نشریه علمی پدافند غیرعامل

سال دهم، شماره ۳، پاییز ۱۳۹۸، (پیاپی ۳۹): صص ۹۳-۷۵

برخی از مباحث نوین در رمزنگاری: ضرورت‌ها و کاربردها

هادی سلیمانی[1*]

تاریخ دریافت: ۱۳۹۷/۰۳/۰۶

تاریخ پذیرش: ۱۳۹۷/۰۷/۲۵

چکیده

طی دهه‌های اخیر همواره رمزنگاری مورد توجه ویژه محافل علمی و صنعتی در داخل و خارج کشور بوده است. علم رمزنگاری مسیر پرفرازونشیبی را در جوامع علمی سپری کرده است. رشد سریع فنّاوری در حوزه فن‌آوری اطلاعات، به همراه طرح مفاهیم نوینی چون اینترنت اشیاء و همچنین گسترش روزافزون کاربران و تنوع سرویس‌های جدید اینترنتی (همچون شبکه‌های پیچیده اجتماعی، سرویس‌های ابری و غیره)، سبب ایجاد چالش‌ها و در نتیجه نیازهای امنیتی جدیدی شده است. این مسئله سبب شده است که علم رمزنگاری به‌سرعت رشد کرده و به زیرشاخه‌های متعدد و نوینی تقسیم شود. هدف اصلی از ارائه این مقاله، بررسی برخی جهت‌گیری‌های اساسی موجود در رمزنگاری نوین است. در این مقاله روند دست‌آوردهای نوین در این حوزه را بررسی می‌کنیم که یا به‌کلی مفاهیمی نو را ارائه می‌کنند و یا شامل نوآوری‌های مهم در حوزه‌های رمزنگاری می‌باشند. بر همین اساس، این مقاله سه هدف را دنبال می‌کند: ۱- تأکید بر ضرورت شناخت و بررسی مباحث نوین رمزنگاری، ۲- روشن ساختن برخی از زوایای جدید رمزنگاری با بررسی برخی از مهم‌ترین تحولات صورت‌گرفته در رمزنگاری طی سالیان اخیر، ۳- بررسی اجمالی برخی از موضوعات و مفاهیم نوین ارائه‌شده با در نظر گرفتن جهت‌گیری‌های آتی رمزنگاری.

کلیدواژه‌ها: رمزنگاری مدرن، رمزنگاری متقارن، آینده‌پژوهی

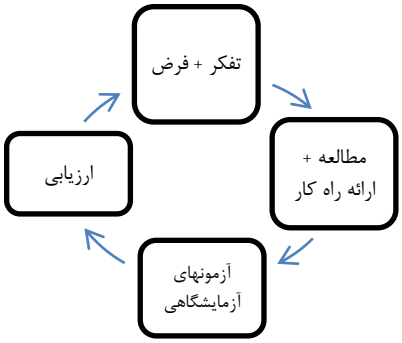
۱- استادیار گروه امنیت و رمزنگاری پژوهشکده فضای مجازی دانشگاه شهید بهشتی- (h_soleimany@sbu.ac.ir) نویسنده مسئول

۱- مقدمه

پیشرفت واقعی در هر جامعه مبتنی بر پیشرفت‌های علمی و درنتیجه تحقیقات هدفمند است. طبیعی است که مطالعات و تحقیقات باید با برنامه‌ای مدون، بر اساس پیش‌فرض‌هایی معلوم و اهدافی روشن و عملیاتی صورت گیرد تا بتوانند به هدف نهائی که پاسخ به نیازهای عملی جامعه است، نائل شوند. اگر یک طرح تحقیقاتی دارای امکان‌سنجی اولیه، طرح‌ریزی منسجم و هدف‌گذاری صحیح و روشن نباشد، نتایج حاصله از آن (از جمله تولید دانش صورت گرفته) شاید نتواند برای پاسخ به نیازهای واقعی یک جامعه به‌کار رود.

۱-۱- چرخه تولید علم هدفمند و انجام تحقیقات کاربردی

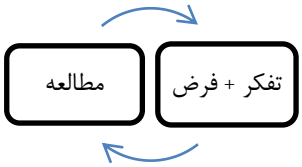
همان‌گونه که در شکل (۱) نمایش داده شده است، در هر پروژه تحقیقاتی، محققان با پیش‌فرض‌ها و ایده‌های خام اولیه شروع کرده و بر اساس آن‌ها مطالعاتی را انجام می‌دهند. بر اساس مطالعات انجام‌شده، راه‌کارهایی برای رسیدن به اهداف از پیش تعیین‌شده ارائه می‌کنند. مطالعات انجام‌شده و روش‌های مستخرج از آن‌ها باید در عمل و در یک محیط عملی، آزمایشگاهی محک شوند تا در گام بعدی ارزیابی شوند. در نهایت ارزیابی‌های حاصله می‌توانند به به‌روزرسانی پیش‌فرض‌ها و ایده‌های اولیه به‌منظور برنامه‌ریزی یک طرح تحقیقاتی و مطالعاتی هدفمند کمک کند. در فرآیند تکرار این چرخه، تولید علم مؤثر شکل می‌گیرد و خروجی‌های حاصل از این حلقه به‌عنوان محصولات عملی و کاربردی می‌توانند مورد استفاده قرار گیرند.



شکل (۱): چرخه تولید دانش هدفمند و مفید

۱-۲- چالش تحقیقات کاربردی (در رمزنگاری)

در عمل اگر به دو عنصر اصلی این چرخه نگاه بیاندازیم (شکل ۲)، این سؤال مطرح می‌شود که نقطه شروع تحقیقات را کجا باید تعریف کرد؟ از طرفی برای داشتن فرض‌ها و چارچوب فکری درست به‌منظور برنامه‌ریزی و طرح‌ریزی دقیق یک پروژه، نیاز به مطالعه است. از طرف دیگر، مطالعه صرف بدون پشتوانه کافی و داشتن طرح و برنامه منسجم، منجر به انجام تحقیقاتی بدون هدف‌گذاری دقیق شده و خروجی آن احتمالاً کاربردی نخواهد بود.



شکل (۲): چرخه تولید دانش هدفمند و مفید

شروع از نقطه مطالعه در تحقیقات رمزنگاری، بدون داشتن پیش‌فرض‌ها و یک چارچوب فکری درست، علاوه بر مشکل ذکرشده، سه چالش اساسی دارد:

چالش اول: وجود اطلاعات انبوه

سالانه هزاران مستند علمی در شاخه‌های رمزنگاری به‌صورت مقالات معتبر در کنفرانس‌ها، مجلات و یا گزارش‌های مراکز تحقیقاتی ارائه می‌شوند که حتی مطالعه گذرای همه این اطلاعات با توجه به امکانات، پشتوانه مالی و نیروی انسانی محدود غیرممکن است. همچنین مطالعه بدون پشتوانه می‌تواند منجر به اتلاف گسترده منابع کشور شود.

چالش دوم: وجود اطلاعات گمراه‌کننده

با توجه به اهمیت عمل رمزنگاری و نقش بی‌بدیل آن، بعضاً برخی دولت‌ها و مراکز تحقیقاتی وابسته به آن‌ها تلاش می‌کنند که موضوعات کم اهمیت را مهم‌تر جلوه دهند و یا بالعکس موضوعات پراهمیت را به‌صورت کم اهمیت نشان دهند. نداشتن برنامه مشخص و فهم صحیح در این حوزه می‌تواند منجر به فریب اطلاعاتی شود.

چالش سوم: عدم دسترسی به برخی اطلاعات کلیدی

با توجه به کاربردهای خاص رمزنگاری چه ازلحاظ مقابله با حملات و چه ازلحاظ اعمال حمله به امنیت دستگاه‌های دیگر، دولت‌ها تلاش می‌کنند که اطلاعات منتشرشده در این حوزه را حتی‌الامکان کنترل کنند. بر همین اساس اطلاعات کلیدی و نتایج مهم، معمولاً طبقه‌بندی محسوب می‌شوند و در اختیار عموم قرار نمی‌گیرند.

۱-۳- اهمیت بررسی هدفمند مباحث نوین و تهیه نقشه‌های راه

همان‌گونه که پیش از این در بخش ۱-۲ گفته شد، مطالعه بدون برنامه موضوعات رمزنگاری برای تحقیقات کاربردی مفید نخواهد بود. در حقیقت این بیان را بدین شکل می‌توان تکمیل کرد که قبل از آغاز طرح‌ریزی و تهیه نقشه راه در یک موضوع تحقیقاتی، احتیاج به یک پیش مطالعه جامع و کلی است. در این پیش مطالعه، هدف صرفاً بررسی کلی نیازهای حال و آینده ما در کنار روند تحولات آتی علمی ـ فنّاورانه است بدون آنکه بخواهیم جزئیات فنی تک‌تک موضوعات را بررسی کنیم. وقتی هدف ما تولید علم هدفمند و انجام تحقیقات کاربردی است، منها این تحقیقات یک «*نیاز*» است. بر همین اساس ابتدا باید موضوعات موردنیاز سنجیده و انتخاب شوند تا پس از آن بررسی شود که با توجه به محدودیت منابع موجود چگونه می‌توان به این نیازها پاسخ داد. بر همین اساس می‌توان مطالعات آینده‌پژوهی را به‌عنوان مقدمه‌ای برای درک فرصت‌ها و چالش‌های پیشرو دانست که می‌تواند زمینه‌ساز تعریف و طراحی نقشه‌های راه در یک حوزه باشند.

۱-۴- ساختار مقاله

در بخش ۲ ابتدا مهم‌ترین تحولات رخداده طی سالیان گذشته مورد بررسی قرار گرفته و هشت محور مختلف در این راستا معرفی شده‌اند. در بخش ۳ برخی موضوعات مهم نوین رمزنگاری معرفی شده‌اند. در بخش ۴ موضوعات معرفی‌شده به تفکیک میزان عملیاتی بودن آن‌ها تقسیم‌بندی شده‌اند. در نهایت بخش ۵ به جمع‌بندی مقاله اختصاص یافته است.

۲- تحولات مهم در تحقیقات رمزنگاری

طی سالیان گذشته پروژه‌های ملی و بین‌المللی متعددی در حوزه رمزنگاری اجرا و نتایج آن‌ها در قالب تعداد بسیار زیادی مقاله و گزارش‌های معتبر علمی و ارزشمند منتشر شده است. نتایج منتشرشده جدید نشان‌دهنده اتفاقات مهمی می‌باشند که فرصت‌ها و چالش‌های جدیدی را در چشم‌انداز این حوزه نوید می‌دهند. پیش از بررسی مباحث نوین رمزنگاری، ضروری است که فهم درستی از تحولات مهم صورت گرفته در تحقیقات اخیر رمزنگاری داشته باشیم. در این بخش، مهم‌ترین تحولات شکل‌گرفته طی سالیان اخیر را به شکل ذیل دسته‌بندی کرده‌ایم:

۲-۱- قابلیت پیاده‌سازی دسته جدیدی از پروتکل‌ها

طی سالیان اخیر اصلاحات بسیار اساسی و تأثیرگذاری توسط محققین در برخی از حوزه‌های رمزنگاری ارائه‌شده است. برخی پروتکل‌های رمزنگاری که پیش از این صرفاً به‌عنوان یک موضوع نظری مورد توجه مجامع علمی بودند، قابلیت پیاده‌سازی در دنیای واقعی را پیدا کرده‌اند و یا حداقل می‌توان گفت که جامعه علمی رمزنگاری نسبت به گذشته به راه‌حل‌های عملی و کارا بسیار نزدیک‌تر شده است. یک مثال مهم از این تغییر، پروتکل‌های *محاسبات چندجانبه امن*[1] یا اصطلاحاً MPC های نوین است. یک پروتکل MPC اجازه می‌دهد که مجموعه‌ای از افراد، تابعی از اطلاعات مخفی خود را محاسبه کنند، بدون آنکه (بخشی از) اطلاعات خصوصی آن‌ها نشت کند و درعین‌حال همه طرف‌ها مطمئن باشند که محاسبه تابع به‌صورت صحیح انجام شده است. از زمان ارائه اولین طرح در [۱]، از پروتکل‌های MPC برای مدت‌های مدیدی در مجامع علمی به‌عنوان یک موضوع غیرعملی و صرفاً نظری یاد می‌شد. اما امروزه با ارائه پروتکل‌های اصلاح‌شده نوین، به‌تدریج MPC می‌تواند به‌عنوان یک موضوع عملی به‌کار رود [۲]. همچنین به‌عنوان مثالی دیگر، می‌توان از برخی طرح‌های رمزنگاری مبتنی بر مشبکه نام برد که به‌تازگی ارائه‌شده‌اند و در مقابل ماشین‌های کوانتومی امن هستند. این دسته از طرح‌ها برخلاف اغلب طرح‌های پساکوآنتومی، کارایی نسبتاً مناسبی برای به‌کارگیری در دنیای واقعی دارند [۶-۳].

۲-۲- فقدان اثبات امنیتی پروتکل‌های کاربردی

تعداد قابل‌توجهی از پروتکل‌های بسیار کاربردی همچون SSL و یا IPsec، تحلیل دقیق امنیتی یا اصطلاحاً امنیت قابل اثبات ندارند. نداشتن امنیت قابل اثبات برای این دسته از پروتکل‌ها دو دلیل عمده دارد: اولین دلیل این است که عموماً مدل‌های امنیتی ارائه‌شده در محیط‌های دانشگاهی، قابلیت بازتعریف برای به‌کارگیری در این پروتکل‌ها را ندارند. دلیل دوم این است که به‌دلیل پیچیدگی پروتکل‌هایی که در واقعیت به‌کار می‌روند، فهم و همچنین تجزیه‌وتحلیل دقیق ریاضیاتی این پروتکل‌ها بسیار سخت و بعضاً غیرممکن است. این دلایل سبب شده است که تلاش‌های جدیدی برای تصحیح مدل‌های امنیتی به‌منظور به‌کارگیری در فهم و تجزیه‌وتحلیل پروتکل‌های واقعی و کاربردی شروع شود. از سوی دیگر با دانستن این نکته که این پروتکل‌ها دارای امنیت اثبات‌پذیر نیستند، تلاش‌هایی به‌منظور یافتن ضعف‌های جدی و استفاده از آن‌ها صورت پذیرفته است.

۲-۳- پیاده‌سازی (نا)امن اولیه‌ها و پروتکل‌ها

تعداد زیادی از محققین در مراکز تحقیقاتی معتبر بر روی نحوه پیاده‌سازی امن اولیه‌ها و پروتکل‌های رمزنگاری متمرکز شده‌اند.

[1] Multiparty Computation

دلیل این امر این است که هرروزه تعداد بیشتری ضعف در پیاده‌سازی اولیه‌ها و پروتکل‌های امنیتی در دنیای واقعی پیدا می‌شود. هر الگوریتم رمزنگاری با امنیت ریاضیاتی مناسب، پس از گذر از مرحله تجزیه‌وتحلیل، باید پیاده‌سازی شود تا در دنیای واقعی به‌کار رود. طبیعی است که اگر در پیاده‌سازی به حملات فیزیکی توجه نشود، الگوریتم علی‌رغم داشتن امنیت ریاضیاتی به‌راحتی شکسته می‌شود.

یک دسته از ضعف‌های مهمی که در مقابل حملات فیزیکی وجود دارند، ضعف‌های پیاده‌سازی در مقابل حملات کانال جانبی می‌باشند. برخلاف تحلیل‌های ریاضی که از ضعف‌های ساختاری الگوریتم بهره می‌برند، حملات کانال جانبی از اطلاعاتی که از نحوه پیاده‌سازی الگوریتم رمز نشت می‌کند، استفاده می‌کنند. پیاده‌سازی ناامن یک طرح رمز که به لحاظ ریاضیاتی امن است، به‌احتمال بسیار بالا در مقابل حملات کانال جانبی آسیب‌پذیر بوده و به‌صورت عملی شکسته می‌شود. در پاسخ به این چالش، طیف وسیعی از محققین بر روی پیاده‌سازی امن الگوریتم‌های رمزنگاری کارکرده و روش‌های متعدد فراوانی برای مقابله با حملات کانال جانبی پیشنهاد داده‌اند.

دسته دیگر از ضعف‌ها ناشی از پیاده‌سازی غلط برخی از اجزای پروتکل‌های امنیتی است. به‌عنوان مثال تحقیقات اخیر نشان داده است که تعداد قابل‌توجهی از کلیدهای عمومی استفاده‌شده در پروتکل‌هایی که مبتنی بر RSA هستند به‌دلیل ضعف مدیریت تولید کلید ناامن هستند.

هرچند این مقاله صرفاً با هدف بررسی اولیه‌ها و پروتکل‌های رمزنگاری نگارش شده است، اما ذکر چالش‌های موجود در حوزه پیاده‌سازی از آن جهت اهمیت دارد که ضعف‌های عملی موجود در پیاده‌سازی اولیه‌های رمزنگاری سبب شده است که برخی از طراحان، معیارهایی را در مرحله طراحی مدنظر قرار دهند که پیاده‌سازی امن الگوریتم‌های رمزنگاری را تسهیل کند [۸-۷].

۲-۴- استفاده از اولیه‌های متقارن ناامن

تحقیقات حوزه رمزنگاری متقارن طی دهه اخیر نشان داده است که تعدادی از اولیه‌های رمزنگاری به‌صورت گسترده در حوزه تبادل اطلاعات به‌کار می‌روند، ناامن هستند. برخی از حملات ارائه‌شده بر روی این اولیه‌ها ناشی از ضعف‌های ساختاری ـ آماری کشف‌شده برای آن‌هاست. برخی دیگر از حملات نیز از این واقعیت نشات می‌گیرند که به خاطر پیشرفت‌های فنّاورانه، قدرت محاسباتی نسبت به گذشته افزایش یافته است.

شکسته‌شدن یک الگوریتم رمزنگاری پس از پیاده‌سازی و استفاده گسترده، می‌تواند آثار خسارت‌بار و غیرقابل‌جبران داشته باشد. پس از تولید محصولات و ارائه به کاربران با توجه به محدودیت‌های مالی و زمانی، نمی‌توان به‌راحتی محصولات قبلی را از دست کاربران جمع‌آوری کرده و نسخه‌ای جدید ارائه کرد. به‌عنوان مثال شکسته شدن رمز Keeloq منجر به حمله‌ای عملی به سیستم امنیتی خودروها شده است و این در حالی است که ده‌ها میلیون خودروی ساخته‌شده در دهه اخیر در مقابل این حمله آسیب‌پذیر می‌باشند. یا به‌عنوان مثالی دیگر شکسته شدن رمزهای الگوریتم A5/1 و A5/2 منجر به حملات عملی به سیستم‌های نسل اول و دوم موبایل شدند [۹]، درحالی‌که صدها میلیون کاربر از آن‌ها استفاده می‌کردند (و در برخی کشورها هنوز هم در حال استفاده می‌باشند). بدافزار Flame که به‌طور گسترده تعدادی از کشورهای خاورمیانه را مورد هدف قرارداد، از ضعف تابع درهم‌ساز MD5 استفاده می‌کند [۱۰]. همچنین به‌تازگی برای تابع درهم‌ساز SHA-1 تصادم‌های عملی پیدا شده است [۱۳-۱۱]. تعداد زیادی از حملات عملی به پروتکل‌های کاربردی رمزنگاری مبتنی بر ضعف‌های شناخته‌شده الگوریتم رمز RC4 است که ضعف‌های آن در مجامع علمی بارها مطرح‌شده است [۱۸-۱۴].

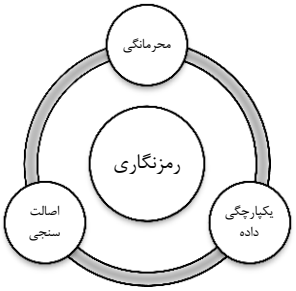
۲-۵- نیازهای جدید

از آنجائی که رمزنگاری دارای جایگاه ویژه‌ای در تأمین امنیت دستگاه‌های ارتباطی است، در طول زمان به‌تدریج برای کاربردهای عملی مختلف، اولیه‌ها و پروتکل‌های رمزنگاری اختصاصی جدیدی طراحی شده است. این طراحی‌ها بعضاً پس از تجزیه‌وتحلیل‌های امنیتی به شکل استانداردهای بین‌المللی درآمده‌اند و امروزه به‌صورت گسترده کاربرد دارند. با پیشرفت‌های خیره‌کننده و بسیار سریع فنّاوری‌های ارتباطی، نیازهای جدیدی شکل‌گرفته است که طرح‌های رمزنگاری معمول قادر به پاسخ‌گویی به آن‌ها نیستند. بر همین اساس برای هر نیاز جدید، احتیاج به طرح‌های با ویژگی‌های نوین است. این امر سبب شده است که طی سالیان اخیر، زیرشاخه‌های جدیدی از علم رمزنگاری شکل بگیرد و به‌طور جدی‌تر دنبال شوند.

به‌عنوان‌مثال با شکل‌گیری تدریجی اینترنت اشیا و یا گسترش استفاده از تراشه‌های RFID، احتیاج به دسته‌ای از اولیه‌های رمزنگاری به‌وجود آمده است که به لحاظ برخی ملاحظات همچون مساحت پیاده‌سازی، توان و انرژی مصرفی، تأخیر و یا پارامترهای دیگر، دچار محدودیت‌های جدی می‌باشند. به‌عنوان مثالی دیگر، می‌توان از نیاز به دسته‌ای خاص از رمزها نام برد که باید قابلیت جست‌وجو بر روی متون رمزشده را برای کاربران در سرویس‌های ابری فراهم کنند.

۲-۶- اهداف جدید رمزنگاری

به‌طورمعمول مهم‌ترین اهداف رمزنگاری را برآورده ساختن محرمانگی، احراز اصالت و همچنین جامعیت پیام می‌دانند (شکل ۳). محرمانگی پیام به این معنی که اطلاعات باید مخفی نگه‌داشته شود و هیچ فرد غیرمجازی که کلید رمزنگار را ندارد، قادر به بازیابی اطلاعات نباشد. احراز اصالت پیام به این معنی است که برای دریافت‌کننده اطلاعات، ممکن باشد که هویت فرستنده حقیقی داده‌ها را احراز کند. جامعیت پیام نیز به این معنی است که با تغییر بخشی از متن رمزشده، فرد گیرنده پیام متوجه شود که پیام تغییر کرده است.

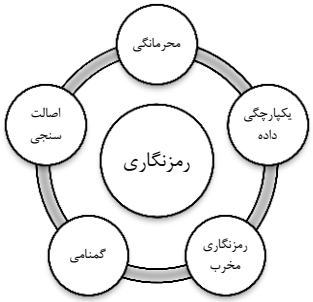


شکل (۳): اهداف معمول رمزنگاری

بدیهی است که با تعریف هر هدف جدید، دسته جدیدی از اولیه‌ها و پروتکل‌های نوین تعریف می‌شوند که در چارچوب مفهومی پیشین صدق نمی‌کنند. به‌نوعی این اهداف جدید را می‌توان در قالب نیازهای جدید که در بخش قبل معرفی شده‌اند، دسته‌بندی کرد. اما از آنجاکه این تحولات ریشه‌ای‌تر بوده و عملاً اهداف جدیدی را به دنبال دارند، به‌عنوان تحولی جداگانه در نظر گرفته شده‌اند. از این منظر می‌توان به دو مفهوم که به‌عنوان اهداف متفاوتی که بر اساس رویکردهای جدید تعریف شده‌اند، اشاره کرد.

مفهوم اول کلپتوگرافی است که در بخش ۳ به‌صورت مختصر آن را شرح خواهیم داد. در حقیقت هدف از کلپتوگرافی برخلاف اهداف اولیه رمزنگاری، ایجاد یک بستر ناامن برای کاربران با ایجاد یک درب پشتی در سیستم رمزنگاری است به‌گونه‌ای که کاربر متوجه آن نشود و اگر متوجه شود نتواند از آن به نفع خود استفاده کند [۱۹].

مفهوم دومی که به‌تازگی و به‌طور ویژه پس از گسترش اینترنت مورد توجه قرار گرفته است، موضوع *گمنامی* است. در حقیقت آنچه در اینجا مورد نیاز است، متفاوت از محرمانگی است. هدف در اینجا ارائه یک سیستم رمزنگاری است به‌گونه‌ای که مشخص نشود که فرد مشغول چه کاری است. به‌عنوان‌مثال شبکه‌های گمنام چون Tor، بستری برای کاربران ایجاد می‌کنند که برای صاحبان شبکه مشخص نشود که کاربر مشغول چه فعالیتی است [۲۰]. به‌عنوان مثالی دیگر پول‌های رمزی[1] مانند بیت کوئن[2] به نحوی طراحی‌شده‌اند که در هنگام دادوستد با این واحدهای پولی، مشخص نشود که خریدار و فروشنده چه کسانی هستند و چه چیزی را معامله کرده‌اند.



شکل (۴): برخی از اهداف تکمیلی رمزنگاری

۲-۷- تمایل به طراحی ابزارهای خودکار

پیچیدگی مضاعف پروتکل‌ها و اولیه‌های رمزنگاری منجر به پیچیدگی‌های بیشتر در فرآیند تحلیل امنیتی و ارائه اثبات‌های امنیتی آن‌ها شده است. از سوی دیگر در بحث پیاده‌سازی امن، شاهد چالشی مشابه هستیم. در نظر گرفتن تمامی تهدیدات فیزیکی به‌صورت هم‌زمان و ارائه یک پیاده‌سازی امن که همچنان کارا باشد تبدیل به موضوعی بسیار پیچیده شده است.

بر همین اساس تمایل به استفاده از ابزارهایی خودکار و کارا برای تجزیه‌وتحلیل امنیت یک الگوریتم و یا پیاده‌سازی امن یک الگوریتم، بیش‌ازپیش گسترش یافته است. یک سؤال کلیدی که می‌تواند تأثیرات عمیقی در حوزه طراحی و همچنین پیاده‌سازی الگوریتم‌های رمزنگاری بگذارد، این است که توسعه این ابزارهای خودکار چقدر می‌تواند مفید فایده باشد؟ آیا یک ابزار به‌صورت خودکار می‌تواند بخش‌هایی از یک الگوریتم (یا بخش‌هایی از پیاده‌سازی آن) را که منجر به ضعف‌های جدی می‌شوند را تشخیص دهد؟

نتایج تحقیقات اخیر نشان می‌دهد که تعداد ضعف‌های ممکن و حملات احتمالی بسیار زیاد می‌باشند. فلذا دست‌یابی به ابزارهای خودکار عمومی به‌گونه‌ای که تمام حالت‌های ممکن را بررسی کنند، قطعاً مفید فایده نخواهند بود. فلذا ابزارهای کارا معمولاً احتیاج به پیش‌فرض‌های خاص و یا به‌کار بردن ابتکارات

[1] Cryptocurrency
[2] Bitcoin

جدید دارد.

به لحاظ تئوریک سؤالات متعددی در این حوزه وجود دارد: چه فاصله‌ای بین یک ابزار ایده‌آل و یک ابزار کارا در عالم واقع وجود دارد؟ برای تقریب ذهن، می‌توان به مثال سنتز یک مدار بولی اشاره کرد که به لحاظ تئوریک در یک‌زمان نمائی قابل انجام است، اما در عمل ابزارهای کارایی وجود دارند که به‌صورت بسیار مناسب می‌توانند طراحان را برای رسیدن به نتیجه‌ای مناسب یاری کنند. اهداف محققان این حوزه نیز بررسی وجود یا عدم وجود چنین ابزارهایی برای تحلیل الگوریتم‌های رمزنگاری و همچنین پیاده‌سازی آن‌ها هست.

۲-۸- طرح موضوعاتی با تخصص‌های ترکیبی

هر پروژه رمزنگاری عموماً توسط گروهی از محققین با تخصص‌های مختلف انجام می‌شود. به‌طورکلی می‌توان محققین را برحسب علاقه و جهت‌گیری‌های کلی تحقیقاتی آن‌ها به سه دسته کلی تقسیم کرد: ۱- محققینی که بر روی مباحث نظری مطلق همچون اثبات‌های امنیتی و یا فرمالیته کردن مدل‌های امنیتی متمرکز هستند. ۲- محققینی که بر روی مباحث کاربردی‌تر همچون طراحی و تحلیل اولیه‌ها و پروتکل‌های کاربردی متمرکز هستند. ۳- پیاده‌سازان که در حقیقت وظیفه پیاده کردن الگوریتم‌های رمزنگاری را در قالب سخت‌افزاری و یا نرم‌افزاری دارند.

پیش از این در موارد متعددی این سه دسته به‌صورت موازی و یا در طول یکدیگر بر روی یک موضوع کار می‌کردند، بدون آنکه به‌صورت جدی در تعامل با یکدیگر باشند. به‌عنوان‌مثال یک محقق کاربردی از تفاهم اولیه مطرح‌شده و قضایای اثبات‌شده در خصوص ساختارهای رمزنگاری توسط گروه اول استفاده می‌کرد تا طرح جدیدی ارائه کند. سپس یک گروه از پیاده‌سازان طراحی ارائه‌شده را به‌صورت امن و کارا پیاده می‌کردند.

طی سالیان اخیر با طرح کاربردهای نوین و پیچیدگی روزافزون حاصل از پیشرفت‌های جدید فنّاورانه، بیش‌ازپیش شاهد تعریف پروژه‌هایی هستیم که سه گروه فوق با همکاری مستمر، نسبت به ترکیب تخصص‌های خود به‌منظور ارائه یک محصول کاربردی، اقدام می‌کنند.

به‌عنوان‌مثال، مرحله طراحی یک اولیه رمزنگاری و مرحله پیاده‌سازی امن در مقابل حملات کانال جانبی، معمولاً به‌صورت مجری صورت می‌پذیرفت (و همچنان می‌پذیرد). در سالیان اخیر چند پروژه تحقیقاتی، اولیه‌های رمزنگاری جدیدی را معرفی کرده‌اند که در طول طراحی و انتخاب ساختار و یا اجزای اولیه، مقاومت در مقابل حملات کانال جانبی توان دیده‌شده است.

به‌عنوان مثالی دیگر می‌توان به رویکرد ترکیب تخصص‌های محققین در مباحث تئوریک امنیت‌های اثبات‌پذیر با تحلیل‌گران پروتکل‌های رمزنگاری را نام برد که معرفی ابزارهای خودکار تائید امنیتی[1] پروتکل‌های رمزنگاری را به‌عنوان هدف خود دنبال می‌کنند. این رویکردهای نوین، صرفاً با بسترسازی مناسب جهت ترکیب تخصص‌های گوناگون امکان‌پذیر است.

۳- برخی از موضوعات نوین رمزنگاری

در حوزه رمزنگاری تعداد بسیار زیادی موضوع و زیرشاخه وجود دارد که کم‌وبیش بر روی همه آن‌ها در مجامع بین‌المللی تحقیقات جدی در حال انجام است. هرچند که بررسی تمامی موضوعات و دنبال کردن تمامی تحقیقات جاری در جوامع بین‌المللی خالی از لطف نیست، اما بررسی تمامی موضوعات رمزنگاری با توجه به محدودیت‌های زمانی و انسانی احتمالی در کشور، امری چالش‌برانگیز است. فلذا با توجه به محدودیت‌های احتمالی، معمولاً ناگزیر به اولویت‌بندی طرح و بررسی موضوعات هستیم. تحولات مهم در حوزه رمزنگاری را در بخش ۲ و در قالب هشت محور بررسی کردیم. بر اساس این تحولات، موضوعاتی مهمی که بر اساس دانش نگارنده می‌توانند مورد توجه قرار گیرند، در این بخش از مقاله معرفی می‌شوند. بدیهی است که اطلاعات نویسنده قطعاً ناقص بوده و احیاناً بدون ایراد و خطا نیست. این مقاله صرفاً تلاشی برای فهم بیشتر مباحث نوین رمزنگاری در چارچوب تعریف‌شده مذکور است که امیدواریم توسط محققین دیگر تکمیل و تصحیح شود.

به‌منظور شفافیت بیشتر، برای هر موضوع پیشنهادی، بخش جداگانه‌ای در نظر گرفته‌ایم. در ابتدای هر بخش، موضوع موردنظر به‌صورت اجمالی معرفی شده و ضمن تبیین جایگاه و دلایل اهمیت آن، سیر تحولات گذشته و شرایط فعلی موضوع بررسی می‌شود. موضوعات تحت دو عنوان کلی تقسیم‌بندی شده‌اند: اولیه‌ها و پروتکل‌های رمزنگاری. در بخش ۴ روشن می‌سازیم که کدام یک از این موضوعات از اهمیت بیشتری برای بررسی برخوردار می‌باشند.

۳-۱- اولیه‌ها

ما ابتدا اولیه‌های رمزنگاری متعارف و معمول را بررسی کرده و به معرفی مسائل باز در حوزه اولیه‌های رمزنگار متقارن و جهت‌گیری‌های مهم این دسته از الگوریتم‌ها می‌پردازیم. پس از آن با در نظر گرفتن این نکته که الگوریتم‌های متعارف، پاسخگوی برخی نیازهای اساسی جدید نمی‌باشند، در ادامه

[1] Verification of cryptography

موضوعات مطالعاتی جدید دیگری را همراه با جهت‌گیری‌های اصلی مرتبط معرفی می‌کنیم.

۳-۱-۱- رمزنگاری متقارن استاندارد و معمول

طی ۱۵ سال گذشته تلاش‌ها و پروژه‌های بین‌المللی متعددی چون AES، SHA-3، eSTREAM منجر به ارائه الگوریتم‌های مختلفی با امنیت‌های بالا و کارایی[1] نسبتاً مناسب شده‌اند و بر اساس نتایج آن‌ها معیارهای مهمی در طراحی اولیه‌های متقارن به‌دست آمده است. این پروژه‌ها سبب شده‌اند که فهم ما از اولیه‌های متقارن در مجموع مناسب باشد. اما کماکان برخی نکات مهم در این حوزه وجود دارد که در ادامه به آن‌ها اشاره می‌شود.

۳-۱-۱-۱- جدول کلید

در حوزه تحقیقات بنیادینِ رمزنگاری متقارن، موضوع جدول کلید رمزهای قالبی و اثرات آن بر روی امنیت اولیه‌های رمزنگاری همچنان یک موضوع باز محسوب می‌شود. جدول طرح کلید از مجموعه‌ای از عملیات ریاضی و منطقی استفاده می‌کند تا از کلید اصلی که نسبتاً کوتاه است، زیر کلیدهای دور را تولید کند. جدول کلید نقشی اساسی در تأمین امنیت الگوریتم می‌تواند داشته باشد. اما نکته اساسی این است که پیچیدگی جدول کلید می‌تواند آثار نامطلوبی بر روی کارآمدی طرح (همچون تأخیر، پیاده‌سازی و ...) داشته باشد. این موضوع هنوز به‌عنوان یک مسئله باز در جامعه رمزنگاری باقی‌مانده است که تأثیر جدول کلید بر تحلیل‌های ریاضی و یا حملات کانال جانبی چیست؟ [۲۳-۲۱] بررسی نقش جدول کلید در امنیت طرح‌های رمزنگاری، موضوعی برجسته و جدید در تحقیقات است. به‌طورکلی عقیده عمومی رمزنگاران بر این است که در حالتی که کلید ثابت و نامعلوم (برای حمله‌کننده) است، امنیت رمزهای قالبی به‌خوبی فهمیده شده و قابل اثبات هستند. الگوریتم‌های تولید کلید معمولاً به‌صورت پیچیده طراحی می‌شوند و شامل اجزای غیرخطی و خطی هستند. اما نکته اساسی این است که پیچیدگی جدول کلید می‌تواند آثار نامطلوبی بر روی کارآمدی طرح داشته باشد (همچون افزایش تأخیر یا مساحت پیاده‌سازی و ...). برخلاف اهمیت این موضوع، جدول کلید کمتر مورد بررسی قرارگرفته است و تنها به‌تازگی تحقیقات جدی در این زمینه شروع شده است. بر همین اساس و برای پاسخ به این پرسش، اخیراً تحقیقات جدیدی به‌منظور بررسی روش‌های طراحی کلید و امنیت آن در مقابل تحلیل‌های ریاضی و حملات کانال جانبی آغازشده است [۲۴].

[1] Efficiency

۳-۱-۱-۲- رمزهای قالبی Tweakable

طراحی رمزهای قالبی Tweakable نیز از موضوعات باز جامعه رمزنگاری است که طی سالیان اخیر توجه بیشتری به آن شده است. کاندیداهای متعددی از مسابقه سزار در رمزهای قالبی Tweakable استفاده می‌کنند. برای مثال می‌توان طرح‌های ذیل را برشمرد: DeoxysDeoxys [۲۵]، SCREAM [26]، Joltik [۲۷]، KIASU [۲۸] و Silver [۲۹]. در این طرح‌ها رمز قالبی علاوه بر کلید از یک ثابت آشکار به نام tweak استفاده می‌کنند. وجود Tweak باعث می‌شود که حمله‌کننده بیش‌ازپیش، توان حمله داشته باشد چراکه می‌تواند مقدار tweak را کنترل کند.

۳-۱-۱-۳- طرح‌های مبتنی بر مقابله با کانال جانبی

مرحله طراحی یک اولیه رمزنگاری و مرحله پیاده‌سازی امن در مقابل حملات کانال جانبی، معمولاً به‌صورت مجزی صورت می‌پذیرفت (و همچنان می‌پذیرد). در سالیان اخیر چند پروژه تحقیقاتی اولیه‌های رمزنگاری جدیدی را معرفی کرده‌اند که در طول طراحی و انتخاب ساختار و یا اجزای اولیه، مقاومت در مقابل حملات کانال جانبی توان برای آن‌ها دیده شده است [۸-۷].

۳-۱-۱-۴- حملات جدید

مطالعات اخیر منجر به ارائه برخی تحلیل‌های جدید همچون تحلیل خطی با همبستگی صفر [۳۰] و یا تحلیل بایکلیک شده است. گسترش تعداد تحلیل‌های موجود سبب به وجود آمدن جهت‌گیری جدیدی مبنی بر یافتن روابط بین این تحلیل‌ها شده است. در نظر گرفتن همه تحلیل‌ها کار بسیار پیچیده‌ای است و دانستن ارتباط بین این حملات می‌تواند در این راستا مفید باشد [۳۳-۳۱].

۳-۱-۲- رمزگذاری احراز اصالت

الگوریتم‌های استاندارد فعلی صرفاً برای کاربردهای خاصی قابل استفاده می‌باشند که صرفاً نیاز به محرمانگی *یا* احراز اصالت است. در برخی از کاربردها احتیاج به فراهم آوردن محرمانگی و احراز اصالت به‌طور هم‌زمان است. رمزگذاری احراز اصالت‌شده (AE)[2] یک عملیات از نوع رمزگذاری است که به‌طور *هم‌زمان* محرمانگی و اصالت داده را برای کاربران تضمین می‌کند. با توجه به کاربردهای گسترده رمزگذاری احراز اصالت شده و نبود یک طرح امن با کارایی بالا، در سالیان گذشته جامعه رمزنگاری توجه خاصی به این دسته از عناصر رمزنگاری از خود نشان داده است. وجود اشتباه در پیاده‌سازی طرح‌های رمزگذاری احراز اصالت‌شده،

[2] Authenticated encryption

اخیراً منجر به دسته‌ای از حملات عملی به پروتکل‌های مهمی چون SSL[1] و TLS[2] شده است [۳۴] که کاربردهای وسیعی در تجارت الکترونیک و بانکداری آنلاین دارند. از سوی دیگر طرح‌های موجود همچون استفاده از یک رمزنگار و سپس به‌کارگیری *کد احراز هویت پیام*[3] (MAC) از کارایی لازم برخوردار نمی‌باشند. به‌طور خاص این طرح‌ها برای هر کاربر، احتیاج به دو کلیددارند (یکی برای رمزنگار و دیگری برای کد احراز هویت پیام). توجه به این نکته از آنجا حائز اهمیت است که در دنیای واقعی، توزیع کلید یکی از مباحث چالش‌برانگیز است. چالش‌های امنیتی و عدم کارایی طرح‌های موجود در کنار نیاز گسترده شبکه‌های بانکی، صنایع مخابراتی، ارتباطات، اینترنت و ... منجر به تعریف یک مسابقه بین‌المللی (تحت عنوان مسابقه سزار[4]) و با حمایت مؤسسه ملی فناوری و استانداردها[5] به‌منظور طراحی و تحلیل طرح‌های رمزگذاری احراز اصالت شده است [۳۵]. این مسابقه در حال حاضر کاندیدهای دور نهائی را انتخاب کرده است و انتظار می‌رود که تا سال ۲۰۱۹ کاندیدهای منتخب معرفی شوند.

جهت‌گیری‌های اصلی:

در حال حاضر جهت‌گیری‌های اصلی در این موضوع عبارت‌اند از: ۱- ارائه طرح‌های نوین و کارآمدتر (که به‌طور خاص طرح‌های مسابقه سزار از اهمیت بیشتری برخوردار هستند) ۲- تلاش برای یافتن نقاط ضعف طرح‌های فعلی.

در حوزه اول یعنی ارائه طرح‌های جدید، موضوعات مهمی وجود دارد که به‌نوعی در اشتراک با بحث جهت‌گیری‌های اصلی حوزه رمزنگاری متقارن متعارف هستند:

ایده‌های جدید؛ حملات جدید: با ارائه طرح‌های جدیدی که مبتنی بر ایده‌های نوین هستند، احتمال کشف حملات جدیدی وجود دارد که پیش از این شناخته‌شده نبودند، چراکه قابل‌اعمال به طرح‌های قدیمی نبودند [۴۰-۳۶].

مسائل بازطراحی: همچون رمزهای قالبی متعارف، موضوع طراحی جدول کلید امن و کارا در این حوزه نیاز به تحقیقات بیشتری دارد. به‌طور ویژه بحث رمزهای قالبی Tweakable در تعداد قابل‌توجهی از طرح‌ها به‌کار رفته‌اند. استفاده از رمزهای قالبی Tweakable در این طرح‌ها، امنیت بهتری را ارائه می‌کنند اما به تحلیل‌گر پتانسیل استفاده از tweak را هم می‌دهند. فلذا به تحقیقات بیشتری برای این دسته از رمزهای قالبی نیاز است [۲۴].

یکی از طرح‌ها با در نظر گفتن حملات کانال جانبی طراحی شده است که می‌تواند در این حوزه الهام‌بخش طراحی‌های جدید باشد.

۳-۱-۳- اولیه‌های سبک

در حوزه اولیه‌های سبک رمزنگاری، یک خلأ نسبی وجود دارد که البته به خاطر طراحی‌های جدید طی سالیان اخیر کمتر شده است. مهم‌ترین مشکل تأمین امنیت در تجهیزات کوچک نظیر RFID این است که اولیه‌هایی که می‌خواهند در این موارد به‌کار بروند، به‌شدت دارای محدودیت‌های نظیر فضای پیاده‌سازی می‌باشند. درنتیجه مساحت پیاده‌سازی اولیه‌های به‌کاررفته باید کم باشد. از آنجائی که در این تجهیزات، تغذیه به‌صورت باتری است یا از یک میدان مغناطیسی خارجی بدین منظور استفاده می‌شود، مصرف توان اولیه‌های به‌کاررفته نیز باید کم باشد. همچنین اولیه‌ها باید دارای سرعت نسبتاً مناسب باشند تا بتوانند در پروتکل‌های واقعی به‌کار روند.

لازم به ذکر است که اغلب قریب به‌اتفاق رمزهای ارائه‌شده در دهه ۹۰ میلادی در دسته رمزهای سبک تقسیم‌بندی می‌شوند. چراکه با توجه به محدودیت‌های شدید سخت‌افزاری در قدیم، طراحان به‌ناچار اولیه‌های با ساختار ساده طراحی می‌کردند که برای محیط‌های با محدودیت منابع، مناسب باشند. با توجه به آنکه این اولیه‌ها عموماً به‌صورت مخفی طراحی و پیاده‌سازی شده‌اند، عموماً شکسته شده‌اند و یا ضعف‌های جدی دارند.

جهت‌گیری‌های اصلی:

درحالی‌که حاضر جهت‌گیری‌های اصلی در این موضوع عبارت‌اند از: ۱- استفاده از اولیه‌های سبک شکسته شده که هنوز کاربرد دارند و یا بهبود حملات. ۲- طراحی اولیه‌های سبک جدید بر مبنای یک یا چند پارامتر خاص مانند مساحت پیاده‌سازی، توان مصرفی، انرژی و یا تأخیر (به‌خصوص در حوزه اولیه‌های با مصرف انرژی کم و یا تأخیر کم). لازم به ذکر است که روند طراحی اولیه‌های سبک که از حدود ده سال پیش آغازشده است [۴۲-۴۱]، کماکان ادامه دارد.

۳-۱-۴- رمزنگاری با فرمت‌های خاص متون آشکار و (یا) متون رمزشده

سرویس‌های جدیدی که در حوزه فن‌آوری اطلاعات و ارتباطات امروزه ارائه می‌شوند، سبب ایجاد نیاز به امنیت‌هایی با تعریف خاص و جدید شده‌اند که توسط اولیه‌های متعارف برآورده

[1] Secure Sockets Layer
[2] Transport Layer Security
[3] Message authentication code
[4] CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness)
[5] National Institute of Standards and Technology

نمی‌شوند. دسته‌ای از کاربردها نیاز به اولیه‌هایی دارند که علاوه برداشتن امنیت، متن‌های آشکار یا رمزشده ویژگی‌های خاصی داشته باشند. در این بخش سه دسته مهم را اجمالاً بررسی و معرفی می‌کنیم: ۱- رمزنگاری با حفظ فرمت اولیه (FPE) [1] ۲- رمزنگاری با انتقال فرمت (FTE) [2] ۳- رمزنگاری شگرف (HE) [3]. دسته اول این رمزها (FPE)، بحث بسیار نوینی در جامعه رمزنگاری نیست اما پیش‌زمینه‌ای برای کاربر روی موضوعات دسته دوم و سوم (FTE و HE) است که در دو سال اخیر ارائه‌شده‌اند.

۳-۱-۴-۱- رمزنگاری با حفظ فرمت اولیه (FPE)

تعریف: رمزنگاری با حفظ فرمت اولیه (FPE) به‌نوعی از رمزنگاری اطلاق می‌شود که خروجی الگوریتم (متن رمزشده) دارای یک *فرمت* [4] مشابه ورودی الگوریتم (متن اصلی) باشد. معنای فرمت در این تعریف برحسب کاربرد می‌تواند متفاوت باشد. رمز کردن یک کلمه انگلیسی به‌گونه‌ای که متن رمزشده نیز یک کلمه انگلیسی شود، نمونه‌ای از یک FPE است (در اینجا فرمت، مجموعه کلمات انگلیسی هست). فرضاً اگر فرمت متن را مجموعه متن‌هایی با n بیت دلخواه در نظر بگیریم (مجموعه $\{\{0,1\}^n, \dots, \{0,1\}^{2n-1}\}$)، یک رمز قالبی دلخواه نیز FPE محسوب می‌شود. امنیت تعریف‌شده برای FPE، همانند رمزهای قالبی بدین شکل است: یک حمله‌کننده نتواند الگوریتم را از یک جایگشت ایده‌آل تشخیص دهد.

کاربردها:

کاربرد یک FPE زمانی است که می‌خواهیم فرمت متن رمزشده به شکل خاصی باشد. به‌طور ویژه، FPE در تولید اعداد طبیعی شبه تصادفی کاربرد دارد. یکی از مهم‌ترین کاربردها در تولید شماره‌های تصادفی بزرگ برای کارت‌های هوشمند است. فرضاً در بانکداری به‌منظور رمز کردن یک عدد ۱۶ رقمی کارت اعتباری بانک به‌گونه‌ای که متن رمزشده نیز یک عدد ۱۶ رقمی شود، می‌توان از یک FPE استفاده کرد. مد FFX [۴۳]، طرح BPS [۴۴]، طرح Swap-or-not [۴۵] از مهم‌ترین طرح‌های ارائه‌شده متأخر می‌باشند.

۳-۱-۴-۲- رمزنگاری با انتقال فرمت (FTE)

رمزنگاری FTE، روشی است که این قابلیت را دارد که متن رمزشده را به هر فرمت انتخابی منتقل کند. در حقیقت FTE مرتبط با FPE است با این تفاوت که در FPE *هدف حفظ فرمت متن آشکار است* و درنتیجه فرض بر این است که خود متن آشکار دارای یک فرمت خاص است (اما در FTE چنین فرضی نداریم). این روش در سال ۲۰۱۳ ارائه شد [۴۶].

کاربرد:

مهم‌ترین کاربرد عملی FTE، استفاده از آن در مقابله با بازرسی ژرف بسته‌ها (DPI) [5] هست. روش DPI، نوعی فیلتر بسته‌ها [6] در شبکه‌های کامپیوتری است که بخش داده‌های بسته را (و بعضاً بخش هدر [7] بسته‌ها) بررسی می‌کند تا بر این اساس بتواند وجود یا عدم وجود اطلاعات خاص دربسته را شناسایی کند. به‌طور دقیق‌تر در روش DPI، بر اساس روش‌های *یادگیری ماشینی* [8] یا دیگر روش‌های آماری، تعدادی *عبارات منظم* [9] برای پروتکل‌های مورد هدف تعریف می‌شوند. با تطبیق دادن محتویات بسته‌ها با این عبارات منظم، سیستم می‌تواند تشخیص دهد که آیا بسته‌ها جزء دسترسی‌های غیرمجاز می‌باشند یا مجاز. به‌عبارتی‌دیگر، می‌توان عبارات منظم را به‌عنوان اثرهای انگشت [10] دسته‌ای خاص از داده تعبیر کرد که به شناخت آن‌ها کمک می‌کنند. ادعای طراحان FTE این است که در صورت استفاده از FTE، سیستم به‌صورت هوشمند توانایی شناخت بسته‌های غیرمجاز را از طریق DPI نخواهد داشت چراکه محتویات بسته به شکلی کدگذاری می‌شوند که منطبق بر عبارات منظم نمی‌باشند و مانند بسته‌ای معمول به نظر می‌رسند. طراحان FTE مهم‌ترین انگیزه خود را مقابله با سانسور اینترنت در برخی از کشورهای آسیایی اعلام کرده‌اند و نرم‌افزاری را نیز به‌عنوان محصول، تولید و در وب‌سایت این پروژه قرار داده‌اند [۴۷]. البته روش‌های مختلفی برای دور زدن سیستم فیلترینگ اینترنت وجود دارد. اما استفاده از FTE، به نظر روشی خلاقانه است که مقابله با آن نیاز به راه‌حلی علمی دارد. روش‌های قدیمی مبارزه با فیلترینگ عموماً به این شکل است که اطلاعات آدرس سایت مورد نیاز توسط کاربر رمز شده و به یک رابط سوم ارسال می‌شود تا داده‌های وب‌سایت فیلترشده برای وی ارسال شود. این روش‌ها از طریق روش‌هایی چون DPI قابل شناسایی است. اما FTE روشی عمیق‌تر است. بر همین اساس طراحان FTE، نرم‌افزار ارائه‌شده خود را (به‌طور موقت) در کشور چین امتحان کرده‌اند که به‌خوبی (برای مدتی) توانسته است که سیستم فیلترینگ را فریب داده و از آن عبور کند. هرچند ذکر این نکته ضروری است که به خاطر خواص آماری

[1] Format-preserving encryption
[2] Format-transforming encryption
[3] Honey Encryption
[4] Format

[5] Deep packet inspection
[6] Packet filtering
[7] Header
[8] Machine learning
[9] Regular expressions
[10] Fingerprints

نامطلوب این طرح اخیراً شکسته شده است.

۳-۱-۴-۳- رمزنگاری شگرف (HE)

تعریف

در زبان انگلیسی کلمه Honey دو کاربرد دارد: ۱- به معنی عسل (و یا در کاربردهایی که استعاره از یک‌چیز شیرین یا دوست‌داشتنی دارد) ۲- درجایی که شیء یا پدیده‌ای را به‌عنوان شگرف، بسیار عالی و یا فاخر می‌خواهند توصیف کنند. در مباحث مطرح‌شده در حیطه امنیت و رمزنگاری، مفهوم Honey به دسته‌ای از الگوریتم‌ها اطلاق می‌شود که ویژگی ممتازی دارند. این الگوریتم‌ها بر اساس سازوکاری خاص، حمله‌کننده را در زمان حمله به یک طعمه[1] حواله می‌دهند که برای فریب دادن مهاجم به‌کار رفته است. این طعمه به‌گونه‌ای است که حمله‌کننده، نتواند تشخیص دهد که حمله‌اش موفقیت‌آمیز بوده است یا خیر. این مفهوم در مدل‌ها و سناریوهای مختلفی مطرح شده است که از آن جمله می‌توان موارد ذیل را برشمرد: Honeypot، Honeytoken و Honeyaccount و Honeyword.

با الهام از این مفهوم در سال ۲۰۱۴ نوع جدیدی از رمزنگاری به نام رمزنگاری شگرف یا Honey Encryption ارائه شد [۴۸]. ویژگی ممتاز این رمزنگاری این است که رمزگشایی متن رمزشده تحت *هر کلید غلط*، منجر به یک متن آشکار معنادار می‌شود که در ظاهر می‌تواند متن اصلی باشد (اما نیست).

کاربرد:

این ویژگی می‌تواند برای تأمین امنیت در الگوریتم‌های رمزی که مبتنی بر کلمه عبور هستند (PBE)[2] به‌کار برود. به‌طور مشخص در برخی سناریوها، حمله‌کننده کلید را حدس زده و متن رمزشده را رمزگشایی می‌کند. سپس بررسی می‌کند که آیا متن رمزگشایی‌شده منطبق بر یک الگوی از پیش‌فرض شده هست یا خیر؟ (مثلاً بامعنی بودن آن در زبان انگلیسی را چک می‌کند). درصورتی‌که متن رمزگشایی‌شده منطبق بر الگو بود (مثلاً معنی‌دار بود)، در این صورت کلید را صحیح و در غیر این صورت، کلید را غلط در نظر می‌گیرد. استفاده از HE سبب می‌شود که در این‌گونه موارد حمله‌کننده نتواند به‌طور مستقیم از روش مذکور استفاده کند. به‌طور خاص HE می‌تواند در محافظت از کلمات عبور کاربران در برخی دستگاه‌های احراز اصالت به‌کار رود [۴۹-۵۰].

[1] Decoy
[2] Password-based encryption (PBE)

۳-۱-۵- رمزنگاری مخرب

استفاده از رمزنگاری می‌تواند در راستای خلاف اهداف اولیه این علم صورت پذیرد. به‌عنوان مثال تعدادی از ویروس‌های کامپیوتری و یا حملات متداول به رایانه‌ها و شبکه‌ها، بر مبنای طرح‌های رمزنگاری صورت می‌پذیرد. ما در این بخش با ارائه مقدمه‌ای کوتاه، مفهوم کلپتوگرافی و دلیل مطرح‌شدن آن طی دو سال اخیر را بررسی می‌کنیم.

۳-۱-۵-۱- درب پشتی[3]

درب پشتی در یک سیستم رمزنگاری، به روشی اطلاق می‌شود که برای عبور از سیستم احراز اصالت توسط یک کاربر غیرمجاز استفاده می‌شود تا (از طریق یک ارتباط دور) بتواند به متن آشکار و یا اطلاعاتی مخفی دست پیدا کند. دسترسی کاربر غیرمجاز در این مفهوم باید به‌گونه‌ای باشد که تلاش مهاجم برای کسب این اطلاعات از دید کاربر و دیگران مخفی بماند. درب پشتی می‌تواند بخشی مخفی از یک قسمت از برنامه باشد یا برنامه‌ای مجزا باشد که بتواند سیستم را از طریق یک *روت کیت*[4] تحت کنترل قرار دهد. روت کیت‌ها اغلب در سطح سیستم‌عامل فعالیت کرده و با تغییراتی که در سیستم‌عامل یا منابع آن انجام می‌دهند، به مقاصد خود دست پیدا می‌کنند.

تعداد زیادی از کرم‌های رایانه‌ای[5] مانند Sobig و یا Mydoom یک درب، پشتی بر روی کامپیوتر هدف نصب می‌کنند (معمولاً کامپیوترهایی که ویندوز دارند) که حمله‌کننده را قادر می‌کند که از طریق رایانه آلوده‌شده ایمیل‌های اسپم ارسال کند.

۳-۱-۵-۲- کلپتوگرافی[6]

تعریف

مفهوم کلپتوگرافی به‌صورت رسمی و در یک چهارچوب علمی برای اولین بار توسط یوآنگ[7] و یونگ[8] در سال ۱۹۹۶ ارائه شد [۵۱]. ایده اصلی مطرح‌شده در مقاله ارائه روشی است که در مرحله پیاده‌سازی یک الگوریتم امن، می‌توان الگوریتم را به نحوی بازتعریف کرد که دارای درب پشتی باشد، به‌گونه‌ای که اولاً افراد استفاده‌کننده متوجه درب پشتی نشوند و ثانیاً اگر وجود آن کشف شد، افراد دیگر قادر به استفاده از درب پشتی نباشند. آن‌ها در این مقاله و کارهای بعدی خود مثال‌های متعددی در مورد رمزهای عموماً کلید عمومی ارائه کردند [۵۲].

[3] Back door
[4] Rootkit
[5] Computer worms
[6] Kleptography
[7] Adam Young
[8] Moti Yung

کاربرد

کاربرد عملی کلپتوگرافی زمانی است که آژانس‌های امنیتی بخواهند به‌صورت گسترده بر فعالیت‌های کاربران نظارت کنند بدون آنکه کاربران متوجه شوند. این مبحث در مجامع علمی کمتر موردتوجه بود تا اینکه در سال‌های اخیر و پس از افشاگری‌های ادوارد اسنودن[1] مشخص شد که سرویس امنیت ملی آمریکا (NSA)[2] از این طریق به‌منظور شنود گسترده اطلاعات استفاده کرده است. بر پایه یافته‌های اخیر علمی مولد شبه تصادفی Dual-EC که توسط مؤسسه ملی فناوری و استانداردهای آمریکا (NIST)[3] به آن استاندارد پردازش اطلاعات فدرال (FIPS)[4] اعطا شده بود، دارای درب پشتی است[5]. مطالعه دقیق نشان می‌دهد بدون شک، ضعف این مولد شبه تصادفی که به‌صورت عمدی (توسط آژانس ملی اطلاعات آمریکا) در این الگوریتم قرار گرفته در کاربردهای عملی قابل سوءاستفاده است [۱۹]. این مسئله سبب شد که در دو سال گذشته بار دیگر بحث کلپتوگرافی و روش‌های مقابله با آن به یکی از موضوعات موردتوجه جامعه رمزنگاری تبدیل شود. به‌طور ویژه اعضای مجمع جهانی رمزنگاری در جلسه‌ای در حاشیه کنفرانس EUROCRYPT2014 ضمن ابراز تأسف از آنچه توسط آژانس‌های امنیتی صورت گرفته، طی فراخوانی از محققین خواستند که روش‌های مقابله با این موضوع را در دستور کار خود قرار داده و نتایج آن را در کنفرانس‌های این مجمع ارائه کنند [۵۳].

۳-۱-۶- رمزنگاری جست‌وجوپذیر

امروزه انبوهی از اطلاعات حساس و خصوصی شهروندان، شرکت‌ها و مؤسسات از طریق دولت‌ها جمع‌آوری و در پایگاه‌های داده[6] ذخیره می‌شود. این اطلاعات که معمولاً به دلایل امنیتی و یا به خاطر دادن سرویس‌های بهتر به شهروندان جمع‌آوری و نگه‌داری می‌شوند، شامل داده‌های حساسی چون اطلاعات پزشکی شهروندان (EMR)[7]، اطلاعات مربوط به مکان‌ها، حافظه جست‌وجوهای اینترنتی، فایل‌های تصویری، تماس‌های تلفنی، ایمیل‌ها، فعالیت‌های افراد در شبکه‌های اجتماعی و غیره است [۵۴]. با بزرگ‌تر شدن پایگاه‌های داده، صاحبان این پایگاه‌های اطلاعاتی باید به اطلاعات دلخواه خود از طریق الگوریتم‌های پیشرفته جست‌وجو دسترسی داشته باشند. امروزه نمی‌توان تصور کرد که یک پایگاه اطلاعاتی بزرگ بدون یک موتور جست‌وجو در عمل کارا باشد.

نکته دیگری که در خصوص بزرگ‌تر شدن پایگاه‌های داده می‌توان اشاره کرد این است که بسیاری از شرکت‌های کوچک و بزرگ خصوصی با توجه به هزینه‌ها و مشکلات در ایجاد پایگاه داده اختصاصی، ترجیح می‌دهند که از سرویس‌های ابری[8] شرکت‌های خصوصی یا دولتی بزرگ‌تر استفاده کنند. استفاده از پایگاه‌های داده غیراختصاصی برای ذخیره کردن اطلاعات اختصاصی خود، بر پیچیدگی توأمان استفاده از داده‌ها در عین نیاز به امنیت مضاعف آن‌ها می‌افزاید.

داده‌ها باید به‌صورت رمزشده ذخیره و نگه‌داری شوند تا از سوءاستفاده‌های احتمالی جلوگیری شود. اما از طرفی دیگر معمولاً برای استفاده بهینه از این داده‌ها لازم است که داده‌های ذخیره‌شده قابل‌جست‌وجو باشند تا اطلاعات موردنیاز، به‌طور بهینه پیدا شده و مورد استفاده قرار گیرد. این امر مستلزم این است که داده به‌صورت عادی و غیررمزشده نگه‌داری شود. برای حل این تناقض در سالیان اخیر جامعه رمزنگاری به دنبال طراحی و ارائه اولیه‌های نوین رمزنگاری است به‌گونه‌ای که قابلیت پردازش‌های خاص بر روی داده‌های رمزشده وجود داشته باشد.

۳-۱-۶-۱- رمزنگاری هم‌ریختی[9] (HE)

رمزنگاری هم‌ریختی نوعی از رمزنگاری است که به‌وسیله آن می‌توان بر روی متن‌های رمزشده، برخی عملیات خاص ریاضی را انجام داد به‌گونه‌ای که اگر عملیات رمزگشایی بر روی متون رمزشده انجام شود، عملیات ریاضی انجام‌شده عیناً بر روی متن آشکار نیز انجام شده باشد. اگر رمزنگاری هر عملیات *دلخواه* را پشتیبانی کند، رمزنگاری هم‌ریختی کامل[10] (FHE) اطلاق می‌شود. برای مدت‌های زیادی مشخص نبود که آیا چنین طرحی وجود دارد یا خیر. گنتری[11] در سال ۲۰۰۹ برای اولین بار با استفاده از رمزنگاری مبتنی بر مشبکه[12] یک طرح رمزنگاری هم‌ریختی را ارائه کرد که عملیات جمع و ضرب را پشتیبانی می‌کرد [۵۵]. بر همین اساس طرح گنتری این امکان را داشت

[1] Edward Snowden
[2] National Security Agency
[3] National Institute of Standards and Technology
[4] Federal Information Processing Standards
[5] لازم به ذکر است که استاندارد FIPS بسیار معتبر بوده و توسط همه موسسات غیرنظامی و پیمانکاران دولتی مورد استفاده واقع می‌شود. این استاندارد همچنین توسط مؤسسه استانداردهای ملی آمریکا (ANSI)، موسسه مهندسان برق و الکترونیک (IEEE) و سازمان بین المللی استانداردسازی (ISO) به عنوان یک مرجع مورد استفاده قرار می‌گیرد.
[6] Datacenter
[7] Electronic medical records
[8] Cloud services
[9] Homomorphic encryption (HE)
[10] Fully-homomorphic encryption (FHE)
[11] Gentry
[12] Lattice-based cryptography

که هر عملیاتی را انجام دهد. در یوروکریپت ۲۰۱۰ دومین طرح FHE ارائه شد که در حقیقت بر مبنای طرح گنتری بود. این طرح به‌طور گسترده از مفاهیم و روش‌های طرح گنتری استفاده می‌کند اما این بار نویسندگان مقاله نشان دادند که فرض استفاده از یک مشبکه ایده‌آل با طرحی بسیار ساده‌تر که از اعداد طبیعی استفاده می‌کند، قابل‌جایگزینی است. پس از آن تلاش‌های بیشتری برای ارائه طرح‌های ساده‌تر و کاراتر FHE انجام شد که از این میان می‌توان به موارد ذیل اشاره کرد که امنیت آن‌ها مبتنی بر سختی مسئله Learning with errors می‌باشند:

- طرح BGV[1] [۵۶]
- طرح Brakerski [۵۷]
- طرح GSW[2] [۵۸]

در هر حال طرح‌های ارائه‌شده بسیار کند و غیر کارآمد می‌باشند. به‌عنوان مثال در یوروکریپت ۲۰۱۱ مقاله‌ای در خصوص پیاده‌سازی طرح گنتری ارائه شد که نشان می‌دهد هر عمل پایه بیتی برای طرح گنتری به حدود سی دقیقه وقت نیاز دارد [۵۹]! در طرح‌های فعلی این زمان به‌شدت کاهش پیدا کرده‌اند اما کماکان غیرکاربردی به نظر می‌رسند [۶۳-۶۰].

۳-۱-۶-۲- رمزنگاری متقارن جست‌وجو پذیر (SSE)[3]

همان‌طور که گفته شد موضوعاتی چون رمزنگاری هم‌ریختی[4] طی سال‌های اخیر توجه بسیاری از رمزنگاران را به خود جلب کرده و ده‌ها طرح با امنیت قابل اثبات ارائه شده است. اما هیچ‌کدام از این طرح‌ها قابلیت استفاده عملی را به‌دلیل نبود کارایی مناسب ندارند و عملاً این مباحث در حد مطالعات تئوریک باقی مانده‌اند. فلذا امروزه در عمل رمزنگاری قابل جست‌وجو که بر اساس کلیدواژه‌های از پیش تعریف‌شده هست، به‌عنوان راه‌کاری عملی مورد استفاده قرار می‌گیرند. طرح حفظ ویژگی[5] که در یوروکریپت ۲۰۱۲ ارائه شد [۶۴] و در [۶۵] مورد بازبینی قرار گرفت، دارای کارایی مناسب است و پرسمان در آن از وضوح خوبی برخوردار است. اما در این طرح در هر عمل بخش (بسیار ناچیزی) از اطلاعات نشت می‌کند. هرچند تاکنون حمله‌ای به این طرح نشده است اما ممکن است اطلاعات نشتی در آینده مورد استفاده قرار گیرند. طرح‌های رمزنگاری قطعی[6] [۶۸-۶۶] نیز در این دسته قرار می‌گیرند که البته در همه این طرح‌ها احتیاج به یک‌زمان خطی برای جست‌وجو دارند به این معنی که کل پایگاه داده باید برای هر پرسش و پاسخ یک‌بار به‌صورت کامل اسکن شود که این امر برای پایگاه‌های داده بزرگ مناسب نیست [۶۹]. همچنین روش رمزنگاری حفظ ترتیب[7] جزء روش‌های بنیادین با کارایی مناسب است که اخیراً به آن پرداخته شده است و در این دسته‌بندی می‌گنجد [۷۲-۷۰]. جست‌وجوی کلیدواژه‌ها با فن‌های بولینی[8] و پویا[9] کارایی بسیار مناسبی دارد (هرچند پرسمان پیچیده‌ای دارند) [۷۵-۷۳]. جست‌وجوی کلیدواژه از طریق این طرح‌ها (که اولین بار در کریپتو ۲۰۱۳ ارائه‌شده) بسیار کارا و سریع است و می‌تواند در زمان بهینه[10] انجام شود. به این معنی که زمان جست‌وجو تابعی خطی از تعداد اسناد[11] حاوی کلیدواژه‌ها هست. جست‌وجو بر اساس رمز ساختارمند[12] [۷۶] که Asiacrypt2010 ارائه شد بسیار کارا بوده و در عین‌حال اطلاعات کمی را نشت می‌دهند. مهم‌ترین محدودیت این طرح‌ها نبود یک پرسمان شفاف است که در طرح‌های جدید تلاش برای اصلاح طرح‌های گذشته صورت گرفته است [۷۸-۷۷].

۳-۱-۷- رمزنگاری مبتنی بر مشبکه[13]

با مطرح‌شدن ماشین‌های کوانتومی، جامعه رمزنگاری به دنبال یافتن راه‌حل‌هایی به‌منظور جایگزینی طرح‌های معمول همچون رمزنگاری مبتنی بر لگاریتم گسسته و یا تجزیه اعداد است. تعداد زیادی طرح تاکنون بدین منظور ارائه شده است و هرساله طرح‌های جدیدی نیز اضافه می‌شوند. به‌موازات این طراحی‌ها، حوزه تحلیل طرح‌های جدید نیز توجه زیادی به خود جلب کرده است. به مجموعه این تحقیقات علمی و طرح‌های ارائه‌شده *رمزنگاری پساکوآنتومی*[14] می‌گویند.

در بین طرح‌های ارائه‌شده، تنها طرح‌های رمزنگاری مبتنی بر مشبکه می‌باشند که هم‌زمان دارای کارایی مناسب بوده و در مقابل محاسبات کوانتومی امن هستند. طی سالیان اخیر تعداد زیادی اولیه‌های رمزنگاری مبتنی بر مشبکه ارائه‌شده است. عموماً مهم‌ترین ابزار برای فهم امنیت این اولیه‌ها، الگوریتم *نمونه‌برداری گوسی*[15] است که برای هر مشبکه دلخواه کار می‌کند. درحالی‌که این روش برای ساخت دسته زیادی از طرح‌های مبتنی بر مشبکه مفید است، اما به لحاظ کارایی، عملیاتی و مناسب نیست. یک راه‌حل ممکن برای غلبه بر این مشکل، در نظر گرفتن برخی

[1] Brakerski-Gentry-Vaikuntanathan
[2] Gentry-Sahai-Waters
[3] Symmetric Searchable Encryption (SSE)
[4] Homomorphic encryption
[5] Property-preserving encryption
[6] Deterministic encryption
[7] Order preserving encryption
[8] Boolean keyword search
[9] Dynamic
[10] Optimal
[11] Document
[12] Structured encryption
[13] Lattice based cryptography
[14] Post quantum cryptography
[15] Gaussian sampling algorithm

پیش‌فرض‌های قوی‌تر برای مشبکه‌های به‌کاررفته است. طبیعی است که این‌گونه راه‌حل‌ها ممکن است که سبب ایجاد ضعف‌های جدی امنیتی شوند. اما تجربه نشان داده است که یافتن فرضیات مناسب، می‌تواند منجر به طراحی‌های امن و درعین‌حال کارا همچون NTRU شود. راه دیگری که هم‌اکنون محققان بر روی آن متمرکز هستند، ترکیب روش‌های است که اخیراً به‌صورت موفق به‌منظور ساخت طرح‌های امضای دیجیتال ساده‌تر به‌کار گرفته‌شده‌اند. درهرصورت تجزیه‌وتحلیل هرکدام از این روش‌ها، موضوعی نوین است که احتیاج به تحقیقات بیشتری دارد. لازم به ذکر است که محققین اروپائی دو پروژه مهم اروپائی SAFEcrypto و PQCrypto در این حوزه به‌صورت فعال مشغول به تحقیق می‌باشند.

۳-۲- پروتکل‌ها

پروتکل‌های رمزنگاری در لایه‌های کاربردی دستگاه‌های امنیتی به‌کار گرفته می‌شوند. بر همین اساس، تعداد زیادی پروتکل رمزنگاری طراحی‌شده و در عمل به‌کار می‌روند. در این بخش، ما موضوعات مهم و نوین در حوزه پروتکل‌های رمزنگاری را معرفی خواهیم کرد.

۳-۲-۱- پروتکل‌های عملی جدید

۳-۲-۱-۱- پروتکل‌های MPC

یک طرح MPC به مجموعه‌ای از افراد اجازه می‌دهد که بدون آن‌که داده‌های خود را برای یکدیگر آشکار کنند، تابعی از داده‌های خود را محاسبه کنند به‌نحوی‌که اولاً مقادیر اصلی آن‌ها کماکان مخفی بماند و در ثانی مطمئن باشند که تابع به‌درستی محاسبه‌شده است. از زمان ارائه اولین طرح MPC (دهه ۸۰ میلادی)، به خاطر پیچیدگی زیاد پروتکل‌ها ارائه‌شده، این موضوع صرفاً به دید تئوریک و نظری دیده می‌شد و نه موضوعی عملی و کاربردی. تا آنکه در سال ۲۰۰۴ اولین پیاده‌سازی یک پروتکل جدید MPC منتشر شد [۷۹]. پس از آن به این دسته از پروتکل‌ها بیشتر پرداخته شد و پروتکل‌های جدیدی معرفی شدند که به‌مراتب کارایی بهتری نسبت به طرح‌های گذشته دارند [۸۰]. البته کماکان پروتکل‌های ارائه‌شده فاصله قابل‌توجهی تا رسیدن به یک کارایی مناسب دارند به‌گونه‌ای که حقیقتاً بتوان از آن‌ها در کاربردهای واقعی بهره برد. پروتکلی موجود دودسته می‌باشند: دسته اول پروتکل‌هایی هستند که بتوانند هر تابعی را محاسبه کنند و دسته دوم پروتکل‌هایی هستند که تنها می‌توانند دسته‌ای خاص از توابع را محاسبه کنند.

سؤالات باز این حوزه شامل مباحثی از قبیل موارد ذیل است:

جنبه‌های ریاضی و الگوریتمی تسهیم راز و تأثیر آن بر روی MPC، میزان عملیاتی بودن پروتکل‌های MPC که در آن‌ها مقادیر مخفی هرکدام از شرکت‌کنندگان محدودیت‌های خاصی دارد (به لحاظ اندازه)، دسته‌بندی‌های امنیتی در مقابل حملات موجود در مقابل این پروتکل‌ها.

۳-۲-۲- Multilinear map

معرفی و به‌کارگیری bilinear map تا در رمزنگاری طی یک دهه اخیر، منجر به ارائه طرح‌های بسیار مناسب و کارایی با کاربردهای متنوع و مهم شده است. تحقیقات منتشرشده‌ی اخیر نشان می‌دهد که چگونه می‌توان به‌صورت مؤثر از multilinear map تا در رمزنگاری استفاده کرد. این رویکرد جدید منجر به طرح کاربردهای بسیار متنوع و زیاد در رمزنگاری‌شده است (مانند رمزنگاری مبتنی بر شناسه[1]، اعتبارنامه ناشناس[2]). در حقت این رویکرد اجازه می‌دهد با معرفی برخی فرض‌های محاسباتی، طرح‌های گذشته را به‌گونه‌ای اصلاح کرد که هم به لحاظ کارایی و هم به لحاظ امنیت، مناسب‌تر باشند.

۳-۲-۳- صحت محاسبات ابری

امروزه استفاده از قابلیت‌هایی که ابرها دارند، روزبه‌روز در حال گسترش است. از ابرها برای دو هدف اساسی استفاده می‌شود. کارکرد اول ابرها، ذخیره و نگه‌داری اطلاعات افراد است. بر همین اساس لازم است اطلاعاتی که در ابرها اخیر می‌شوند، دارای امنیت قابل‌اعتمادی باشند به‌گونه‌ای که حتی صاحبان ابر نیز از آن‌ها باخبر نباشند. معمولاً انتظار کاربران این است که اطلاعات آن‌ها مخفی باقی بماند. این بخش به بحث رمزنگاری جست‌وجوپذیر باز می‌گردد که پیش از این معرفی شد. کارکرد دوم استفاده از ابرها به‌منظور انجام محاسبات پیچیده و سنگین است. در این راستا لازم است که سازوکارهایی تعبیه شود که کاربران مطمئن باشند که محاسبات به‌صورت صحیح و همان‌گونه که برای ابر تعریف کرده‌اند، قابل انجام است. یک موضوع کلی و مهم در این حوزه که اخیر مطرح‌شده است، تحلیل و طراحی پروتکل‌های است که قابلیت تصدیق محاسبات رادارند[3]. لازم به ذکر است که عموماً این پروتکل‌ها در مرحله تحقیقات اولیه هستند و عموماً تا عملیاتی شدن برای کاربردهای عملی فاصله زیادی در پیش دارند.

۳-۲-۴- اثبات (عدم) امنیت پروتکل‌های کاربردی

مهم‌ترین کاربردهای رمزنگاری ایجاد محرمانگی و همچنین احراز

[1] Identity based encryption
[2] Anonymous credential
[3] Verifiable computation protocols

اصالت اطلاعات است که در عمل از طریق پروتکل‌های متعدد برای کاربران فراهم می‌شوند. مهم‌ترین پروتکل‌های کاربردی عبارت‌اند از: TLS (که در https به‌کار می‌رود)، IPsec (در شبکه خصوصی مجازی)، EMV (در کارت‌ها اعتباری و بانکی) و Kerberos (به‌صورت گسترده در سرویس‌های احراز اصالت شبکه به‌کار می‌روند). درحالی‌که استانداردهای مشخصی برای استفاده از این پروتکل‌ها توسط مجامع بین‌المللی ارائه شده است، اما حقیقت امر این است که امنیت آن‌ها به‌طور کامل توسط جامعه رمزنگاری قابل فهم نیست. به‌عنوان‌مثال می‌توان به تحقیقات اخیری که در خصوص پروتکل TLS انجام و منتشر شد، اشاره کرد که به مطالعه برخی سازو کارهای عملی همچون دنباله زدن[1]، پیام‌های تصدیق کلید[2]، توابع به‌دست آوردن کلید[3] و برخی طرح‌های کلید عمومی. کماکان در این حوزه سؤالات متعددی وجود دارد؛ همانند اینکه پیام‌های تصدیق کلید چه مقدار بر امنیت روش می‌افزایند؟ چه مفروضاتی برای توابع استنتاج کلید لازم است؟ چه مفروضاتی برای انتقال کلید از طریق یک سیستم کلید عمومی لازم است؟

به‌عنوان مثالی دیگر می‌توان به پروتکل بسیار مشهور و کاربردی PKCS#1 v1.5 اشاره کرد که در آن‌گونه‌ای از رمز کلید عمومی مشهور RSA به‌کار رفته است. همان‌گونه که می‌دانیم RSA به شکل‌های گوناگون می‌تواند به‌کار رود که بعضاً برخی از آن‌ها ناامن هستند. گونه‌ای از RSA که در PKCS#1 v1.5 به‌کار رفته است، هیچ‌گونه اثبات امنیتی ندارد! هرچند که این‌گونه از پروتکل‌ها تاکنون مورد حمله قرار نگرفته‌اند (منظور حملاتی است که منتشر شده باشند)، اما نشان‌دهنده فاصله عمیق و همچنین بسیار مهم بین تئوری و عمل است.

در هر حال رصد تلاش‌هایی که به‌منظور فهم پروتکل‌های کاربردی انجام گرفته است و بررسی روند تحلیل و همچنین طراحی این پروتکل‌ها، از موضوعات مهمی است که می‌تواند مورد توجه جامعه رمزنگاری در کشور باشد.

۳-۲-۵- راستی آزمائی رمزنگاری[4]

طرح‌های رمزنگاری (همانند طرح‌های امضای دیجیتال و یا الگوریتم‌های رمزکننده) و یا پروتکل‌های رمزنگاری عموماً از اجزای پیچیده‌ای تشکیل می‌شوند و بر همین اساس طبیعی است که اثبات‌های امنیتی آن‌ها نیز پیچیده باشند. این پیچیدگی می‌تواند منجر به وجود برخی اشتباهات در اثبات‌های امنیتی خاصی شود که توسط اشخاص و به‌صورت دستی ارائه می‌شوند. با افزایش پیچیدگی طرح‌ها و پروتکل‌ها و درنتیجه افزایش طبیعی پیچیدگی اثبات‌های امنیتی ارائه‌شده توسط اشخاص، این دغدغه ایجاد شده است که چگونه می‌توان به این‌گونه از اثبات‌ها اعتماد کرد؟ در پاسخ به این نگرانی حوزه جدیدی از تحقیقات رمزنگاری ایجاد شده است که هدف آن، تعریف ابزارهای خودکار و رایانه محور است که بر اساس آن‌ها بتوان اثبات‌های امنیتی را تائید کرد. یکی از ابزارهای معروف در این حوزه ابزار easycrypt است که در [۸۱] قابل دسترس است. برای دست‌یابی به ابزاری مناسب، محققان دو حوزه اثبات امنیتی و همچنین حوزه روش‌های فرمال با همکاری یکدیگر باید فعالیت کنند.

هدف اصلی این ابزارها افزایش اعتماد به امنیت طرح‌ها و پروتکل‌های رمزنگاری از طریق به‌کارگیری تصدیق‌هایی است که با کمک کامپیوتر و اصطلاحاً در *مدل محاسباتی* انجام می‌شوند. بر همین اساس این ابزارها به ما اجازه می‌دهند که ویژگی‌های امنیتی محاسباتی را از طریق برنامه‌های کامپیوتری کوتاه فرمالیزه کرده و مشخص کنیم که چگونه یک حمله‌کننده می‌تواند با سیستم طراحی‌شده، پرس و پاسخ داشته باشد. در حقیقت این برنامه‌های کامپیوتری ترجمه‌ای مستقیم از *بازی‌های* امنیتی است که پیش از این توسط رمزنگاران استفاده می‌شدند. در حال حاضر تحقیقات وسیعی در این حوزه درحالی‌که انجام است که متمرکز بر دو موضوع اصلی است: ۱- تلاش برای پوشش طیف بیشتری از روش‌های اثبات امنیتی ۲- اصلاح کارایی عملی این ابزارها به گونه که بتوانند به‌صورت گسترده موردپذیرش قرار گیرند.

۳-۲-۶- ارتباط گمنام

با گسترش شبکه‌های ارتباطاتی و به‌خصوص اینترنت، یکی از مهم‌ترین ویژگی‌هایی که نیاز به آن در حین ارتباط امن در شبکه‌ها احساس شد، حفظ گمنامی[5] است که ایده ایجاد آن اولین بار توسط چام[6] مطرح شد. در صورت عدم گمنامی، هرچند ممکن است که محرمانگی و احراز اصالت داده‌ها حفظ شود، اما مهاجم می‌تواند طرفین ارتباط را بشناسد. به‌عنوان مثال در هنگام استفاده یک کاربر از اینترنت، مهاجم می‌تواند تشخیص دهد که شخص هدف خود، از چه سرویسی در اینترنت استفاده می‌کند و یا به چه سروری در آن متصل است. در تعریف حریم خصوصی افراد و ایجاد یک ارتباط امن، نشت این اطلاعات به مهاجم قابل‌قبول نیست و بنابراین، استفاده از روشی برای ایجاد یک ارتباط گمنام لازم به نظر می‌رسد.

با توجه به نکات گفته‌شده واضح است که در بسیاری از

[1] Padding
[2] Key confirmation messages
[3] Key derivation functions
[4] Verification of cryptography

[5] Anonymity
[6] Chaum

ارتباطات، گمنامی یک ویژگی امنیتی مهم تلقی می‌شود که ایجاد آن برای امنیت ارتباط لازم است. اما باید توجه کرد که در برخی موارد، هدف می‌تواند عکس گمنامی باشد. به این معنی که جلوی ارتباط گمنام گرفته شود یا گمنامی یک ارتباط شکسته شود. برای روشن‌تر شدن این موضوع نیز از چند مثال استفاده می‌کنیم. فرض کنید در یک شرکت امنیتی، یک جاسوس شناسایی شده است و این جاسوس به‌صورت گمنام اطلاعات را برای یک سرور نامشخص در اینترنت ارسال می‌کند. بنابراین، شناسایی طرف ارتباط با جاسوس قبل از دستگیری وی بسیار حائز اهمیت است، چراکه می‌تواند منجر به شناسایی تمام سازمان دشمن شود. در این شرایط شکستن ارتباط گمنام ایجادشده توسط جاسوس و سرور هدف مدنظر است.

همان‌طور که از مثال‌های فوق مشخص است، در مواردی که حریم خصوصی و امنیت لینک ارتباطی مدنظر است، ایجاد گمنامی یک ویژگی خوب هست. اما در مواردی که سوءاستفاده از گمنامی برای اهداف سودجویانه یا سیاسی مدنظر باشد، شکستن گمنامی هدف خواهد بود. بنابراین، هر دو هدف ایجاد یا شکستن گمنامی دارای ارزش تحقیقاتی و عملی است و مسیر تحقیقات بسیاری از دانشمندان در آن دو قرارگرفته است.

مواردی که لازم است که بررسی شود بدین شرح می‌باشند: بررسی اهمیت گمنامی، بررسی و شناسایی ارتباطاتی که برای امنیت بیشتر باید گمنام‌سازی شوند، بررسی و شناسایی ارتباطاتی که برای امنیت بیشتر، باید گمنامی آن‌ها شکسته شود، بررسی و مطالعه انواع شبکه‌های گمنام‌سازی.

۳-۲-۷- اینترنت اشیاء

اینترنت اشیاء، کارکرد همه دستگاه‌های هوشمند در کنار هم است که هدف آن‌ها، آسایش، راحتی و بهبود کیفیت زندگی است. اثرات این فناوری، بسیار گسترده است و می‌تواند به همان اندازه که مزایا دارد، معایب نیز به همراه داشته باشد. اگرچه با ظهور این فن‌آوری، فرصت‌های تجاری متعددی ایجاد خواهد شد و زمان ارائه ایده‌های جدید و نوآوری‌ها خواهد رسید، اما بدون تأمین امنیت مناسب، اثرات مخرب آن گریبان‌گیر جامعه خواهد شد. در ادامه این متن به چالش‌های این فناوری و امنیت آن پرداخته می‌شود و مسیرهای تحقیقاتی لازم در جهت امنیت اینترنت اشیاء مطرح می‌شوند.

چالش‌های اصلی اینترنت اشیاء عبارت‌اند از: ۱- نبود یک معماری سازگار برای تمامی ارتباطات و اتصالات آن ۲- عدم سازوکار امنیتی مناسب.

ارتباطات در اینترنت اشیاء، میان حسگرهای ساده‌ای مثل حسگر دما و رطوبت با یک پردازنده مرکزی مثل موبایل یا خانه انجام می‌شود. درنتیجه ایجاد امنیت در این ارتباطات، می‌تواند یک چالش جدی باشد. همچنین به‌دلیل سادگی ادوات و سخت‌افزارها، رویکرد در اینترنت اشیاء به سمت پروتکل‌هایی است که در یک‌طرف به پردازش بسیار پایین احتیاج داشته باشند و بار پردازشی روی طرف دیگر باشد. این پروتکل‌ها ضمن برقراری ارتباط، باید امنیت را نیز تضمین دهند. همچنین یکی از چالش‌های اساسی دیگر در اینترنت اشیاء حفظ حریم خصوصی افراد است که به‌دلیل وارد شدن انواع حسگرهای الکترونیکی به زندگی انسان‌ها اهمیت پیدا می‌کند. به هر حال، در ادامه به‌صورت سرفصل نیازهای تحقیقاتی این حوزه را بیان می‌کنیم که همگی به‌نوعی سایر چالش‌های اینترنت اشیاء را مشخص می‌سازند:

- پروتکل‌های امن ارتباطی که بار پردازشی در یک سمت ارتباط قرار می‌گیرد
- فناوری‌های حفظ حریم خصوصی افراد
- فناوری‌های ایجاد اعتماد قبل از انتقال اطلاعات

البته لازم به ذکر است که پروتکل‌های امنیت اینترنت اشیاء از برخی موضوعاتی که درگذشته نیز مطرح کردیم همچون اولیه‌های سبک بهره می‌برند.

۴- تقسیم‌بندی موضوعات معرفی‌شده

علی‌رغم آنکه ما تنها مباحث خاصی از رمزنگاری را بر اساس معیارهای مشخص انتخاب کردیم، اما کماکان موضوعات مطرح‌شده در بخش ۳ و جهت‌گیری‌های ارائه‌شده برای هر موضوع، طیف وسیعی از مباحث ویژه رمزنگاری را پوشش می‌دهند. برای داشتن نمائی روشن‌تر، ما در این بخش ابتدا یک دسته‌بندی بر اساس میزان عملی بودن هرکدام از موضوعات ارائه می‌کنیم. سپس تمامی موضوعات ارائه‌شده در بخش ۳ را در قالب این دسته‌بندی به چهار گروه تقسیم می‌کنیم. تقسیم‌بندی موردنظر به شکل زیر است:

گروه الف: موضوعاتی که هم‌اکنون در عالم واقع به‌کار می‌روند و عملیاتی هستند. تعریف پروژه‌های مناسب در این موضوعات، پتانسیل آن را دارد که منجر به محصولی عملی شود.

گروه ب: موضوعاتی که هرچند هم‌اکنون کاربردی هستند، اما جزء مباحث پایه و نظری رمزنگاری هستند. این موضوعات لازمه انجام برخی پروژه‌های عملی می‌باشند.

گروه پ: موضوعاتی که هم‌اکنون به‌طور گسترده در عالم

واقع استفاده نمی‌شوند، اما با در نظر گرفتن روند پیشرفت‌های موجود و نیاز مبرم به آن‌ها، پیش‌بینی می‌شود که در آینده نزدیک به مبحثی کاربردی تبدیل شوند.

گروه ت: موضوعاتی که هم‌اکنون کاربردی نیستند و علی‌رغم آن‌که به آن‌ها نیاز واقعی وجود دارد، روند پیشرفت‌ها به‌گونه‌ای نیست که بتوان با قطعیت از زمان به‌کارگیری آن‌ها تخمینی ارائه کرد (هرچند احتمال رسیدن به نتیجه‌ای عملی امکان‌پذیر است).

۴-۱- اولیه‌ها

موضوعات ارائه‌شده در بخش ۳-۱ که مختص اولیه‌ها می‌باشند به شکل زیر تقسیم‌بندی می‌شوند:

گروه الف: پیاده‌سازی حملات عملی بر روی اولیه‌های متقارن که هنوز کاربرد دارند، رمزنگاری با فرمت‌های خاص.

گروه ب: طراحی اولیه‌های امن با در نظر گرفتن حملات کانال جانبی، رمزنگاری احراز اصالت، طراحی رمزهای قالبی سبک با مشخصاتی که کمتر مورد توجه قرار گرفته‌اند (نظیر انرژی بهینه و یا تأخیر حداقلی)، کلپتوگرافی و روش‌های مقابله با آن، رمزنگاری جست‌وجو پذیر متقارن.

گروه پ: رمزنگاری هم‌ریختی کامل FHE، رمزنگاری مبتنی بر مشبکه.

گروه ت: تحلیل‌های جدید رمزنگاری متقارن و روابط آن‌ها با یکدیگر، مباحث ذیل مجموعه رمزنگاری متقارن معمول (شامل جدول کلید، رمزهای قالبی Tweakable و تحلیل‌های جدید).

۴-۲- پروتکل‌ها

موضوعات ارائه‌شده در بخش ۳-۲ که مختص پروتکل‌ها می‌باشند، به شکل زیر تقسیم‌بندی می‌شوند:

گروه الف: حمله به پروتکل‌های کاربردی، شبکه‌های گمنام، پول رمزی.

گروه ب: رأی‌گیری الکترونیک، موضوعات ارائه‌شده ذیل بحث اینترنت اشیاء (حریم خصوصی، پردازش سمت ابر و ایجاد اعتماد پیش از انتقال اطلاعات).

گروه پ: پروتکل‌های MPC.

گروه ت: صحت محاسبات ابری، پروتکل‌های مبتنی بر Multilinear map، اثبات امنیت پروتکل‌های کاربردی، راستی آزمائی رمزنگاری.

۵- نتیجه‌گیری

همان‌گونه که پیش از این ذکر شد، هدف اصلی از ارائه این مقاله، بررسی برخی جهت‌گیری‌های اساسی موجود در رمزنگاری نوین است. بر همین اساس، ابتدا ضرورت‌های شناخت و بررسی مباحث نوین رمزنگاری را بررسی کردیم. سپس برخی از مهم‌ترین تحولات صورت گرفته در حوزه رمزنگاری طی سالیان اخیر را معرفی کرده و بر اساس آن‌ها، به بررسی اجمالی برخی از موضوعات و مفاهیم نوین ارائه‌شده پرداختیم. بر همین اساس و با یادآوری این مطلب که هدف از انجام این مقاله، تولید علم و یا بررسی جزئیات فنی موضوعات مطرح‌شده نیست، تلاش کردیم موضوعات معرفی‌شده را بر اساس میزان عملیاتی بودن آن‌ها دسته‌بندی کنیم. بدیهی است که نگارنده با توجه به دانش و تجربه محدود خود اقدام به معرفی موضوعات کرده است و به‌هیچ‌وجه ادعا نمی‌شود که این مقاله تمامی مباحث نوین رمزنگاری را پوشش می‌دهد. قطعاً طرح و بررسی دقیق‌تر مباحث نوین رمزنگاری، نیازمند همفکری تمامی صاحب‌نظران کشور در این زمینه مهم علمی هست.

تقدیر و تشکر

نگارنده از آقای سیاوش احمدی به خاطر همکاری ایشان در طرح و نگارش مباحث مربوط به «گمنامی» و «اینترنت اشیاء» تشکر می‌کند. این مقاله با استفاده از پژوهانه دانشگاه شهید بهشتی نوشته شده است.

۶- مراجع

1. A. Yao, “protocols for secure computations,” in SFCS '82 Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, 1982.
2. J. B. Nielsen, “Secure Multiparty Computation Basic Technology + Past, Present, Future,” 2015.
3. J. A. Garay, Y. Ishai, R. Ostrovsky, and V. Zikas, “The Price of Low Communication in Secure Multi-party Computation,” In CRYPTO 2017, 2017.
4. A. Kiayias, H. S. Zhou and V. Zikas, “Fair and Robust Multi-party Computation Using a Global Transaction Ledger,” In EUROCRYPT 2016, 2016.
5. S. Coretti, J. Garay, M. Hirt, and V. Zikas, “Constant-Round Asynchronous Multi-Party Computation Based on One-Way Functions,” In ASIACRYPT, 2016.
6. Y. Lindell, N. Smart, and E. S. Vazquez, “More Efficient Constant-Round Multi-party Computation from BMR and SHE,” In TCC, 2016.

7. V. Grosso, G. Leurent, F. X. Standaert, and K. Varici, "LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations," In Fast Software Encryption (FSE 2014), 2014.

8. B. Gerard, V. Grosso, M. N. Plasencia, and F. X. Standaert, "Block Ciphers That Are Easier to Mask: How Far Can We Go?," In Cryptographic Hardware and Embedded Systems (CHES 2013), 2013.

9. A. Biryukov, A. Shamir, and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," In Fast Software Encryption, 7th International Workshop (FSE 2000), 2000.

10. M. Fillinger and M. Stevens, "Reverse-Engineering of the Cryptanalytic Attack Used in the Flame Super-Malware," In Advances in Cryptology- ASIACRYPT 2015, 2015.

11. M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The First Collision for Full SHA-1," in CRYPTO, 2017.

12. M. Stevens and D. Shumow, "Speeding up detection of SHA-1 collision attacks using unavoidable attack conditions," In USENIX Security Symposium 2017, 2017.

13. M. Stevens , P. Karpman, and T. Peyrin, "Freestart Collision for Full SHA-1," In EUROCRYPT 2016, 2016.

14. P. Sepehrdad, S. Vaudenay, and M. Vuagnoux, "Statistical Attack on RC4 - Distinguishing WPA," In Advances in Cryptology - EUROCRYPT 2011, 2011.

15. P. Sepehrdad, P. Susil, S. Vaudenay, and M. Vuagnoux, "Tornado Attack on RC4 with Applications to WEP and WPA," IACR Cryptology ePrint Archive, 2015.

16. A. Jana and G. Paul, "Revisiting RC4 key collision: Faster search algorithm and new 22-byte colliding key pairs," Cryptography and Communications, vol. 10, no. 3, pp. 479-508, 2018.

17. R. Bricout, S. Murphy, K. Paterson, and T. V. D. Merwe, "Analysing and exploiting the Mantin biases in RC4," Des. Codes Cryptography, vol. 86, no. 4, pp. 743-770, 2018.

18. S. Sarkar and A. Venkateswarlu, "Revisiting (nested) Roos bias in RC4 key scheduling algorithm," Des. Codes Cryptography, vol. 83, pp. 131-148, 2018.

19. S. Checkoway, R. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D. J. Bernstein, J. Maskiewicz, H. Shacham, and M. Fredrikson, "On the Practical Exploitability of Dual EC in TLS Implementations," In Proceedings of the 23rd USENIX Security Symposium, 2014.

20. "Tor Project: Anonymity Online," [Online]. Available: https://www.torproject.org.

21. F.-X. Standaert, O. Pereira, and Y. Yu, "Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions," In CRYPTO 2013, 2013.

22. M. Medwed, F.-X. Standaert, J. Großschädl, and F. Regazzoni, "Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices," In AFRICACRYPT 2010, 2010.

23. K. Pietrzak, "A Leakage-Resilient Mode of Operation," In EUROCRYPT 2009, 2009.

24. J. Jean, I. Nikolic and T. Peyrin, "Tweaks and Keys for Block Ciphers: The TWEAKEY Framework," in ASIACRYPT 2014, 2014.

25. J. Jean, I. Nikolić and T. Peyrin, "Deoxys," http://competitions.cr.yp.to/caesar-submissions.html, 2014.

26. V. Grosso, G. Leurent, F.-X. Standaert, K. Varici, F. Durvaux, L. Gaspar, and S. Kerckhof, "SCREAM and iSCREAM Side Channel Resistant Authenticated Encryption with Masking," http://competitions.cr.yp.to/caesar-submissions.html, 2014.

27. J. Jean, I. Nikolić, and T. Peyrin, "Joltik," http://competitions.cr.yp.to/caesar-submissions.html, 2014.

28. J. Jean, I. Nikolić, and T. Peyrin, "KIASU," http://competitions.cr.yp.to/caesar-submissions.html, 2014.

29. D. Penazzi and M. Montesg, "Silver," http://competitions.cr.yp.to/caesar-submissions.html, 2014.

30. A. Bogdanov and V. Rijmen, "Zero-correlation Linear Cryptanalysis of Block Ciphers," Des. Codes Cryptogr, vol. 70, no. 3, p. 369–383, 2014.

31. C. Blondeau, A. Bogdanov, and M. Wang, "On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel and Skipjack-Type Ciphers," In Applied Cryptography and Network Security 12th International Conference, ACNS 2014, 2014.

32. C. Blondeau and K. Nyberg, "Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities," In Advances in Cryptology EUROCRYPT 2014, 2014.

33. B. Sun, Z. Liu, V. Rijmen, R. Li, L. Cheng, Q. Wang, H. AlKhzaimi, and C. Li, "Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis," In Advances in Cryptology - CRYPTO 2015, 2015.

34. N. AlFardan, D. Bernstein, K. Paterson, B. Poettering, and J. Schuldt, "On the Security of RC4 in TLS," Royal Holloway University of London, March 2013.

35. "CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness," competitions.cr.yp.to/caesar.html.

36. A. Canteaut and G. Leurent, "Distinguishing and Key-recovery Attacks against Wheesht," https://www.rocq.inria.fr/secret/Anne.Canteaut/Publications/wheesht.pdf, 2014.

37. I. Dinur and J. Jean, "Cryptanalysis of FIDES," In FSE 2014, 2014.

38. Y. Sasaki and L. Wang, "A Forgery Attack against PANDA-s," Cryptology ePrint Archive: Report 2014/217, 2014.

39. Y. Sasaki and L. Wang, "A Practical Universal Forgery Attack against PAES-8," Cryptology ePrint Archive: Report 2014/218, 2014.

40. S. Wu, H. Wu, T. Huang, M. Wang and W. Wu, “Leaked-State-Forgery Attack Against The Authenticated Encryption Algorithm ALE,” In ASIACRYPT 2013 , 2013.

41. G. Leander, C. Paar, A. Poschmann and K. Schramm, “New Lightweight DES Variants,” In Fast Software Encryption, 14th International Workshop, FSE 2007, 2007.

42. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, and Y. Seurin, “PRESENT: An Ultra-Lightweight Block Cipher,” In Cryptographic Hardware and Embedded Systems CHES 2007, 2007.

43. M. Bellare and P. Rogaway, “Terence Spies: The FFX Mode of Operation for Format-Preserving Encryption,” http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec.pdf, 2010.

44. E. Brier, T. Peyrin, and J. Stern, “BPS a Format-Preserving Encryption Proposal by Peyrin,” NIST, 2010.

45. B. Morris, V. Hoang, and P. Rogaway, “An Enciphering Scheme Based on a Card Shuffle,” In CRYPTO, 2012.

46. K. P. Dyer, S. E. Coull, T. Ristenpart, and T. Shrimpton, “Protocol misidentification made easy with format-transforming encryption,” 2013.

47. “https://fteproxy.org,” [Online].

48. A. Juels and T. Ristenpart, “Honey Encryption: Security Beyond the Brute-Force Bound,” In EUROCRYPT, 2014.

49. W. Yin, J. Indulska, and H. Zhou, “Protecting Private Data by Honey Encryption,” Security and Communication Networks, 2017.

50. H. Choi, H. Nam, and J. Hur, “Password typos resilience in honey encryption,” In ICOIN 2017, 2017.

51. M. Yung, “The Dark Side of,” Black-Box Cryptography, or: Should We Trust Capstone?,” In CRYPTO, 1996.

52. Q. Tang and M. Yung, “Cliptography: Post-Snowden Cryptography,” In CCS 2017, 2017.

53. “IACR,” [Online]. Available: https://www.iacr.org/misc/statement-May2014.html.

54. S. Kamara, “Encrypted Search,” Microsoft Research, 2015.

55. C. Gentry, “Fully homomorphic encryption using ideal lattices,” In Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, 2009.

56. Z. Brakerski, C. Gentry, and V. Vaikuntanathan, “Fully Homomorphic Encryption without Bootstrapping,” In Innovations in Theoretical Computer Science, 2012.

57. Z. Brakerski, “Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP,” In CRYPTO, 2012.

58. C. Gentry, A. Sahai, and B. Waters, “Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based,” In CRYPTO, 2013.

59. C. Gentry and S. Halevi, “Implementing Gentry's Fully-Homomorphic Encryption Scheme,” In EUROCRYPT, 2011.

60. S. Halevi and V. Shoup, “Bootstrapping for HElib,” in EUROCRYPT, 2015.

61. Y. Doroz , J. Hoffstein, J. Pipher, J. Silverman, B. Sunar, W. Whyte, and Z. Zhang, “Fully Homomorphic Encryption from the Finite Field Isomorphism Problem,” In PKC 2018, 2018.

62. B. Wang, Y. Zhan, and Z. Zhang, “Cryptanalysis of a Symmetric Fully Homomorphic Encryption Scheme,” EEE Trans. Information Forensics and Security, vol. 13, no. 6, pp. 1460-1467, 2018.

63. K. Gai, M. Qiu , Y. Li, and Y. X. Liu, “Advanced Fully Homomorphic Encryption Scheme Over Real Numbers,” In CSCloud 2017, 2017.

64. O. Pandey and Y. Rouselakis, “Property Preserving Symmetric Encryption,” In EUROCRYPT, 2012.

65. S. Chatterjee and M. P. L. Das, “Property Preserving Symmetric Encryption: Revisited,” IACR Cryptology ePrint Archive, 2013.

66. Y. C. Chang and M. Mitzenmacher, “Privacy Preserving Keyword Searches on Remote Encrypted Data,” In ACNS, 2005.

67. E.-J. Goh, “Secure Indexes,” IACR Cryptology ePrint Archive, 2004.

68. D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” In IEEE Symposium on Security and Privacy, 2000.

69. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” In CCS, 2006.

70. R. Agrawa, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” In SIGMOD, 2004.

71. A. Boldyreva, N. Chenette, and A. O'Neill, “Order-preserving encryption revisited: Improved security analysis and alternative solutions,” In CRYPTO, 2011.

72. A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, “Order-preserving symmetric encryption,” In EUROCRYPT, 2009.

73. D. Cash, S. Jarecki, C. S. Jutla, H. Krawczyk, M. C. Rosu, and M. Steiner, “Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries,” In CRYPTO, 2013.

74. D. Cash, J. Jaeger, S. Jarecki, C. S. Jutla, H. Krawczyk, M. C. Rosu, and M. Steiner, “Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation,” In NDSS, 2014.

75. S. Kamara and T. Moataz, “Boolean Searchable Symmetric Encryption with Worst-Case Sub-linear Complexity,” In EUROCRYPT 2017, 2017.

76. M. Chase and S. Kamara, “Structured Encryption and Controlled Disclosure,” In ASIACRYPT, 2010.

77. P. Xu, S. Liang, W. Wang, W. Susilo, Q. Wu, and H. Jin, “Dynamic Searchable Symmetric Encryption with Physical Deletion and Small Leakage,” In ACISP 2017, 2017.

78. S. K. Kim, M. Kim, D. Lee, J. H. Park, and W. H. Kim, “Forward Secure Dynamic Searchable Symmetric Encryption with Efficient Updates,” In ACM, 2017.

79. D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, “Fairplay Secure Two-Party Computation System,” In Proceedings of the 13th USENIX Security Symposium, 2004.

80. Y. Lindell, B. Pinkas, N. P. Smart, and A. Yanai, “Efficient Constant Round Multi-party Computation Combining BMR and SPDZ,” In Advances in Cryptology - CRYPTO 2015, 2015.

81. [Online]. Available: ttps://www.easycrypt.info/trac.

82. D. Majidi and Z. Norouzi, “Introduction to Quantum Cryptography,”, Padafand Gherie Amel 2010 (In Persian).

Some New Topics in Cryptography: Essentials and Applications

H. Soleimany[*]

Abstract

Over the past decades, cryptography has always been a concern for both scientific and industrial researchers. The rapid growth in the field of information technology, along with the introduction of new concepts such as the Internet of Objects, as well as the growing range of users and a variety of new Internet services (such as social networks, cloud services, etc.), have created many challenges and consequently new security criteria are needed. This has led to the rapid growth of cryptographic science. The main purpose of this article is to introduce new approaches in the field of modern cryptography which either provide some new concepts or take significant steps to improve previous efforts. Accordingly, this paper follows three objectives: 1. Emphasizing the need to identify and review new cryptographic issues; 2. Clarifying some of the new cryptographic aspects by studying some of the most important developments in cryptography in recent years; 3. Reviewing briefly some of the latest issues and concepts considering future cryptographic orientations.

Key Words: *Futures studies, Modern cryptography, Symmetric cryptography*

[*] Shahid Beheshti University (h_soleimany@sbu.ac.ir)- Writer-in-Charge