاد می‌گردد، رخ می‌دهد.

۱- شرط زیر با احتمال 2^{-192} برقرار است:

$$z_{j-2038} \parallel z_{j+7} \parallel z_{j-2037} \parallel Y_{j-2038} \parallel Y_{j+7} \parallel Y_{j-2037} = z_{j-2048} \parallel z_{j-3} \parallel z_{j-2047} \parallel Y_{j-2048} \parallel Y_{j-3} \parallel Y_{j-2047}$$

۲- دو عبارت زیر هر دو با احتمال $2^{-46} = 2^{-23} \cdot 2^{-23}$ و با در نظر گرفتن شرط یک برقرار است (از قسمت ملاحظات).

$$z_{(j+10)}^{(2)} \parallel z_{(j+10)}^{(1)} \parallel z_{(j+10)}^{(0)} = z_{(j-10)}^{(2)} \parallel z_{(j-10)}^{(1)} \parallel z_{(j-10)}^{(0)}$$

$$Y_{(j+10)}^{(2)} \parallel Y_{(j+10)}^{(1)} \parallel Y_{(j+10)}^{(0)} = Y_{(j-10)}^{(2)} \parallel Y_{(j-10)}^{(1)} \parallel Y_{(j-10)}^{(0)}$$

۳- عبارت زیر با در نظر گرفتن شروط ۱ و ۲ دارای احتمال $2^{-16} - 1$ می‌باشد (از قسمت ملاحظات).

$$(z_{j+10}^{(3)})^7 \parallel (Y_{j+10}^{(3)})^7 \neq (z_{j-10}^{(3)})^7 \parallel (Y_{j-10}^{(3)})^7$$

$$z_{j+10}^{31} \parallel Y_{j+10}^{31} \neq z_{j-10}^{31} \parallel Y_{j-10}^{31}$$

هرکدام از اعداد صحیح ۳۲ بیتی z و Y را می‌توان به‌صورت چهار بیتی نمایش داد یعنی $z = z^{(3)} \parallel z^{(2)} \parallel z^{(1)} \parallel z^{(0)}$ و $Y = Y^{(3)} \parallel Y^{(2)} \parallel Y^{(1)} \parallel Y^{(0)}$ در این‌جا $z^{(0)}$ ، $Y^{(0)}$ و $z^{(3)}$ ، $Y^{(3)}$ به‌ترتیب بایتهای پایین رتبه و بالاتر رتبه z و Y می‌باشند. هم‌چنین رویداد F را می‌توان به‌صورت زیر تعریف نمود:

$$z_{(j+10)}^{(2)} \parallel z_{(j+10)}^{(1)} \parallel z_{(j+10)}^{(0)} = z_{(j-10)}^{(2)} \parallel z_{(j-10)}^{(1)} \parallel z_{(j-10)}^{(0)}$$

$$Y_{(j+10)}^{(2)} \parallel Y_{(j+10)}^{(1)} \parallel Y_{(j+10)}^{(0)} = Y_{(j-10)}^{(2)} \parallel Y_{(j-10)}^{(1)} \parallel Y_{(j-10)}^{(0)}$$

حال با داشتن معادله (۹) روابط زیر را خواهیم داشت:

$$Y_{j+10} = Y_{j-2038} + Y_j + g_2(Y_{j+7}, Y_{j-2037})$$

$$z_{j+10} = z_{j-2038} + z_j + g_1(z_{j+7}, z_{j-2037}) \quad (۱۴)$$

ملاحظات:

به‌فرض رویداد E رخ دهد، با توجه به معادله‌های (۹) و (۱۴)، شکل عبارات z_{j+10} ، z_{j-10} ، Y_{j+10} و Y_{j-10} به‌صورت زیر خواهد بود:

$$z_{j-10} = -A + B, z_{j+10} = A + B + C \pmod{2^{32}}$$

$$Y_{j+10} = D + E + F \pmod{2^{32}}, C \pmod{2^{32}}$$

و $Y_{j-10} = -D + E - F \pmod{2^{32}}$. بیت‌های پایین رتبه از عبارات z_{j+10} و Y_{j+10} به‌ترتیب با بیت‌های پایین رتبه از عبارات z_{j-10} و Y_{j-10} برابر می‌باشند (Sekar and Preneel, 2009). در نتیجه داریم: $\Pr[F|E] = 2^{-23} \cdot 2^{-23} = 2^{-46}$.

به‌علاوه بیت‌های بالا رتبه از عبارات z_{j+10} و Y_{j+10} به‌ترتیب با بیت‌های بالاتر رتبه از عبارات z_{j-10} و Y_{j-10} برابر می‌باشند، اگر $Y_{j-10} = Y_{j+10}$ که این مورد با احتمال $2^{-62} = 2^{-31} \cdot 2^{-31}$ رخ خواهد داد. به بیان دیگر:

$$\Pr[z_{j+10} = z_{j-10}, Y_{j+10} = Y_{j-10} | E] = 2^{-62}$$

بنابراین:

$$\Pr[z_{j+10} = z_{j-10} | E] = 2^{-31} = \Pr[(z_{j+10})^{31} = (z_{j-10})^{31}] ,$$

$$\Pr[Y_{j+10} = Y_{j-10} | E] = 2^{-31} = \Pr[(Y_{j+10})^{31} = (Y_{j-10})^{31}] .$$

۴- عبارت

$$r_{j+10} \parallel r_j = 768 + z_{j+10}^{(3)} \parallel 768 + z_{j-10}^{(3)} \quad \text{(با احتمال } 2^{-20} \text{) یا}$$

$$r_{j+10} \parallel r_j = 768 + z_{j-10}^{(3)} \parallel 768 + z_{j+10}^{(3)} \quad \text{(با احتمال } 2^{-20} \text{) تحت شرط سه احتمال آن}$$

$$2^{-20} + 2^{-20} = 2^{-19}$$

$$s_{j+10} \parallel s_j = 768 + y_{j-10}^{(3)} \parallel 768 + y_{j+10}^{(3)} \quad \text{هم‌چنین}$$

$$s_{j+10} \parallel s_j = 768 + y_{j+10}^{(3)} \parallel 768 + y_{j-10}^{(3)} \quad \text{(با احتمال } 2^{-20} \text{) یا}$$

$$Y_{j-10}^{(3)} \quad \text{(با احتمال } 2^{-20} \text{) تحت شرط ۳ احتمال آن}$$

$$2^{-20} + 2^{-20} = 2^{-19}$$

بنابراین احتمال کل $2^{-19} \cdot 2^{-19} = 2^{-38}$ خواهد بود.

در نتیجه داریم:

$$\Pr[S_1] = 2^{-192} \cdot 2^{-46} \cdot (1 - 2^{-16}) \cdot 2^{-38} \approx 2^{-276}$$

۵-۳- وضعیت دو

شرایط زیر را با عنوان S_2 تعریف می‌نماییم:

۱- شرط زیر با احتمال 2^{-192} برقرار است:

$$z_{j-2038} \parallel z_{j+7} \parallel z_{j-2037} \parallel y_{j-2038} \parallel y_{j+7} \parallel y_{j-2037} =$$

$$z_{j-2048} \parallel z_{j-3} \parallel z_{j-2047} \parallel y_{j-2048} \parallel y_{j-3} \parallel y_{j-2047}$$

۲- دو عبارت زیر ($z_{j+10} = z_{j-10}$ و $y_{j+10} = y_{j-10}$) با احتمال $2^{-62} = 2^{-31} \cdot 2^{-31}$ و با در نظر گرفتن شرط یک برقرار است (از قسمت ملاحظات).

$$z_{(j+10)}^{(3)} \parallel z_{(j+10)}^{(2)} \parallel z_{(j+10)}^{(1)} \parallel z_{(j+10)}^{(0)} = z_{(j-10)}^{(3)} \parallel$$

$$z_{(j-10)}^{(2)} \parallel z_{(j-10)}^{(1)} \parallel z_{(j-10)}^{(0)}$$

$$y_{(j+10)}^{(3)} \parallel y_{(j+10)}^{(2)} \parallel y_{(j+10)}^{(1)} \parallel y_{(j+10)}^{(0)} = y_{(j-10)}^{(3)} \parallel$$

$$y_{(j-10)}^{(2)} \parallel y_{(j-10)}^{(1)} \parallel y_{(j-10)}^{(0)}$$

۳- عبارت $r_{j+10} \parallel s_{j+10} = r_j \parallel s_j$ با احتمال 2^{-20} با شروط بالا برقرار است. در نتیجه:

$$\Pr[S_2] = 2^{-192} \cdot 2^{-62} \cdot 2^{-20} = 2^{-274}$$

از شرط سوم S_1 و شرط دوم S_2 این چنین استنباط می‌گردد که S_1 و S_2 دو به دو ناسازگارند^۱. بنابراین

$$\Pr[S_1 \cup S_2] = 2^{-276} + 2^{-274} \approx 2^{-273/7}$$

یادآوری می‌گردد بعضی از رویدادهای دیگری ممکن است منجر به وقوع L گردد؛ اما احتمال وقوع آن‌ها کم‌تر از S_1 و S_2 می‌باشند؛ بنابراین این رویدادها مورد بررسی قرار نگرفته‌اند. وقتی هیچ‌کدام از رویدادهای ذکر شده رخ ندهد، یعنی $(S_1 \cup S_2)^c$ ، معادله (۸) و به دنبال آن معادله (۷) با

احتمال یکنواخت و به مقدار $\frac{1}{2}$ با شرط این‌که الگوریتم پیش‌پردازش و مقداردهی اولیه کامل باشد، منعقد می‌باشد. در نتیجه با به‌کار بردن قانون بیز نتیجه زیر را خواهیم داشت: یادآوری می‌گردد:

$$\Pr[L] = \Pr[L|(S_1 \cup S_2)] \cdot \Pr[S_1 \cup S_2] + \Pr[L|(S_1 \cup S_2)^c] \cdot \Pr[(S_1 \cup S_2)^c] =$$

$$1 \cdot 2^{-273/7} + 0.5 \cdot (1 - 2^{-273/7}) = \frac{1}{2} + 2^{-274/7}$$

که اگر الگوریتم رمز 'HC-256' یک رمز ایده‌آل باشد، احتمال وقوع رشته‌کلیدهای خروجی رمز $\frac{1}{2}$ می‌باشد درحالی‌که در حمله تمایز پایه این مقدار $2^{-277} + \frac{1}{2}$ نشان داده شد. اما در این بخش اریبی با ضریب $2^{2.3}$ بهبود داده‌شد. حال با توجه به نتایج بالا می‌توانیم تمایزگر را بر روی الگوریتم 'HC-256' بنا نماییم. درواقع این فرآیند مانند بخش قبلی می‌باشد، به‌طوری‌که در این حالت $p = \frac{1}{2} + 2^{-274/7}$ و $p' = \frac{1}{2}$ می‌باشد (رج. آخرین پاراگراف بخش قبل). حال می‌توان رشته‌کلیدهای مورد نیاز حمله تمایز پایه با حمله تمایز بهبود داده‌شده به‌صورت زیر مورد مقایسه قرار گیرد. شایان ذکر است که معادله (۷) و (۱۱) به‌ترتیب دارای ۲۰ و ۱۶ رشته کلید خروجی می‌باشند. بنابراین در تمایزگر بهبود داده‌شده نیاز به $2^{555/4} = 2^{551/4} \cdot 16$ رشته‌کلید خروجی داریم؛ درحالی‌که در تمایزگر پایه نیاز به $2^{560/3} = 20 \cdot 2^{556}$ رشته‌کلید خروجی است. بنابراین حمله تمایز بهبودیافته به‌طور تقریبی $2^{4/9} = 30$ برابر کم‌تر، نیاز به رشته‌کلید خروجی دارد.

۶- نتیجه گیری

در این مقاله حمله تمایز پایه به الگوریتم رمزجریانی 'HC-256' ارائه گردید. در ادامه این حمله، احتمال اریبی و داده‌های مورد نیاز برای حمله تمایز بر روی الگوریتم مورد اشاره بهبود داده شد. در این ارزیابی تحلیلی، احتمال اریبی را 2^{-277} به‌دست آوردیم و هم‌چنین با این احتمال تعداد خروجی‌های مورد نیاز برای حمله، یعنی $2^{560/3}$ محاسبه گردید. در حمله بهبودیافته احتمال اریبی بر روی خروجی‌های این الگوریتم $2^{-274/7}$ به‌دست آمد و برای اجرای حمله نیاز به $2^{555/4}$ رشته کلید خروجی می‌باشد. بنابراین قادر به بهبود داده‌های مورد نیاز حمله تمایز به اندازه سی برابر بوده‌ایم.

¹ Mutually exclusive

۷- مراجع



احمدرضا ویزندان مدرک کارشناسی

خود را در رشته مهندسی مخابرات در سال ۱۳۷۹ از دانشگاه امام حسین علیه السلام و مدرک کارشناسی ارشد در رشته مهندسی مخابرات را در سال ۱۳۸۴ از دانشگاه آزاد اسلامی واحد تهران جنوب اخذ نموده است و در حال حاضر دانشجوی دکتری رشته رمز می باشد. زمینه مورد علاقه وی رمزنگاری، پنهان نگاری و تئوری کدینگ می باشد.

نشانی پست الکترونیک ایشان عبارت است از:

a_vizand@yahoo.com



جواد شیخزادگان مدرک کارشناسی

مهندسی مخابرات را در خردادماه سال ۱۳۶۳ از دانشکده مهندسی برق دانشگاه شریف اخذ کرد و بلافاصله در اولین دوره کارشناسی ارشد مخابرات در دانشگاه خواجه نصیرالدین طوسی پذیرفته شد و در تیرماه ۱۳۶۷ این دوره را به پایان رساند. ایشان پس از سپری کردن دوره طرح سربازی خود در مهرماه سال ۱۳۶۹ در اولین دوره دکتری مخابرات در دانشگاه تربیت مدرس پذیرفته شد و در سال ۱۳۷۴ از این رشته فارغ التحصیل شد. نامبرده علاوه بر تدریس در دانشگاه های مختلف تهران از اواسط سال ۱۳۶۶ تا حال حاضر، از اوایل سال ۱۳۷۰ فعالیت های تحقیقاتی خود را در زمینه پردازش سیگنال های صوتی شروع کرد و در سال ۱۳۷۳ موفق به تأسیس یک مؤسسه تحقیقاتی گردید که از سال ۱۳۷۷ با مجوز وزارت علوم، تحقیقات و فناوری به نام پژوهشکده پردازش هوشمند علائم فعالیت خود را ادامه می دهد. ایشان در حال حاضر عضو هیئت علمی، هیئت امنا و هیئت مدیره پژوهشکده مذکور، و نیز عضو هیئت مؤسس و شورای اجرایی انجمن رمز ایران از بدو تأسیس (سال ۱۳۷۹) تاکنون هستند. علاوه بر زمینه های تحقیقاتی اصلی وی که عبارتند از: بازشناسی گوینده، بازشناسی زبان و دادگان های گفتاری زبان فارسی، موضوعاتی از قبیل: رمزنگاری، پنهان نگاری و امنیت اطلاعات و ارتباطات نیز از زمینه های مورد علاقه ایشان می باشند.

آدرس پست الکترونیکی نامبرده عبارت است از:

sheikhzadegan@rcisp.ac.ir

ECRYPT. eSTREAM: ECRYPT Stream Cipher Project, IST-2002-507932.
<http://www.ecrypt.eu.org/stream/> (2008)

NESSIE. New European Schemes for Signatures, Integrity, and Encryption.
<http://www.cryptoneessie.org> (1999)

Wikipedia. A5/1-wikipedia, the free encyclopedia, 2008. <http://en.wikipedia.org/wiki/A5/1>

Wikipedia. RC4-wikipedia, the free encyclopedia, 2008. <http://en.wikipedia.org/wiki/RC4>

Babbage S., Christophe De Canni_ere, Anne Canteaut, Carlos Cid, Henri Gilbert, Thomas Johansson, Matthew Parker, Bart Preneel, Vincent Rijmen, Matthew Robshaw, 2005, The stream Portfolio <http://www.ecrypt.eu.org/stream>.

The eSTREAM Project, available at <http://www.ecrypt.eu.org/stream/>.

Wu, H., 2004. A New Stream Cipher HC-256, In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 226-244.

Sekar, G., Preneel, B., 2009. Improved Distinguishing Attacks on HC-256, International Workshop on Security.

Wu, H., 2008. The Stream Cipher HC-128, New Stream Cipher Designs (M. Robshaw and O Billet, eds. vol. 4986 of LNCS, pp.39-47.

Sarkar, P., 2004. On Approximating Addition by Exclusive OR, available at <http://eprint.iacr.org/2009>

Paul, S., Preneel, B., 2005. On the (In)security of Stream Ciphers Based on Arrays and Modular Addition, Cryptology ePrint Archive: Report 2005/448, Available online at <http://eprint.iacr.org>

Hell, M., Johansson, T., Brynielsson, L., 2009. An overview of distinguishing attacks on stream ciphers, cryptography and communications, vol.1, No.1, pp.71-94, Springer.

Rijmen, V., 2010. Stream Ciphers and the eSTREAM Project, Isecure, Vol.2, No.1,

Menezes, A ., Oorschot, P., Vanstone, S., 1965. Handbook of Applied Cryptography, CRC press.



عبدالرسول میرقدری مدرک کارشناسی،
کارشناسی ارشد و دکتری خود را در
رشته آمار به ترتیب در سال‌های ۱۳۶۵،
۱۳۶۸ و ۱۳۸۰ از دانشکده علوم دانشگاه
شیراز اخذ نموده‌اند و در حال حاضر

استادیار دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات
دانشگاه جامع امام حسین (ع) می‌باشد. زمینه مورد علاقه وی
رمزنگاری، آمار و فرآیندهای تصادفی می‌باشد.
نشانی پست الکترونیک ایشان عبارت است از:

Amrghdri@ ihu.ac.ir