به نام خدا

پژوهشکده علوم کامپیوتر

پیشنهاد همکاری به‌عنوان تک پروژه مقیم

عنوان پروژه:

تحلیل خودکار امنیت رمزهای متقارن سبک

Automated security analysis of lightweight symmetric ciphers

مجری:

نصور باقری

اسفند ماه ۱۴۰۱

عنوان طرح: تحلیل خودکار امنیت رمزهای متقارن سبک

مجری اصلی: دکتر نصور باقری

آدرس محل کار: تهران، لویزان، دانشگاه تربیت دبیر شهید رجایی، دانشکده مهندسی برق، گروه مخابرات

چکیده: بهره گیری از روش‌های خودکار سازی تحلیل مانند MILP، CP و SAT در سال‌های اخیر منجر به دستیابی به نتایج بهتری در قیاس با روش‌های کلاسیک برای تحلیل رمزهای متقارن شده‌است. اگر چه خودکار سازیهای فعلی در قیاس با روش‌های مرسوم، منجر به بهبود نتایج و کاهش زمان ارزیابی شده‌است، اما هنوز تا حد زیادی بر پایه دانش تحلیل گر برای مدل کردن سیستم است. هدف از انجام این پروژه تحقیقاتی، در کنار ارزیابی رمزهای متقارن به روش‌های متداول، توسعه ابزارهای خودکار به‌منظور تسهیل امر تحلیل و طراحی رمزهای متقارن است. در صورت انجام موفقیت‌آمیز این طرح، پیش بینی می‌شود در کنار انجام تحقیقات در سطح آخرین دستاوردهای بین‌المللی، بستر لازم برای توسعه ابزارهای مورد نیاز ویژه، که به هر دلیل امکان برون سپاری ارزیابی امنیت سامانه‌ای خود را ندارند، راه اندازی شود. به‌عنوان نمونه‌های عینی قابل ارزیابی، اولویت تحقیق در این طرح پژوهشی تمرکز بر بررسی امنیت رمزهای قالبی سبک و رمزهای احراز اصالت شده، با اولویت استاندارد رمزنگاری سبک جدیدNIST است، ASCON.

کلید واژه‌ها: رمزنگاری متقارن، تحلیل رمز، مسابقه رمزهای سبک NIST، تحلیل خودکار، ابزار، ASCON

Abstract: Using automated approaches for the security analysis of symmetric ciphers, e.g., MILP, SAT, and CP-based approaches, has received extensive attention recently and shown much better enhancement compared to classical cryptanalysis. Although the current automated security analysis has improved the previous results and reduced the analysis time, it still heavily depends on the analyst's experience to model the cipher. The main target of this research project, besides analyzing the symmetric ciphers using conventional approaches, is to develop automated security analysis tools to facilitate designing and analyzing symmetric ciphers. If we complete this project successfully, besides developing research in international standards, we expect to initiate the required foundation to develop the necessary tools for the specific organization that, for any reason, cannot outsource the security analysis of their products. To choose concrete primitives for analysis, the NIST's new standard for lightweight ciphers, ASCON, is given top priority.

Key words: symmetric cryptography, cryptanalysis, NIST competition for lightweight cryptography automated analysis, tools, ASCON.

۱. پیشگفتار:

سامانه‌های رمزنگاری را در حالت کلی می‌توان به دو دسته متقارن و نامتقارن تقسیم کرد. سامانه‌های نامتقارن عموماً از امنیت اثبات پذیر برخوردار هستند و امنیت آن‌ها وابسته به یک مسئله سخت ریاضی (عموماً از کلاس NP) است. اما این سامانه‌ها عموماً کند هستند و دارای کاربرد محدود. از سوی دیگر سامانه‌های متقارن، از سرعت بسیار بالاتری در قیاس با سامانه‌های نامتقارن برخوردارند و از کاربرد بیشتری برخوردار هستند. اما امنیت این گروه از سامانه‌ها، به‌دلیل ماهیت طراحی آن‌ها که ترکیبی است از توابع ساده، به‌صورت مطلق قابل اثبات نیست. در نتیجه گروه‌های تحقیقاتی مختلفی فعالیت خود را بر تحلیل یا طراحی این گروه از سامانه‌های رمز متمرکز کرده‌اند.

سامانه‌های متقارن را می‌توان دربرگیرنده رمزهای قالبی، توابع چکیده‌ساز، رمزهای جریانی و الگوریتم‌های رمز احراز اصالت شده دانست. رمزهای قالبی و جریانی عموماً با هدف تأمین محرمانگی به کار گرفته می‌شوند و توابع چکیده ساز بیشتر برای تأمین جامعیت پیام یا احراز اصالت آن استفاده می‌شوند. در کنار این‌ها، رمزنگاری احراز اصالت شده قرار دارد که به نوعی هر دو هدف را برآورده می‌سازد. نیازهای امنیتی هر کدام از این اولیه‌ها متفاوت است. به‌عنوان‌مثال توابع چکیده‌ساز یک ورودی با طول دلخواه را به‌عنوان ورودی دریافت کرده و یک مقدار با طول ثابت را در خروجی تحویل می‌دهند که به آن مقدار خروجی، چکیده پیام یا اثر انگشت پیام گفته‌می‌شود. پیش بینی می‌شود که برای یک تابع چکیده‌ساز خوب، پیدا کردن دو ورودی که به یک خروجی نگاشت می‌شوند، از نظر محاسباتی غیر عملی باشد. در نتیجه هر اولیه‌ای را باید با لحاظ کردن کاربرد مورد نظر و نیازمندی‌های آن مورد بررسی قرار داد. به‌دلیل وسعت اولیه‌های متقارن و سطح کاربردهای آن‌ها، تحقیقات زیادی در حوزه رمز به این گروه از اولیه‌ها اختصاص یافته‌است. در همین راستا و با توجه به اهمیت موضوع، در این طرح به بررسی امنیت رمزهای متقارن پرداخته می‌شود.

به‌عنوان‌مثال، در تحلیل‌های خطی [۱] و تفاضلی [۲]، به‌عنوان نمونه‌ای از تحلیل‌های متداول برای رمزهای قالبی، به‌دنبال یک مشخصه بین ورودی و خروجی با ویژگی‌های خاص می‌گردیم. در اکثر موارد این مشخصه‌ها به‌صورت دستی پیدا می شوند. اما به‌دلیل زیاد بودن تعداد همه مشخصه‌های ممکن، در اکثر موارد اطمینانی از بهینه بودن این مشخصه‌ها نیست. از طرفی، چگونگی به‌کارگیری توان محاسباتی سیستم‌های کامپیوتری برای دستیابی به نتایج تحلیلی بهتر در سامانه‌های رمز نگاری همواره مورد توجه بوده است. در سال‌های اخیر نیز تحقیقات زیادی بر روی به‌کارگیری روش‌های خودکار برای تحلیل متمرکز شده‌اند [۳-۱۰]. حال با توجه به در جریان بودن مسابقه سزار که یک مسابقه برای معرفی طرح‌های رمزنگاری احراز اصالت شده‌است، به‌کارگیری این قابلیت برای رسیدن به نتایج تحلیلی بهتر می‌تواند به‌عنوان یک مسئله مهم باشد که مد نظر این طرح پژوهشی است.

۲. پژوهش:

تا اوا سط دهه ۷۰ میلادی، دانش رمز نگاری بی شتر کاربرد نظامی دا شت و فعالیت ساختار یافته دان شگاهی در این حوزه انجام نمی‌شـد. به‌دنبال توسـعه ارتباطات دیجیتال و سـامانه‌های کامپیوتری در بازرگانی، احسـاس نیاز برای تأمین امنیت داده‌های مبادله شده افزایش پیدا کرد. از این روی، در اوا سط دهه ۷۰ الگوریتم رمز قالبی ا ستاندارد DES تو سط مؤ س سه US NSB که اکنون

[1] Data Encryption Standard

[2] National Bureau of Standard

NIST[1] نام دارد، استاندارد شد[۶]. نقش الگوریتم DES در توسعه دانش رمز غیر قابل‌انکار است و عملاً ارائه این استاندارد تجاری رمزنگاری باعث فعال شدن تیم‌های پژوهشی و گسترش رمزنگاری مدرن شد. الگوریتم DES عملاً استاندارد جهانی الگوریتم رمز تا اواسط دهه ۹۰ میلادی بود. اما بعد از آن، نظر به افزایش توان محاسباتی، طول کوتاه کلید این الگوریتم (۵۶ بیت) و هم‌چنین طول کوتاه قالب داده (۶۴ بیت) انتقادات زیادی را برانگیخت و مشکلات زیادی را متوجه آن ساخت. از این روی NIST تصمیم بر انتخاب الگوریتم رمز قالبی استاندارد دیگری گرفته و در قالب یک فراخوان همگانی، یک الگوریتم پیشنهادی به نام Rijndael را به‌عنوان الگوریتم رمز استاندارد پیشرفته (AES[2]) کرد[۷و۸].

به‌جز این الگوریتم استاندارد، رمزهای قالبی بسیاری در کاربری‌های گسترده مورد استفاده قرار می‌گیرند. از قبیل IDEA (که سابقاً در PGP استفاده می شده‌است)، RC5 (در S/MIME)، MYSTY1 و نسخه دیگر آن KASUMI (مورد استفاده در شبکه نسل سوم مخابرات سیار UMTS برای رمزنگاری و حفظ یک‌پارچگی داده).

در کنار الگوریتم‌های رمز قالبی ذکر شده در فوق، به‌دنبال فراگیر شدن کاربردهای دارای محدودیت مانند RFID، در سال‌های اخیر توجه زیادی به الگوریتم‌های رمز قالبی سبک وزن جذب شده‌است. الگوریتم‌های رمز قالبی سبک وزن زیر تنها نمونه‌هایی از این تلاش‌ها هستند (البته شاید مهم‌ترین آنها):

SKINNY, SIMECK, SIMON, SPECK, Prince, PrintCipher, LBlock, TWIS, EPCBC, LED, PRESENT, KATAN/KTANTAN, KLEIN, ICEBERG, HIGHT, TEA, XTEA, mCrypton, CLEFIA, MIBS

اهمیت رمزهای قالبی سبک وزن زمانی مشخص‌تر می شود که بدانیم الگوریتم رمز قالبی PRESENT [۹] در سال ۲۰۱۲ به عنوان استاندارد ISO و IEC انتخاب شده‌است[۱۰] و پیش بینی می شود به‌زودی شاهد استاندارد شدن رمزهای SIMON و SPECK توسط ISOباشیم (این دو رمز توسط NSA ارائه‌شده‌اند).

مجموعه پژوهش‌ها و مطالعاتی که طی ۳۰ سال روی DES انجام شد، و بعد از آن بر روی AES و سایر الگوریتم‌های رمز قالبی، منجر به دستاوردهای تئوری مهمی در زمینه طراحی الگوریتم‌های رمز قالبی شد. برجسته‌ترین آن‌ها کشف و توسعه روش های تحلیل خطی[3][۱] و تحلیل تفاضلی[4][۲] در اوایل دهه نود و پس از آن‌ها روش‌های بر پایه پیش‌محاسبات، از جمله مصالحه زمان-حافظه هلمن[۱۱] برای تحلیل DES و حتی در حالت کلی‌تر برای تحلیل الگوریتم‌های رمز با ساختارهای تکرارشونده می باشد. هم اکنون مقاومت در برابر حملات خطی و تفاضلی، معیار مهمی در ارزیابی امنیت الگوریتم‌های رمز قالبی است. برای ارزیابی امنیت الگوریتم‌های رمز قالبی در برابر این گروه از حملات روش‌های اثباتی توسط محققان ارائه شده‌است [۱۲و۱۳]. جایگزینی DES با AES، مجموعه تلاش‌ها برای تحلیل AES را افزایش داد و منجر به معرفی یا تو سعه روش‌های تحلیل مهمی چون حمله جبری[5][۱۴و۱۵]، حمله تفاضلات ناممکن[6][۱۶-۱۸] و حمله دوبخشی[7][۱۹] شده‌است. این روش‌ها برای تحلیل سایر الگوریتم‌های رمز نیز استفاده می‌شوند.

با توسعه دانش رمز، نیاز به تأمین جامعیت داده‌ها نیز مد نظر قرار گرفت. این امر منجر به گسترش توابع چکیده ساز شد. تابع چکیده‌ساز یک پیام با طول دلخواه را به‌عنوان ورودی دریافت می‌کند و یک نتیجه چکیده‌سازی شده با طول ثابت از آن تولید می‌نماید. طول خروجی در عمل مقداری بین ۱۲۸ بیت تا ۵۱۲ بیت را دارا است. توابع چکیده‌ساز کاربردهای متفاوتی دارند. کاربردهای متفاوت نیازهای امنیتی متفاوتی را به‌دنبال خود دارند. اما برخی از ویژگی‌های مورد انتظار از یک تابع چکیده ساز در بین

---

1 National Institute for Standard and Technology

2 Advanced Encryption Standard

3 Linear Cryptanalysis

4 Differential Cryptanalysis

5 Algebraic Attack

6 Impossible Differential Attack

7 Biclique Attack

تمامی کاربردها مشترک هستند. به‌عنوان نمونه، همواره پیش بینی می شود که یک تابع چکیده ساز، یک طرفه[1] باشد. یعنی، با داده شدن یک تصویر تصادفی مانند y پیدا کردن یک پیام مانند x به‌گونه‌ای که $H(x)=y$، سخت باشد (غیر عملی باشد). یک نیازمندی دیگر این است که مقدار خروجی، اثر انگشت پیام باشد. البته از آن‌جایی که فضای خروجی به‌مراتب کوچک‌تر از فضای ورودی است، همواره وجود خواهد داشت دو مقدار ورودی که به یک مقدار یکسان در خروجی نگاشت شوند. بنابراین، در یک تابع چکیده‌ساز، شرط لازم برای این‌که خروجی آن بتواند یک اثر منحصربه‌فرد از پیام را ارائه کند این است که پیدا کردن زوج‌های دارای برخورد[2] پیام‌هایی که به یک خروجی یکسان نگاشت شوند، با توجه به توان محاسباتی و طول چکیده عملی نباشد[۲۰].

بیشترین توابع چکیده‌ساز در ابتدای دهه ۹۰ توسعه و ارائه شدند. اما در این بین باید MD5 [۲۱] و SHA-1 [۲۲] را از همه پرکاربرد تر دانست. به‌علت سرعت و نیز اعتمادی که به امنیت این توابع چکیده ساز وجود داشت و به‌دلیل انتخاب شدن SHA-1 به‌عنوان الگوریتم‌های استاندارد چکیده‌سازی، این الگوریتم‌ها را باید الگوریتم‌هایی دانست که بیشترین استفاده را داشته‌اند.

با توجه به تحلیل‌هایی که بعداً برای این گروه از توابع فشرده‌ساز ارائه‌شده‌اند[۲۳-۲۶] توجه جامعه جهانی رمزنگاری به توابع چکیده ساز بیشتر معطوف شده است. مهم‌ترین تلاش را باید فراخوانی NIST برای طراحی الگوریتم استاندارد چکیده سازی جدید دانست که در پایان منجر به ارائه SHA-3 شد[۲۷]. فرایند انتخاب SHA-3 نیز خود منجر به توسعه معیارهای ارزیابی جدید مانند حملات چرخشی[۲۸] و حملات بازگشتی گشت[۲۹].

گروهی دیگر از توابع که بیشتر در احراز اصالت پیام کاربرد دارند کدهای احراز اصالت پیام هستند. یکی از مهم‌ترین روش‌ها برای تولید کدهای احراز اصالت به‌کارگیری توابع چکیده ساز به‌همراه کلید است که به‌اصطلاح به آن توابع چکیده ساز کلیددار نیز گفته‌می شود. مهم‌ترین خاصیتی که یک احراز اصالت باید فراهم کند، ویژگی جعل ناپذیر است. مهم‌ترین تابع احراز اصالت پیام را باید HMAC دانست[۳۰]. این گروه از توابع نیز به‌تازگی تحقیقات زیادی را متوجه خود کرده‌اند که به‌عنوان‌مثال می‌توان به مراجع [۳۱-۳۳] اشاره کرد.

از طرفی، دلایل زیادی وجود دارد که برای حفظ امنیت اطلاعات و ارتباطات نباید از رمزگذاری بدون احراز اصالت استفاده‌کرد. به‌عبارت دیگر محرمانگی و احراز اصالت می‌بایست همراه با هم برآورده شوند. طرح‌های رمزنگاری که بتوانند این کار را انجام دهند، طرح‌های رمزگذاری احراز اصالت شده[3] یا به‌اختصار طرح‌های AE نامیده می‌شوند. روش سنتی برای به‌دست آوردن یک طرح AE، ترکیب مستقیم روش‌های تولیدکننده محرمانگی و احراز اصالت پیام می‌باشد. به این معنی که ابتدا یک الگوریتم رمزنگاری، برای رمز کردن پیام به کار می‌رود، سپس از یک کد احراز اصالت پیام برای احراز اصالت آن استفاده می شود. اگر چه به‌دلیل جدا بودن الگوریتم‌ها در این روش، بررسی امنیت طرح AE مورد نظر به نسبت ساده می‌باشد (چون امنیت الگوریتم رمز و کد احراز اصالت پیام، به‌طور مستقل از هم بررسی می‌شوند)، اما مهم‌ترین مساله در این روش، نیاز دو الگوریتم رمزنگاری و احراز اصالت مجزا، با کلیدهای متفاوت و نیز انجام دو سری محاسبات (دو گذر) روی پیام می‌باشد. در برابر روش سنتی، دسته دیگری از طرح‌های AE وجود دارند که برای ایجاد هم‌زمان محرمانگی و احراز اصالت پیام از یک الگوریتم و یک کلید استفاده کرده و بنابراین یک سری محاسبات (یک گذر) روی پیام انجام می‌دهند.

اگر چه در زمینه مُدهای عمل AE مُدهایی به‌عنوان استاندارد پذیرفته‌شده‌اند، ولی درباره مُدهای AE اختصاصی کارهای صورت گرفته محدود بوده و یک AE اختصاصی استاندارد نیز وجود ندارد. با توجه به اهمیت طرح‌های AE و اینکه با داشتن یک طرح AE می‌توان کار یک الگوریتم رمزگذاری و یک الگوریتم احراز اصالت را به‌طور هم‌زمان انجام داد، در سال‌های اخیر تلاش‌های زیادی در جهت معرفی طرح‌های جدید AE، به‌کارگیری و استاندارد سازی آن‌ها انجام شده است. از مهم‌ترین این فعالیت‌ها می‌توان به برگزاری اولین کارگاه آموزشی در زمینه رمزگذاری احراز اصالت شده، تحت عنوان DIAC[4] اشاره کرد. این کارگاه در پنجم و

---

1 One Way

2 Collision

3 **A**uthenticated **E**ncryption

4 **D**irections in **A**uthenticated **C**ipher

ششم جولای ۲۰۱۲ در سوئد برگزار شد و در آن افراد صاحب‌نظر در حوزه رمزهای متقارن (به‌خصوص رمزهای قالبی و توابع چکیده ساز)، به ارائه طرح‌ها و نظرهای خود پرداختند. در این کارگاه زمزمه‌هایی درباره برگزاری یک مسابقه جهانی در زمینه AE مطرح شد تا اینکه در پانزدهم ژانویه سال ۲۰۱۳ فراخوان این مسابقه، با عنوان مسابقه CAESAR[1] صادر و تقویم زمانی آن مشخص شد [۳۴]. بعد از مسابقاتی مانند AES، eSTREAM و SHA-3 در حوزه رمزهای متقارن، هم اکنون مسابقه NIST-LWC، رویداد مهم دیگری در این حوزه است.

از طرفی، مدل برنامه‌ریزی خطی با اعداد صحیح[2] مدل برنامه‌ریزی ریاضی است که متغیرهای آن عدد صحیح هستند. مدلی که در آن تنها تعدادی از متغیرها اعداد صحیح باشند مدل برنامه ریزی خطی عدد صحیح آمیخته (MILP) نامیده می‌شود. شکل کلی یک مسئله MILP از نوع مینیمم با تابع هدف f[3] به‌صورت زیر می‌باشد:

$$\min f = \sum_i c_i x_i$$
$$S.t \quad Ax \leq b$$
$$x \geq 0$$
$$x \in \mathbb{Z}^k \times \mathbb{R}^{n-k} \subseteq \mathbb{R}^n,$$

که در آن $(c_1, \dots, c_n) \in \mathbb{R}^n$، $A \in \mathbb{R}^{m \times n}$ و $b \in \mathbb{R}^m$.

Mouha و همکارانش [۳۵]، از روش MILP برای پیدا کردن کمترین S-boxهای فعال در تحلیل تفاضلی[4] و خطی طرح‌های رمزنگاری که بر پایه بایت-گرا[5] بودند، استفاده کردند. بعد از آن نویسندگان مقاله‌های [۳۶و۳۷] با به‌کارگیری روش MILP، شیوه ای را برای به‌دست آوردن مقدارهای دقیق مشخصه‌های خطی در تحلیل تفاضلی و خطی با کمترین S-box های فعال ارائه نمودند.

برای اعمال روش MILP، متناظر با هر بیت از ورودی و خروجی عملگرهای استفاده شده در طرح، متغیر x_i طوری تعریف می شود که به‌ازای بیت‌های فعال مقدار یک و به‌ازای بیت‌های غیر فعال مقدار صفر را اختیار کند. همچنین برای هر S-box یک متغیر x_j تعریف می‌شود که این متغیر بر پایه اینکه خروجی S-box مربوطه فعال یا غیر فعال باشد به‌ترتیب مقدارهای یک یا صفر را اختیار می‌کند. سپس از آنجا که جمع x_j ها تعداد S-boxهای فعال را نشان‌می‌دهد تابع هدف را می‌توان به‌صورت مینیمم جمع x_j ها در نظر گرفت، یعنی $f = \sum_j x_j$. با به‌کارگیری ایده در [۳۸و۳۹] نتایج بهتری برای رمزهای قالبی بر پایه بیت ارائه شده است که در این طرح نیز مد نظر قرار خواهند گرفت. در طی سالهای اخیر، این روش خودکار سازی تحلیل و ارزیابی الگوریتم‌های رمز در کنار سایر روش‌ها توجه زیادی را به خود جلب کرده‌اند و منجر به نتایج بسیار خوبی شده‌اند. به‌عنوان نمونه‌ای از آخرین مقالات منتشر شده با به‌کارگیری خودکار سازی تحلیل رمز، خوانندگان به مراجع [۴۰-۴۹] ارجاع داده می‌شوند.

مجری طرح پیشنهادی نیز در سالیان اخیر تحقیقات قابل توجهی در این زمینه داشته است و به‌همراه محققین همکار توانسته است نتایج قابل توجهی به‌دست‌آورد. نتایج این تحقیقات در قالب طرح‌های پژوهشی و مقالات منتشر شده‌اند[۵۰-۵۳].

۳. دلایل انجام طرح:

در این پژوهش، امنیت توابع رمز متقارن مد نظر قرار می‌گیرد. نتایج این طرح به فهم ما از توابع متقارن و در پایان بایدهای طراحی یک طرح متقارن کمک می‌کند. در ادامه به چرایی انجام تحقیق پرداخته می‌شود.

---

[1] **C**ompetition for **A**uthenticated **E**ncryption: **S**ecurity, **A**pplicability and **R**obustness
[2] Integer Linear Programming
[3] Objective Function
[4] Differential Cryptanalysis
[5] Byte-oriented

با وجود همه تلاش‌های انجام شده در راستای تحلیل اگوریتم‌های رمز قالبی، نمی‌توان از امنیت الگوریتم‌های رمز قالبی کاملاً مطمئن بود و انجام تحقیقات برای توسعه یا ارائه راه کارهای تحلیل جدید همواره باید مد نظر قرار گیرد. در این راستا، بخشی از فعالیت‌های مورد نظر در این طرح پژوهشی تحلیل الگوریتم‌های رمز قالبی موجود یا توسعه تحلیل‌های کنونی با هدف ارائه حملات کارا خواهد بود.

در حوزه توابع چکیده‌ساز، اگر چه استاندارد SHA-3 مشخص شده‌است، اما پیش بینی می‌شود که به‌کارگیری توابع چکیده‌سازی مانند MD5، SHA-1 و SHA-2 هم‌چنان ادامه داشته‌باشد. در نتیجه بدیهی است که تلاش برای یافتن حملات کارا برای این توابع هم‌چنان ادامه داشته‌باشد. این حوزه هم‌چنان شاهد انتشار دستاوردهای جدید در کنفرانس های سطح اول رمزنگاری است. افزون بر این، نه SHA-3 و نه توابعی که قبل از آن به‌عنوان استاندارد شناخته می‌شدند، قابلیت استفاده در کاربردهایی که دارای محدودیت منابع هستند، مانند برچسب‌های RFID، را ندارند. از این روی در سال های اخیر توجه محققین به طراحی توابع چکیده‌ساز سبک جلب شده‌است. در این راستا تلاش‌های قابل توجهی انجام شده است که خروجی آن‌ها را می‌توان چکیده‌سازهای سبکی مانند Photon [۲] و Quark [۳] دانست. نکته مشترک در این توابع را باید این نکته دانست که برای پرهیز از نیاز به حافظه بیشتر از ساختار اسفنجی استفاده می‌شود که حجم حافظه کمتری در قیاس با ساختار چکیده‌ساز MD دارد. افزون بر این، سعی شده‌است در تابع دور از توابع سبک استفاده شود. برای نمونه در Photon از جعبه جانشینی ۴ به ۴ استفاده شده‌است که قابلیت پیاده‌سازی با تعداد کم گیت را دارا هستند، در قیاس با جعبه AES[۵].

از طرفی، NIST یک مسابقه برای استاندارد سازی الگوریتم‌های رمز سبک مناسب محیطهای دارای محدودیت منابع تدارک دید [۵۴و۵۵] که الگوریتم‌های زیر به‌عنوان الگوریتم‌های فینالیست معرفی شدند:

Ascon, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, SPARKLE, TinyJambu, Xoodyak

بعد بررسی‌های بسیار، در پایان در هفتم فوریه ۲۰۲۳ الگوریتم ASCON [۵۶] به‌عنوان برگزیده مسابقه معرفی شد و به زودی فرایند استاندارد سازی آن شروع خواهد شد[۵۷].

خودکار سازی تحلیل رمز می‌تواند زمان صرف شده توسط نیروی انسانی را به‌شدت کاهش دهد. از طرفی، فعالیت جامعی در این حوزه برای تحلیل کاندیداهای سزار انجام نشده است. در کنار این، دستاوردهای این پژوهش برای تربیت نیروی انسانی متخصص مورد نیاز کشور بسیار دارای اهمیت است.

۴. اهداف و محصولات طرح:

هدف اصلی از این طرح بهبود ترفندهای خودکار سازی تحلیل رمزهای متقارن است. نتایجی که به‌تازگی با به‌کارگیری این روش ها حاصل شده‌است، بسیار امیدوارکننده است و توجه ویژه به آن در کشور نیز از نظر نگارنده یک ضرورت است.

اهداف فرعی که در کنار این هدف اصلی حاصل خواهند شد بر این پایه‌اند:

- توسعه دانش تحلیل رمز و تربیت نیروی انسانی مورد نیاز کشور.
- بهبود نتایج موجود و پیدا کردن حملات بهبود یافته برای رمزهای متقارن شناخته شده با تمرکز بر روی طرح‌های راه یافته به مرحله نهایی مسابقه NIST-LWC، با تمرکز بر رمز ASCON به‌عنوان استاندارد نوین.
- ارائه الگوریتم‌های مناسب برای کاهش فضای جستجو در حین جستجو برای مشخصه‌های بهینه.

نتایج کمی مورد انتظار به‌صورت زیر است:

۱. ارائه حداقل یک مقاله در یکی از کنفرانس‌های حوزه (مانند: CRYPTO, EUROCRYPT, ACISP، SAC، INDOCRYPT، FSE, CHES, ASIACRYPT).

۲. یا ارائه حداقل دو مقاله در مجلات معتبر حوزه.

۵. برنامه و نحوه اجرای طرح:

در این پژوهش، ابتدا پیشینه طرح مورد مطالعه قرار می‌گیرد و تعداد الگوریتم به‌عنوان الگوریتم هدف برای اعمال حملات خودکار انتخاب می‌شوند. در قدم بعد سعی می‌شود الگوریتم‌های تحلیل خودکار مناسب توسعه داده شده و صحت کارکرد الگوریتم‌ها در مقیاس کوچک راستی آزمایی شود. در قدم بعدی الگوریتم‌های نهایی شده به الگوریتم‌های هدف اعمال می شود و نتایج حاصل با نتایج موجود مقایسه می‌شود. در پایان نتایج حاصل انتشار یافته و در قالب گزارش طرح مستند سازی می‌شوند.

۶. برنامه زمانی:

شماره مرحله / فعالیت	نام مرحله / فعالیت	مرحله / فعالیت پیش‌نیاز	درصد وزنی به‌کل پروژه	مدت زمان اجرا (ماه)	نمودار زمان‌بندی (ماه)											
					۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
۱	**بررسی پیشینه تحقیق**		٪۱۰	۲												
۲	**شبیه سازی نتایج موجود در مقیاس کوچک**	۱	٪۵	۲												
۳	انتخاب الگوریتم‌های هدف	۱و۲	٪۵	۲												
۴	توسعه نرم‌افزار و الگوریتم برای تحلیل خود کار کاندیداهای هدف	۲-۴	٪۱۵	۴												
۵	راستی آزمایی نتایج در اندک	۵	٪۵	۱												
۶	تکمیل الگوریتم‌ها و تولید نرم افزارهای مناسب برای کاندیدهای هدف	۶	٪۲۰	۲												
۷	اعمال حملات طراحی شده به کاندیداهای هدف	۷	٪۳۰	۶												
۸	مستند سازی و انتشار نتایج	۱-۸	٪۱۰	۲												

۳. همکاران طرح:

- **دکتر نصور باقری**: دکتری الکترونیک- رمزنگاری، دانشیار گروه مخابرات دانشکده مهندسی برق دانشگاه تربیت دبیر شهید رجایی (https://scholar.google.com/citations?user=32llx44AAAAJ&hl=en)
- دانشجوهای تحت هدایت

۴. ابزار مورد نیاز:

- کامپیوتر پرسرعت برای انجام شبیه سازی به‌همراه خط اینترنت با سرعت مناسب که تا اندازه‌ای فراهم است.

- امکان دسترسی به مستندات چاپ شده در زمینه رمزنگاری که در برگیرندهٔ آخرین دستاوردهای پژوهشگران این علم است. از جمله این مستندات می‌توان از مجله تخصصی Cryptology و مجموعه مقالات کنفرانس‌های Crypto، Eurocrypt، Asiacrypt، CHESE و FSE نام برد.

۵. بودجه‌بندی:

رده	شرح هزینه	مبلغ ماهیانه (ریال)	تعداد ماه	جمع (میلیون ریال)
۱	دستمزد	۲۰۰۰۰۰۰۰	۱۲	۲۴۰
۲	جمع کل (دویست و چهل)			۲۴۰

۶. مراجع:

1. *M. Matsui." Linear Cryptanalysis Method for DES Cipher", EUROCRYPT, Lecture Notes in Computer Science, 765, pages 386-397, Springer, (1994).*
2. *Biham, E., Shamir, A." Differential Cryptanalysis of the Full 16-Round DES". In: Brickell, E.F. (ed.) CRYPTO '92. LNCS, vol. 740, pp. 487-496. Springer (1992)*
3. *Sadegh Sadeghi, Nasour Bagheri, Mohamed Ahmed Abdelraheem: Cryptanalysis of reduced QTL block cipher. Microprocessors and Microsystems - Embedded Hardware Design 52: 34-48 (2017)*
4. *Ahmed Abdelkhalek, Yu Sasaki, Yosuke Todo, Mohamed Tolba, Amr M. Youssef: MILP Modeling for (Large) S-boxes to Optimize Probability of Differential Characteristics. IACR Trans. Symmetric Cryptol. 2017(4): 99-129 (2017)*
5. *Yu Sasaki, Yosuke Todo: New Algorithm for Modeling S-box in MILP Based Differential and Division Trail Search. SECITC 2017: 150-165*
6. *Yuki Funabiki, Yosuke Todo, Takanori Isobe, Masakatu Morii: Several MILP-Aided Attacks Against SNOW 2.0. CANS 2018: 394-413*
7. *Danping Shi, Siwei Sun, Patrick Derbez, Yosuke Todo, Bing Sun, Lei Hu: Programming the Demirci-Selçuk Meet-in-the-Middle Attack with Constraints. ASIACRYPT (2) 2018: 3-34*
8. *Siwei Sun, David Gerault, Pascal Lafourcade, Qianqian Yang, Yosuke Todo, Kexin Qiao, Lei Hu: Analysis of AES, SKINNY, and Others with Constraint Programming. IACR Trans. Symmetric Cryptol. 2017(1): 281-306 (2017)*
9. *Frédéric Lafitte: CryptoSAT: a tool for SAT-based cryptanalysis. IET Information Security 12(6): 463-474 (2018)*
10. *Frédéric Lafitte, Jorge Nakahara Jr., Dirk Van Heule: Applications of SAT Solvers in Cryptanalysis: Finding Weak Keys and Preimages. JSAT 9: 1-25 (2014)*
11. *J. Guo, T. Peyrin, and A. Poschmann: "The PHOTON Family of Lightweight Hash Functions", CRYPTO: 222-239(2011).*

12. *J. P. Aumasson, L. Henzen, W. Meier, M.N. Plasencia" Quark: A Lightweight Hash". J. Cryptology 26(2): 313-339 (2013).*

13. *J. Daemen, V. Rijmen: The Design of Rijndael " AES - The Advanced Encryption Standard." Information Security and Cryptography, Springer, ISBN 3-540-42580-2 FIPS 46-3(2002).*

14. *National Institute of Standards and Technology/U. S. Department of Commerce. Federal Information Processing Standards Publication, FIPS PUB 197: Advanced Encryption Standard. Federal Information Processing Standards Publication,(2001).*

15. *J. Daemen, V. Rijmen " Rijndael for AES." AES Candidate Conference: 343-348 (2000).*

16. *A. Bogdanov,, et al. "PRESENT: An Ultra-Lightweight Block Cipher." In Pascal Paillier and Ingrid Verbauwhede, editors, Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings, volume 4727 of Lecture Notes in Computer Science, pages 450{466. Springer,(2007).*

17. *ISO. "ISO/IEC 29192-2:2012"*

18. *M. E. Hellman. "A cryptanalytic time memory trade-off." IEEE Transactions on Information Theory, (26):401–406,(1980).*

19. *K. Nyberg and L.R. Knudsen. "Provable security against a differential attack." Journal of Cryptology, 8(1):27–37,(1995).*

20. *S. Vaudenay. Provable security for block ciphers by decorrelation. In Proceedings of STACS '98, number 1371 in Lecture Notes in Computer Science, pages 249–275. Springer-Verlag,(1998).*

21. *N. T. Courtois and J. Pieprzyk. "Cryptanalysis of block ciphers with overdefined systems of equations". In Advances in Cryptology - ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 267–287. Springer-Verlag,(2002).*

22. *S. Murphy and M. Robshaw. "Essential Algebraic Structure within the AES." In Advances in Cryptology - CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, pages 1–16. Springer-Verlag,(2002).*

23. *B. Bahrak and M. R. Aref. "A novel impossible differential cryptanalysis of AES." In Proceedings of the Western European Workshop on Research in Cryptology 2007 (WEWoRC'07), pages 152–156,(2007).*

24. *H. Mala,, et al." Improved Impossible Differential Cryptanalysis of 7-Round AES-128". In INDOCRYPT'10, volume 6498 of Lecture Notes in Computer Science, pages 282–291. Springer,(2010).*

25. *J. Lu, et al. "New impossible differential attacks on AES." In INDOCRYPT'08, volume 5365 of Lecture Notes in Computer Science, pages 279–293. Springer,(2008).*

26. *A. Bogdanov, D. Khovratovich, and C. Rechberger. "Biclique cryptanalysis of the full AES." In Dong Hoon Lee and XiaoyunWang, editors, ASIACRYPT 2011, volume 7073 of LNCS, pages 344-371. Springer-Verlag,(2011).*

۲۷. محمود سلماسی زاده و جواد مهاجری " (چالش‌های علم رمز) رویکردهای جدید در طراحی و تحلیل الگوریتم‌ها و پروتکل‌های رمزنگاری" معاونت علمی و فناوری ریاست‌جمهوری، ستاد توسعه فناوری اطلاعات و ارتباطات، اسفند ۱۳۹۱.

28. *R. L. Rivest. "The MD5 Message-Digest Algorithm." Internet Request for Comments (RFC) 1321,(1992).*

29. *National Institute of Standards and Technology/U. S. Department of Commerce. Federal Information Processing Standards Publication (FIPS PUB) 180-1. Secure Hash Standard, (1995).*

30. *X. Wang, H. Yu, Y. L. Yin: "Efficient Collision Search Attacks on SHA-0". CRYPTO 2005: 1-16, (2005).*

31. *X. Wang, Y. L. Yin, H. Yu: "Finding Collisions in the Full SHA-1". CRYPTO 2005: 17-36, (2005).*

32. *X. Wang, et al. "Cryptanalysis of the Hash Functions MD4 and RIPEMD". EUROCRYPT 2005: 1-18, (2005)*

33. *X. Wang, H. Yu: "How to Break MD5 and Other Hash Functions". EUROCRYPT 2005: 19-35 (2005).*

34. *National Institute of Standards and Technology/U. S. Department of Commerce. Federal Information Processing Standards Publication, FIPS PUB 202: SHA-3 Standard,(2013).*

35. *D. Khovratovich and I. Nikolic, "Rotational Cryptanalysis of ARX, " FSE,(2010).*

36. *F. Mendel, et al." The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl." FSE 2009: 260-276, (2009)*

37. *M. Bellare, R. Canetti, H. Krawczyk: " Keying Hash Functions for Message Authentication". CRYPTO 1996: 1-15 (1996).*

38. *Y. Dodis, J.P. Steinberger " Domain Extension for MACs Beyond the Birthday Barrier". EUROCRYPT 2011: 323-342 (2011).*

39. *P. Gazi, K. Pietrzak, M. Rybár "The Exact PRF-Security of NMAC and HMAC." CRYPTO (1): 113-130, (2014).*

40. *A. Abdelkhalek, et al. "MILP Modeling for (Large) S-boxes to Optimize Probability of Differential Characteristics". IACR Trans. Symmetric Cryptol. 2017(4): 99-129 (2017)*

41. *S. Sadeghi, N. Bagheri, M. A. Abdelraheem: Cryptanalysis of reduced QTL block cipher. Microprocessors and Microsystems - Embedded Hardware Design 52: 34-48 (2017)*

42. *Y. Sasaki, Yo. Todo: New Impossible Differential Search Tool from Design and Cryptanalysis Aspects - Revealing Structural Properties of Several Ciphers. EUROCRYPT (3) 2017: 185-215*

43. *S. Sadeghi, N. Bagheri: Improved Zero-Correlation and Impossible Differential Cryptanalysis of Reduced-round SIMECK Block Cipher. IET Information Security (2018)*

44. *Y. Sasaki, Y. Todo" New Algorithm for Modeling S-box in MILP Based Differential and Division Trail Search. SECITC 2017: 150-165*

45. *Z. Li,, et al." Improved Conditional Cube Attacks on Keccak Keyed Modes with MILP Method". ASIACRYPT (1) 2017: 99-127*

46. *R. Rohit, R. AlTawy, G. Gong "MILP-Based Cube Attack on the Reduced-Round WG-5 Lightweight Stream Cipher". IMACC 2017: 333-351*

47. *K. Fu, et al."MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck." FSE 2016: 268-288*

48. *S. Sun, et al. "Analysis of AES, SKINNY, and Others with Constraint Programming." IACR Trans. Symmetric Cryptol. 2017(1): 281-306 (2017)*

49. *K. Qiao, et al. "Improved MILP Modeling for Automatic Security Evaluation and Application to FOX." IEICE Transactions 98-A(1): 72-80 (2015)*

50. *Hosein Hadipour, Sadegh Sadeghi, Majid M. Niknam, Ling Song, Nasour Bagheri: Comprehensive security analysis of CRAFT. IACR Trans. Symmetric Cryptol. 2019(4): 290-317 (2019), FSE 2020*

51. *Sadegh Sadeghi, Tahereh Mohammadi, Nasour Bagheri: Cryptanalysis of Reduced round SKINNY Block Cipher. IACR Trans. Symmetric Cryptol. 2018(3): 124-162 (2018), FSE 2019*

52. *Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, Yu Sasaki: Cryptanalysis of Reduced NORX. FSE 2016: 554-574 (2015). FSE 2016*

53. *Sadegh Sadeghi, Vincent Rijmen, Nasour Bagheri: Proposing an MILP-based method for the experimental verification of difference-based trails: application to SPECK, SIMECK. Des. Codes Cryptogr. 89(9): 2113-2155 (2021)*

54. *NIST, Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. 2018. pp. 1–17. Available online: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwcsubmission-requirements-august2018.pdf (accessed on 21 Feb. 2023)*

55. *Lightweight Cryptography|CSRC. Available online: https://csrc.nist.gov/Projects/lightweight-cryptography/ (accessed on 21 Feb. 2023)*

56. *Dobraunig, C.; Eichlseder, M.; Mendel, F.; Schläffer, M. Ascon v1.2. Submission to NIST LWC Project. 2021. Available online: https://ascon.iaik.tugraz. (accessed on 21 Feb. 2023)*

57. *NIST, "NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices" CSRC. Available online: https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices#: ~: text=The%20winner%2C%20a%20group%20of, myriad%20tiny%20sensors%20and%20actuators. (accessed on 21 Feb. 2023).*