به نام خدا

پژوهشکده علوم کامپیوتر

پیشنهاد همکاری به‌عنوان تک پروژه مقیم

عنوان پروژه:

تحلیل رمز مبتنی بر یادگیری عمیق

Deep Learning-Based Cryptanalysis

مجری:

نصور باقری

اسفند ماه ۱۴۰۲

عنوان طرح: تحلیل رمزهای متقارن با استفاده از یادگیری عمیق

مجری اصلی: دکتر نصور باقری

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

چکیده: با گسترش روزافزون استفاده از یادگیری عمیق و شبکه‌های عصبی در علوم مختلف و موفقیت‌های حاصل از آن، در سال ۲۰۱۹ شبکه‌های عصبی عمیق برای تحلیل رمز تفاضلی اتخاذ شدند و پس از آن توجه فزاینده‌ای به این زمینه از تحقیقات جلب شد. اکثر تحقیقات انجام شده بر روی بهبود و به‌کارگیری تمایزگرهای عصبی متمرکز هستند و مطالعات محدودی نیز در رابطه با اصول ذاتی و ویژگی‌های یادگرفته شده توسط تمایزگرهای عصبی صورت گرفته است. در این مطالعه با تمرکز بر روی رمزهای قالبی مانند Speck، Simon و Simeck، به تجزیه و تحلیل فرایند و روش تحلیل رمزهای قالبی با کمک یادگیری عمیق خواهیم پرداخت. در این میان، عوامل مؤثر و مولفه‌های موجود در جهت دسترسی به عملکرد بهتر، واکاوی و استخراج خواهند شد. همچنین با تشریح و توسعه حملات و مقایسه نتایج، به دنبال پاسخ این سوال پاسخ خواهیم بود که چگونه از شبکه‌های عصبی و یادگیری عمیق می‌توان به عنوان یک ابزار کارا برای تحلیل رمزهای قالبی استفاده نمود.

کلید واژه‌ها: رمزنگاری متقارن، تحلیل رمز، یادگیری عمیق.

Abstract: With the increasing and widespread application of deep learning and neural networks across various scientific domains and the notable successes achieved, deep neural networks were employed for differential cryptanalysis in 2019. This marked the initiation of growing interest in this research domain. While most existing works primarily focus on enhancing and deploying neural distinguishers, limited studies have delved into the intrinsic principles and learned characteristics of these neural distinguishers. In this study, our focus will be on analyzing block ciphers such as Speck, Simon, and Simeck using deep learning. We will investigate the factors and components that contribute to better performance on security analysis of ciphers. Additionally, by extending the current studies and attacks and comparing the results, we aim to address the question of how the neural networks and deep learning can effectively serve as tools for block cipher.

Key words: Symmetric cryptography, Cryptanalysis, Deep learning.

۱. پیشگفتار:

رمزنگاری[1]شاخه‌ای از علم رمزشناسی[2]و یک علم و فناوری حیاتی در عصر ارتباطات مدرن است. رمزنگاری اطلاعات حساس و مهم را به شیوه‌ای تبدیل می‌کند که تنها افراد مجاز به آن دسترسی دارند و افراد غیرمجاز نمی‌توانند آن را تفسیر کنند. از اهداف اصلی رمزنگاری می‌توان به حفظ محرمانگی[3]حریم خصوصی و امنیت اطلاعات اشاره کرد. در این فرآیند، اطلاعات اصلی با استفاده از یک الگوریتم (الگوریتم رمزگذاری) و یک کلید (کلید رمزگذاری) تبدیل می‌شوند. تنها افرادی که دارای کلید رمزگشایی معتبر هستند، می‌توانند اطلاعات را به حالت اصلی بازگردانند. در رمزنگاری حرفه‌ای، نه تنها متن اصلی[4]محافظت می‌شود، بلکه کلید رمزگذاری و رمزگشایی نیز مورد محافظت قرار می‌گیرد. این اصول امنیتی باعث می‌شوند که اطلاعات مهم در مقابل دسترسی غیرمجاز و حملات امنیتی محافظت شوند.

رمزنگاری متقارن[5]رایج‌ترین روش برای تضمین محرمانه بودن یک پیام یا اطلاعات است. هنگامی که سیستم رمزنگاری از یک کلید یکسان برای رمزگذاری و رمزگشایی استفاده می‌کند، متقارن نامیده می‌شود. در بیشتر موارد، رمزگذاری داده‌ها با استفاده از الگوریتم‌های متقارن توصیه می‌شود. رمزنگاری متقارن به شرطی که طول کلید رمزگذاری به اندازه کافی بزرگ باشد، ایمن و سریع است. کلید رمزگذاری از طریق یک کانال امن یا روش‌های رمزنگاری نامتقارن[6]مبادله می‌شود.

رمزهای متقارن به طور کلی به دو زیر دسته تقسیم می‌شوند: رمزهای جریانی[7]و رمزهای قالبی[8].رمزهای قالبی متن اصلی را به دنباله‌هایی با اندازه ثابت از بیت‌ها به نام بلوک یا قالب تقسیم می‌کنند و به طور بالقوه مقداری لایه‌گذاری[9]را اعمال می‌کنند. سپس روی هر بلوک روش رمزگذاری را اجرا می‌کنند.

ارزیابی امنیت یک الگوریتم رمزنگاری یک مسئله بسیار مهم است. در رمزنگاری متقارن، این امر معمولاً با ارزیابی مقاومت و انعطاف‌پذیری در برابر انواع حملات شناخته شده انجام می‌شود [۱]. حملات تفاضلی[10][۲] و خطی[11][۳] از اولین و مهم‌ترین حملات برای تحلیل رمزهای متقارن هستند. امنیت هر الگوریتم رمز طراحی‌شده در مرحله اول در برابر این حملات مورد ارزیابی قرار می‌گیرد. از دیگر حملات شناخته‌شده می‌توان به حمله انتگرالی[12][۴]، حمله بومرنگ[13][۵] و حمله کلید مرتبط[14][۶] اشاره کرد.

یادگیری ماشین یک زیرشاخه از هوش مصنوعی[15]است که در آن، مدل‌ها و الگوریتم‌ها طراحی می‌شوند تا کامپیوترها بتوانند از داده‌ها یاد بگیرند و بدون نیاز به برنامه‌ریزی صریح، وظایف و مسائل خاص را انجام دهند. هدف اصلی یادگیری ماشین، استخراج الگوها و اطلاعات مفهومی از داده‌ها است به‌گونه‌ای که مدل‌ها قادر به تعمیم آن‌ها به داده‌های جدید

---

1 Cryptography
2 Cryptology
3 Confidentiality
4 Plaintext
5 Symmetric cryptography
6 Asymmetric cryptography
7 Stream cipher
8 Block cipher
9 Padding
1 Differential attack
1 Linear attack
1 Integral attack
1 Boomerang attack
1 Related-key attack
1 Artificial intelligence

باشند و پیش‌بینی‌ها و تصمیم‌گیری‌های دقیقی انجام دهند. برای دستیابی به این هدف، مراحلی شامل جمع‌آوری داده‌ها، پیش‌پردازش داده‌ها، انتخاب مدل، آموزش مدل، ارزیابی مدل و استفاده از مدل صورت می‌گیرد. یادگیری عمیق یک شاخه از یادگیری ماشین است که از شبکه‌های عصبی عمیق[1]استفاده می‌کند و در زمینه‌های مختلفی مانند طبقه‌بندی تصویر و ترجمه ماشینی[2]به کار گرفته شده است. هدف این است که داده‌ها را بر اساس برچسب‌هایشان که در چندین کلاس قرار دارند، طبقه‌بندی کنیم.

یادگیری ماشین و به‌خصوص یادگیری عمیق به‌تازگی به دلیل پیشرفت‌های چشمگیر در حوزه‌های مهمی مانند بینایی ماشین[3]، تشخیص گفتار[4]و غیره، توجه زیادی را به خود جلب کرده است. تحلیل رمز[5]و یادگیری ماشین، روش‌ها و ویژگی‌های مشترک بسیاری دارند. در برخی جنبه‌ها، پیداکردن کلید یک الگوریتم رمزنگاری معادل پیداکردن مجموعه مناسبی از وزن‌های شبکه‌های عصبی در یک الگوریتم یادگیری عمیق است. اما با وجود این شباهت‌ها و پیشرفت‌های اخیر در ابزارها و مدل‌های یادگیری عمیق، پژوهشگران در کاربرد تکنیک‌های یادگیری ماشین در تحلیل رمز پیشرفت چندانی نداشته‌اند.

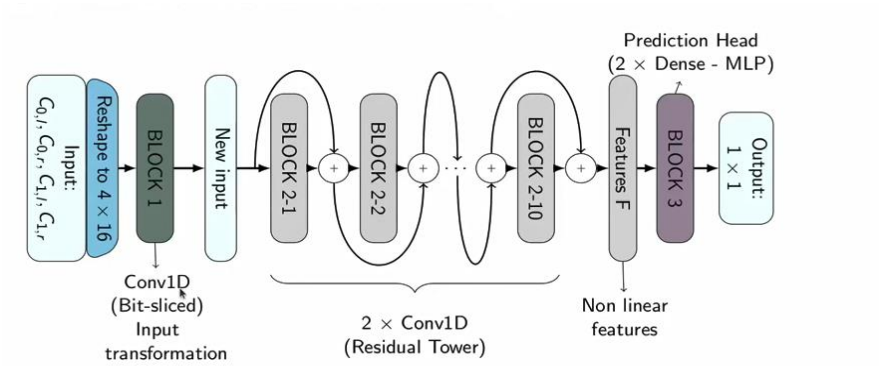
در سال ۲۰۱۹، یک نوع حمله جدید با کمک یادگیری ماشین به رمز قالبی SPECK پیشنهاد شد. با داشتن مبانی آن در تحلیل رمز تفاضلی[6]، ایده این است که جفت‌های متن رمزی[7]را که به یک تفاضل متن اصلی ثابت تعلق دارند از جفت‌های تصادفی متمایز کنیم. برای این کار، از شبکه های عصبی استفاده می‌شود که منجر به حمله بازیابی کلید ۱۱ دوری در SPECK32/64 می‌شود و حداقل با شبکه‌های کلاسیک قابل رقابت است [۷].

در حالی که واضح است که یادگیری ماشین به طور کامل جایگزین تحلیل رمز کلاسیک نخواهد شد، به ویژه از آنجایی که به تفاوت کاملاً واضحی در توزیع مسئله یادگیری نیاز دارد، این سوال مطرح می‌شود که چقدر این رویکرد عمومی است و تا چه حد می‌تواند کار یک تحلیل‌گر رمز را تکمیل کند. به عبارت دیگر، آیا می‌توانیم یادگیری ماشین را به‌عنوان ابزاری که به تحلیل رمز کمک می‌کند، شبیه به روشی که حل‌کننده‌های SAT[8] [۸] و MILP[9] [۹] تاکنون دیده‌اند، ببینیم؟

استفاده از یادگیری ماشین در تحلیل رمز متقارن می‌تواند به بهبود دقت، کاهش زمان و دادهٔ موردنیاز برای تحلیل رمز متقارن کمک کند. همچنین، با کشف الگوهای پیچیده توسط مدل یادگیری ماشین و افزایش قابلیت پیش‌بینی، می‌توان به بهبود روش‌های موجود در تحلیل رمز متقارن و توسعه آن دست‌یافت. در شکل ۱ معماری پایه استفاده شده برای تحلیل الگوریتم رمز SPECK32/64 توسط مقاله [۷] را مشاهده می‌نماییم. در این معماری از لایه‌های باقی‌مانده[10]کانولوشنی استفاده شده است. داده‌های ورودی به مدل، متن‌های رمزی حاصل از یک تفاضل ورودی معین برای کلاس توزیع حقیقی و حاصل از تفاضل ورودی تصادفی برای کلاس توزیع تصادفی هستند. هدف مدل ایجاد تمایزگر بین این دو توزیع، تبدیل مسئله تمایز به طبقه‌بندی و سپس استفاده از تمایزگر برای حمله بازیابی کلید است. ترکیب روش‌های تحلیل کلاسیک با

1 Deep neural network
2 Machine translation
3 Computer vision
4 Speech recognition
5 Cryptanalysis
6 Differential cryptanalysis
7 Ciphertext
8 Satisfiability
9 Mixed-Integer linear programming
1 Residual 0

«سرعت ماشین» برای ارزیابی کارآمد و هوشمندانه امنیت اجزای الگوریتم رمزنگاری، یکی از نکات و روندهای حیاتی تحقیقات کنونی است. توسعه هوش مصنوعی فرصت های جدیدی را برای تحلیل رمز فراهم می کند [۱۰].



شکل ۱. معماری شبکه عصبی استفاده شده در مقاله [۷] برای تحلیل الگوریتم‌های رمز قالبی

۲. پیشینه پژوهش:

در کنفرانس مطرح کریپتو ۲۰۱۹، آرون گور به طور خلاقانه‌ای یادگیری عمیق را با تحلیل رمز تفاضلی ترکیب می‌کند و آن را برای الگوریتم رمز قالبی Speck32/64 اعمال می کند، به این ترتیب تمایزگر عصبی (ND) می‌تواند از متمایز کننده مبتنی بر جدول توزیع تفاضل[1](DD) پیشی بگیرد. سپس، یک تمایزگر ترکیبی[2](HD) متشکل از یک ND و یک تفاضل کلاسیک[3](CD) با استراتژی‌های جستجوی کلید انتخابی منجر به حملات بازیابی کلید ۱۱ و ۱۲ دوری برای الگوریتم مذکور می‌شود [۷]. در کنفرانس یوروکریپت ۲۰۲۱، Benamira و همکاران، تحلیل کاملی از شبکه عصبی گور ارائه کردند. آنها کشف کردند که این تمایزگرها تصمیمات خود را بر اساس تفاضل جفت متن رمزی و تفاضل حالت داخلی در دورهای ماقبل آخر قرار می‌دهند [۱۱].

برای حمله به دورهای بیشتر، جزء CD یا ND باید گسترش یابد. در کنفرانس آسیاکریپت ۲۰۲۲، بائو و همکاران، اولین حملات ۱۳ دوری عملی و بهبود یافته ۱۲ دوری حملات بازیابی کلید مبتنی بر ND را برای الگوریتم Speck32/64 با تقویت CD ابداع کردند و به طور عمیق بیت‌های خنثی[4]تعمیم یافته‌تری از تفاضل‌ها را بررسی کردند. علاوه بر این، آن‌ها ND تا ۱۱ دور از الگوریتم رمز Simon32/64 را با استفاده از مدل‌های DenseNet و SENet به دست آوردند، بنابراین حمله عملی بازیابی کلید ۱۶ دور را ارائه دادند [۱۲]. ژانگ و همکاران بر بهبود دقت ND متمرکز شدند و ماژول تلقین[5]متشکل از لایه‌های کانولوشنی موازی چندگانه را قبل از شبکه باقی‌مانده اضافه کردند تا اطلاعات در ابعاد چندگانه را ضبط کند. تحت تأثیر بهبودهای ترکیب چندگانه، آن‌ها پیچیدگی زمانی حملات بازیابی کلید را برای ۱۲ و ۱۳ دور از الگوریتم Speck32/64 و ۱۶ دور از الگوریتم Simon32/64 کاهش دادند. آن‌ها همچنین اولین بازیابی کلید ۱۷ دور عملی را برای الگوریتم Simon32/64 ارائه کردند [۱۳].

در سال ۲۰۲۲، لیو و همکاران چارچوب گور را بهبود بخشیدند و آن را در الگوریتم Simeck32/64 اعمال کردند. آنها NDهای ۸ تا ۱۰ دور را برای الگوریتم Simeck32/64 به دست آوردند و حملات را برای ۱۳ تا ۱۵ دور از الگوریتم Simeck32/64 با پیچیدگی داده و زمانی کم با موفقیت انجام دادند [۱۴]. در همان سال، لو و همکاران جفت‌های متن

[1] Difference distribution table
[2] Hybrid distinguisher
[3] Classical differential
[4] Neutral bits
[5] Inception

رمزی چندگانه (۸ جفت متن رمزی) را برای آموزش شبکه عصبی SE-ResNet که با فرمت داده‌ای جدید برای الگوریتم‌های Simon و Simeck تغذیه می‌شد، به کار گرفتند. در نهایت، آنها ۹ تا ۱۲ دور ND برای الگوریتم Simeck32/64 به دست آوردند [۱۵].

در جدول ۱ نیز خلاصه و مقایسه‌ای از کارهای پیشین آورده شده است.

جدول ۱. مقایسه کارهای پیشین

خلاصه	مقاله
اثربخشی شبکه‌های عصبی در تحلیل تفاضلی.	گور [۷]
اثر تمایز مدل پرسپترون چندلایه[1](MLP).	جین و همکاران [۱۶]
مقایسه تمایزگر شبکه عصبی و تمایزگر کلاسیک.	بلینی و همکاران [۱۷]
تأثیر تمایز مدل‌های مختلف یادگیری عمیق بر SIMON32/64.	تیان و همکاران [۱۸]
اثر تمایز مدل‌های FNN[2] و CNN[3].	وانگ و همکاران [۱۹]
اثربخشی تمایزگرهای یادگیری عمیق در رمزهای غیر مارکوف.	بکسی و همکاران [۲۰]
دقت تمایزگر برای الگوهای مختلف تفاضل ورودی.	هو و همکاران [۲۱]
یک چارچوب تمایزگر توسعه‌یافته با استفاده از یادگیری ماشین.	یاداو و همکاران [۲۲]
دقت تمایزگر برای الگوهای جفت متن رمزی چندگانه و متعدد.	چن و همکاران [۲۳]
تحلیل دقیق و توضیح کامل کار گور.	بنامیرا و همکاران [۱۱]
روش استخراج برای ویژگی‌های دقیق‌تر در تمایزگر عصبی.	گو و همکاران [۲۴]
سازی خودکار تمایزگرهای تفاضلی عصبی.بهینه	گور و همکاران [۱]

۳. دلایل انجام طرح:

اگرچه این یک سؤال طولانی‌مدت بوده است که آیا ماشین‌ها می‌توانند انجام وظایف تحلیل رمز را بیاموزند، پاسخ‌های مثبتی که توسط تحلیل رمزنگاری مبتنی بر یادگیری ماشین به دست می‌آید هنوز نادر است. این ایده برای اولین‌بار در سال ۲۰۱۹ با کار قابل‌توجهی که توسط آرون گور انجام شد پاسخ مثبتی گرفت [۷]. تحقیقات حول این ایده صورت خواهد گرفت. با توجه به بررسی‌های انجام شده، مستندی از تحقیقات در این زمینه و حملات تمایزگر با استفاده از یادگیری عمیق در داخل کشور موجود نیست.

با توجه به رشد روزافزون تهدیدات و پیچیدگی رمزنگاری، اجرای تحلیل رمزهای متقارن با استفاده از یادگیری ماشین با توجه به توانایی آن در تشخیص روابط و ویژگی‌های پیچیده که توسط تحلیل کلاسیک قابل‌تشخیص نیستند، می‌تواند

[1] Multilayer perceptron
[2] Fully connected neural network
[3] Convolutional neural network

ضعف الگوریتم‌های رمزنگاری متقارن را به‌صورت بهینه‌تر شناسایی کند و در نتیجه به وسیله ترکیب آن با تحلیل رمز کلاسیک، بهبودهایی در امنیت سیستم‌ها و شبکه‌ها با انتخاب مناسب الگوریتم ایجاد کند.

.

۴. اهداف و محصولات طرح:

هدف ا صلی از این طرح بهبود ترفندهای تحلیل رمزهای متقارن مبتنی بر یادگیری عمیق ا ست ا ست. نتایجی که به‌تازگی با به کارگیری این روش‌ها 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:

- کسب دانش، توسعه و ارتقای دانش موجود پیرامون موضوع تحلیل رمز به کمک یادگیری عمیق.
- به‌کارگیری مدل‌های یادگیری عمیق در کنار تحلیل رمز کلاسیک و کمک به آن.
- ارائه تمایزگر عصبی[1] برای رمزهای متقارن و روش بازیابی جزئی زیرکلید دور بر مبنای تمایزگرها.
- ترکیب، بهبود و توسعه روش‌های موجود در تحلیل رمزهای متقارن با استفاده از یادگیری عمیق و ارائه روش عمومی.
- امکان تحلیل رمزهای تحلیل نشده با این روش و نیز تحلیل رمزهای بومی.
- امکان تحلیل اجزا تشکیل‌دهنده الگوریتم‌های رمزنگاری مانند جعبه‌های جانشانی.

نتایج کمی مورد انتظار به‌صورت زیر است:

۱. ارائه حداقل یک مقاله در یکی از کنفرانس‌های حوزه (مانند: CRYPTO, EUROCRYPT, ACISP، SAC، INDOCRYPT، ASIACRYPT, FSE, CHES).
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 مبتنی بر یادگیری عمیق انتخاب می‌شوند. در قدم بعد سعی می‌شود شبکه های عصبی مناسب توسعه داده شده و صحت کارکرد ایده حمله که از دنیای تحلیل رمز کلاسیک نشات می گیرد در مقیاس کوچک راستی آزمایی شود. در قدم بعدی شبکه نهایی شده به الگوریتم‌های هدف اعمال می‌شود و نتایج حاصل با نتایج موجود مقایسه می‌شود. در پایان نتایج حاصل انتشار یافته و در قالب گزارش طرح مستند سازی می‌شوند.

[1] Neural distinguisher

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 شبکه عصبی برای اعمال به کاندیداهای هدف	۲-۴	٪۱۵	۴												
۵	راستی آزمایی نتایج	۵	٪۵	۱												
۶	تکمیل شبکه و توسعه آن برای حمله به 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، استاد تمام 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	۴۰۰۰۰۰۰۰	۱۲	۴۸۰
۲	جمع کل			۴۸۰

۶. مراجع:

[1] Gohr, A., G. Leander, and P. Neumann, *An assessment of differential-neural distinguishers.* Cryptology ePrint Archive, 2022.

[2] Biham, E. and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems.* Journal of CRYPTOLOGY, 1991. **4**: p. 3-72.

[3] Matsui, M. *Linear cryptanalysis method for DES cipher*. in *Workshop on the Theory and Application of of Cryptographic Techniques*. 1993. Springer.

[4] Knudsen, L. and D. Wagner. *Integral cryptanalysis*. in *Fast Software Encryption: 9th International Workshop, FSE 2002 Leuven, Belgium, February 4–6, 2002 Revised Papers 9*. 2002. Springer.

[5] Wagner, D. *The boomerang attack*. in *International Workshop on Fast Software Encryption*. 1999. Springer.

[6] Biham, E., *New types of cryptanalytic attacks using related keys.* Journal of Cryptology, 1994. **7**: p. 229-246.

[7] Gohr, A. *Improving attacks on round-reduced speck32/64 using deep learning*. in *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*. 2019. Springer.

[8] Soos, M., K. Nohl, and C. Castelluccia. *Extending SAT solvers to cryptographic problems*. in *International Conference on Theory and Applications of Satisfiability Testing*. 2009. Springer.

[9] Mouha, N., Q. Wang, D .Gu, and B. Preneel. *Differential and linear cryptanalysis using mixed-integer linear programming*. in *Information Security and Cryptology: 7th International Conference, Inscrypt 2011, Beijing, China, November 30–December 3, 2011. Revised Selected Papers 7* .2012 .Springer.

[10] Zhang, L., J. Lu, Z. Wang, and C. Li, *Improved Differential-neural Cryptanalysis for Round-reduced Simeck32/64.* arXiv preprint arXiv:2301.11601, 2023.

[11] Benamira, A., D. Gerault, T. Peyrin, and Q.Q. Tan. *A deeper look at machine learning-based cryptanalysis*. in *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of*

Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I 40. 2021. Springer.

[12] Bao, Z ,.et al. *Enhancing differential-neural cryptanalysis*. in *International Conference on the Theory and Application of Cryptology and Information Security*. 2022. Springer.

[13] Zhang, L., Z. Wang, and J. Guo, *Improving Differential-Neural Cryptanalysis with Inception.* Cryptology ePrint Archive, 2022.

[14] Lyu, L., Y. Tu, and Y. Zhang. *Deep Learning Assisted Key Recovery Attack for Round-Reduced Simeck32/64.* in *International Conference on Information Security*. 2022. Springer.

[15] Lu, J., et al., *Improved Neural Distinguishers with (Related-key) Differentials: Applications in SIMON and SIMECK.* IACR Cryptol. ePrint Arch., 2022. **2022**: p. 30.

[16] Jain, A., V. Kohli, and G. Mishra, *Deep learning based differential distinguisher for lightweight cipher PRESENT.* Cryptology ePrint Archive, 2020.

[17] Bellini, E. and M. Rossi. *Performance comparison between deep learning-based and conventional cryptographic distinguishers*. in *Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3*. 2021. Springer.

[18] Tian, W. and B. Hu, *Deep learning assisted differential cryptanalysis for the lightweight cipher simon.* KSII Transactions on Internet & Information Systems, 2021. **15**.(٢)

[19] Wang, H., P. Cong, H. Jiang, and Y. Wei, *Security analysis of SIMON32/64 based on deep learning.* Computer Research and Development, 2021. **5**: p. 1056-1064.

[20] Baksi, A. and A. Baksi, *Machine learning-assisted differential distinguishers for lightweight ciphers.* Classical and Physical Security of Symmetric Key Cryptographic Algorithms, 2022: p. 141-162.

[21] Hou, Z., J. Ren, and S. Chen, *Cryptanalysis of round-reduced SIMON32 based on deep learning.* Cryptology ePrint Archive, 2021.

[22] Yadav, T. and M. Kumar. *Differential-ml distinguisher: Machine learning based generic extension for differential cryptanalysis*. in *International Conference on Cryptology and Information Security in Latin America*. 2021. Springer.

[23] Chen, Y., Y. Shen, H. Yu, and S. Yuan, *A new neural distinguisher considering features derived from multiple ciphertext pairs.* The Computer Journal, 2023. **66**(6): p. 1419-1433.

[24] Bao, Z., et al., *Conditional Differential-Neural Cryptanalysis.* IACR Cryptol. ePrint Arch., 2021. **2021**: p. 719.