رمزنگاری مشبکه-مبنا

مؤلف:
دکتر امیر حسنی کرباسی

فروردین ۱۳۹۷

سر شناسه : حسنی کرباسی،امیر،۱۳۶۴-
عنوان و نام پدیدآور : رمزنگاری مشبکه-مبنا/مولف امیر حسنی کرباسی
مشخصات نشر : تهران: ناقوس،۱۳۹۷
شخصات ظاهری :۱۲۸ص
شابک :978-600-473-104-1 ۱۴۰۰۰۰ریال
وضعیت فهرست نویسی : فیپا
یادداشت :رمز گذاری داده ها
موضوع : Data encryption(Computer science)
موضوع : رمز نگاری
موضوع : Cryptography
موضوع : شبکه های کامپیوتری—تدابیر ایمنی
موضوع : Computer networks—Security measures
رده بندی کنگره : ۱۳۹۷ ۵ ح ۸ ر/QA۷۶/۶/۹
رده بندی دیویی : ۰۰۵/۸۲
شماره کتابشناسی ملی : ۵۱۰۷۰۰۴

NAGHOOS PUBLICATION
انتشارات ناقوس

S.M.S : ۳۰۰۰۴۵۲۳۲۳

نام کتاب : رمزنگاری مشبکه -مبنا
ناشر : انتشارات ناقوس
مولفین : امیر حسنی کرباسی
چاپ اول : ۱۳۹۷
تیراژ : ۱۰۰
چاپ و صحافی : نارنجستان
صفحه آرایی : ثریا صفر زاده
ناظر چاپ : یاسمن تجلی محدث
قیمت : ۱۴۰۰۰۰ریال
شابک : ۹۷۸ -۶۰۰-۴۷۳-۱۰۱-۴
ISBN : 978-600-473- 101-4

مرکز پخش: انتشارات ناقوس
۱-خیابان بلوار کشاورز-خیابان ۱۶آذر-کوچه پارسی-پلاک ۱۰
تلفاکس-۶۶۴۷۸۹۵۱-۶۶۴۷۸۹۵۴

مقدمه مؤلف:

سپاس بی پایان نثار ایزد منان که به ما معرفت بخشید و توان درک علوم پر رمز و راز این جهان را عطا فرمود.

ایجاد ارتباط بین ساختارهای جبری پیچیده و طرح های رمزنگاری بهینه و امن، عامل اصلی تحقیقات و پژوهش های انجام شده در زمینه طراحی و تحلیل امنیتی پروتکل های رمزنگاری مشبکه-مبنا است. با گذشت زمان و با گسترش روش های تحلیل رمز و حملات سایبری بهینه، نیاز به جایگزینی و تهیه سامانه ها و پروتکل های هوشمند و امن براساس ساختارهای رمزنگاری مدرن و جدید به جای رمزنگاری سنتی و طرح های فرسوده و قدیمی در امنیت اطلاعات به طور چشمگیری احساس می شود. یکی از چالش های موجود در رمزنگاری در سال های اخیر، روی کار آمدن پرشرفت ها و ساختارهای جبری در پروتکل های جدید رمزنگاری است که در کاربردهای محصولات دنیای واقعی بکار برده می شوند و نیز یافتن راهی برای تضمین امنیت طرح ها و پروتکل های ضعیف و قدیمی است. درواقع، کمبود پروتکل های بهینه و امن با تعریف دقیق پارامترها و اثبات امنیت و با قابلیت پیاده سازی، دیده می شود.

رمزنگاری مشبکه-مبنا به عنوان حوزه ای با ساختارها و پروتکل های رمزنگاری متنوع و متعدد مطرح شده است که اثبات های امنیتی مستحکم در برابر حالت مسائل سخت مشبکه ها، مقاومت در برابر حملات کوانتومی، انعطاف پذیری و کارایی بالقوه شبه خطی را در مقابل طرح های رمزنگاری سنتی و کلاسیک فراهم می کند. طراحی، تحلیل امنیتی و پیاده سازی در رمزنگاری مشبکه-مبنا برای کاربردهای دنیای واقعی بسیار جذاب و مطلوب است.

در این کتاب، گامی به سوی تحقیقات نظری و کاربردی در حوزه رمزنگاری مشبکه-مبنا و به خصوص در زمینه طراحی و تحلیل امنیتی طرح ها و پروتکل های رمزنگاری مشبکه-مبنا بر اساس ساختارهای جبری برداشته می شود و به طراحی و تحلیل امنیتی سامانه های رمزنگاری GGH، NTRUEncrypt، سامانه طرح دوگان، طرح چکیده سازهای SPHF، پروتکل تبادل کلید PAKE، سامانه EEH و NETRU می پردازیم که مسیر جدیدی را برای تحقیقات نظری و کاربردی رمزنگاری مشبکه-مبنا در امنیت اطلاعات و امنیت

شبکه از جمله رایانش ابری، اینترنت اشیاء، دستگاه های بی سیم با قابلیت محدود و ... می‌گشایند. در این طرح ها و سامانه های رمزنگاری، کاربرد Dedekind domain، نمایش چندجمله ای ها، میدان های متناهی، حلقه های ماتریسی و سایر ساختارهای جبری را در رمزنگاری نشان می دهیم.

ضرورت رشد سامانه ها و پروتکل های پساکوانتومی امن و کاربردی برای مقابله کردن با حملات کامپیوترهای کوانتومی، مجموعه ای از زمینه های تحقیقاتی را ایجاد کرده است. بر این اساس، رمزنگاری مشبکه-مبنا یک حوزه جدید محسوب می شود که سامانه NTRU-Encrypt به عنوان یک کاندیدای امیدبخش پساکوانتومی در رمزنگاری مشبکه-مبنا در سال ۱۹۹۸ ارائه شد. NTRUEncrypt استاندارد شده و به مدت هجده سال مورد توجه جامعه تحلیل رمز قرار گرفته است. با این حال، حملات مکرر صورت گرفته روی طرح های امضای دیجیتال مشبکه-مبنا، باعث به وجود آمدن تردید در مورد تکامل رمزنگاری مشبکه-مبنا در جامعه رمزنگاری شد. به طور مشخص، یکی از مشکلات اصلی این بود که این نوع طرح ها و پروتکل ها، فاقد اثبات های امنیتی بودند که فقدان سخت بودن بنیان آن ها را نتیجه می داد. اکنون در سیزده سال اخیر، چشم انداز رمزنگاری مشبکه-مبنا با شروع از کار Regev و معرفی مسئله حالت متوسط LWE با نشان دادن کاهشی از مسائل الگوریتمی بدترین حالت روی مشبکه ها، به طور چشمگیری تغییر کرده است. شایان ذکر است الگوریتم های روی مشبکه های اقلیدسی حداقل از هر کاربرد رمزنگاری، به طور گسترده ای مورد مطالعه قرار گرفته اند و تعداد زیادی از مسائل بهینه سازی به آن ها بستگی دارند. سختی موجود در این مسائل و کاهش بدترین حالت به حالت متوسط، ثابت کرده است که تقریباً همه مشبکه هایی که با آن ها سر و کار داریم برخلاف رمزنگاری منحنی های بیضوی یا میدان های متناهی، سخت هستند.

رمزنگاری مشبکه-مبنا، مجموعه کاملی از سامانه ها، طرح ها و پروتکل های رمزنگاری را در خود دارد ولی بکار بردن این طرح ها را به صورت جعبه سیاه، مشکل می‌کند. زیرا طرح های رمزنگاری مشبکه-مبنا شامل پارامترهای زیادی هستند که با همدیگر ارتباط دارند که این حالت به طور فوق العاده ای روی پیچیدگی حملات شناخته شده و کارایی طرح ها اثر می‌گذارد. بنابراین انتخاب پارامترها با تضمین درست بودن طرح در یک سطح امنیتی مشخص، یک مسئله بهینه سازی حساس و دقیق است که در این کتاب، سامانه ها و طرح های ارائه شده، از این حالت پشتیبانی می‌کنند.

رمزنگاری مشبکه-مبنا در تئوری دارای محاسبات ساده ای بوده و وابسته به عملیات

ساده، کارا و توانمند است ولی در عمل، پیچیدگی های خاص خود را دارد. به عنوان مثال، یکی از بلوک های سازنده آن، نمونه برداری پارامترها با توزیع گوسی گسسته است و به طور معمول، نمونه برداری با توزیع گوسی گسسته همچنان نیازمند کار کردن با اعداد ممیز شناور است که با ساده بودن عملیات یعنی محاسبات برداری و ماتریسی در تناقض است. خوشبختانه، طرح های پیشنهادی جدید نیاز به نمونه برداری با توزیع گوسی گسسته روی اعداد صحیح دارند که الگوریتم های بهینه ای برای آن وجود دارد. مورد دیگر، وجود دو نوع مشبکه در رمزنگاری مشبکه-مبنا است: مشبکه هایی که یا تصادفی بوده یا دارای ساختار ریاضی قوی (مشبکه های ایده آل) هستند. متأسفانه، کار کردن با مشبکه های تصادفی، طرح های رمزنگاری را بسیار آهسته و اندازه کلیدهای عمومی را بسیار بزرگ می سازد و این مغایر با کارایی الگوریتم های رمزنگاری است. بنابراین، سوالاتی در مورد سختی مسائل الگوریتمی روی مشبکه های ایده آل مطرح می شود. هم اکنون، مشبکه های ایده آل با روش های تحلیل رمز مشبکه های تصادفی مورد آزمایش و مقایسه قرار می گیرند و انتخاب پارامترها در مشبکه های ایده آل براساس حملات شناخته شده روی مشبکه های تصادفی است. درنتیجه، بسیار مناسب خواهد بود که روش های تحلیل رمز مبتنی بر مشبکه های ایده آل در این حوزه تحقیقاتی، ارائه شوند.

این کتاب در قالب پنج فصل تنظیم شده است.

در فصل اول، مقدمه ای بر رمزنگاری و پیشینه رمزنگاری مشبکه-مبنا ارائه می شود.

در فصل دوم، تعاریف و مفاهیم پیش زمینه مطالعه می شوند که پایه ای برای فصل های آتی خواهند بود. یعنی، مشبکه ها و نمادگذاری های آن، الگوریتم ها و مسائل سخت مشبکه، توزیع گوسی گسسته و نمونه برداری خطاها، مشبکه های ایده آل و نتایج جدید در آن، بحث می شوند.

در فصل سوم، سامانه های رمزنگاری مهم مشبکه-مبنا یعنی، GGH، NTRUEn-crypt و سامانه طرح دوگان شرح داده می شوند.

درفصل چهارم، خانواده توابع چکیده سازی تصویری هموار و پروتکل تبادل کلید احراز هویت شده مبتنی بر کلمه عبور بیان می شوند.

در فصل پنجم، سامانه های رمزنگاری جدید و پیشرفته مشبکه-مبنا معرفی می شوند. ابتدا، طراحی سامانه رمزنگاری EEH ارائه می شود و اثبات درستی و تحلیل امنیتی آن بررسی می شود. سامانه رمزنگاری EEH عضوی از خانواده سامانه های رمزنگاری مشبکه-مبنای شبه GGH است که مبتنی بر اعداد صحیح آیزنشتاین $\mathbb{Z}[\zeta_3]$ بوده به طوری که ζ_3

ریشه سوم واحد است و از دید امنیتی به مسائل محاسباتی مبتنی بر مسئله کوتاهترین بردار (CVP) در مشبکه ها وابسته است. در طراحی و تحلیل امنیتی این سامانه، به اندازه کلید و نحوه انتخاب پارامترها پرداخته و نمایش چندجمله ای ها به کار گرفته شده است. بعلاوه، نتایج نظری و تجربی برای مقایسه امنیت و کارایی بین طرح های EEH و GGH فراهم شده و نشان داده می شود که EEH یک سامانه بهبود یافته از نظر امنیتی و کارایی است. سپس در ادامه، طراحی سامانه رمزنگاری NETRU مورد مطالعه قرار می‌گیرد و اثبات درستی و تحلیل امنیتی NETRU فراهم می شود. سامانه NETRU عضوی از خانواده سامانه های رمزنگاری مشبکه-مبنای شبه NTRU است که مبتنی بر میدان های متناهی بوده و نسخه ناجابجایی از سامانه رمزنگاری CTRU است و بر اساس حلقه ناجابجایی $M = M_k(\mathbb{Z}_p)[T, x]/ < X^n - I_{k\times k} >$ عمل می کند به طوری که M یک حلقه ماتریسی از ماتریس های $k \times k$ روی چندجمله ای های $R = \mathbb{Z}_p[T, x]/ < x^n - 1 >$ است. در تحلیل امنیتی NETRU نشان داده می شود که محاسبات رمزگذاری و رمزگشایی در آن ناجابجایی بوده و در مقابل حملات مشبکه و حملات جبر خطی مقاوم است.

امیر حسنی کرباسی
دکتری رمزنگاری و امنیت اطلاعات
amirhassanikarbasi@gmail.com
فروردین ۱۳۹۷

فهرست مطالب