The ISC Int'l Journal of Information Security
ISeCure

July 2015, Volume 7, Number 2 (p. 167)
http://www.isecure-journal.org

Persian Abstract

تسهیم چند راز با امنیت محاسباتی: مدل‌ها، طرح‌ها و تحلیل امنیت رسمی

سمانه مشهدی[1]

[1]دانشکده ریاضی، دانشگاه علم و صنعت ایران، تهران، ایران

در یک طرح تسهیم چند راز، واسطه تعدادی راز را به‌نحوی بین سهام‌داران توزیع می‌نماید که هر مجموعه مجاز از آن‌ها قادر به بازسازی رازها باشند. طرح‌های تسهیم راز موجود، یا به طور محاسباتی امن نبودند یا جهت تامین امنیت کامل، ناگزیر به استفاده از سهم‌هایی با طول بسیار بزرگ بودند. تا اینکه در سال ۲۰۱۳، هرانز و همکارانش اولین تعریف رسمی از امنیت محاسباتی در مدل استاندارد را برای طرح‌های تسهیم چند راز چند مرحله‌ای به همراه یک طرح کارا و امن ارائه نمودند. براساس اطلاعات ما، طرح ایشان، تنها طرح تسهیم چند راز به طور محاسباتی امن در مدل استاندارد است و برای سایر دسته بندی‌های طرح‌های تسهیم چند راز، هیچ تعریف رسمی از امنیت ارائه نشده است. بدین منظور ما در این مقاله برای سایر دسته بندی‌های طرح‌های تسهیم چند راز، امنیت در مقابل حمله راز انتخابی در مدل استاندارد را تعریف می‌نماییم. همچنین دو نمونه طرح تسهیم چند راز که متعلق به دسته بندی‌های متفاوت می‌باشند ارائه می‌کنیم. طرح‌های ارائه شده طول سهم‌هایی بسیار کوتاه دارند و امنیت محاسباتی آن‌ها در مدل استاندارد اثبات شده است.

واژه‌های کلیدی: طرح تسهیم چند راز، طرح تسهیم راز چند مرحله‌ای، امنیت اثبات‌پذیر، سیستم رمز کلید خصوصی، مدل استاندارد.

The ISC Int'l Journal of Information Security
ISeCure

July 2015, Volume 7, Number 2 (p. 168)
http://www.isecure-journal.org

Persian Abstract

پیاده‌سازی کارا با پیچیدگی زمانی کم و خط لوله‌ای ضرب‌کننده بیت-موازی با پایه چند جمله‌ای بر روی میدان‌های متناهی دودویی

بهرام رشیدی[۱]، رضا رضائیان فراشاهی[۲,۳] و سید مسعود سیدی[۱]

[۱]دانشکده برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

[۲]دانشکده علوم ریاضی، دانشگاه صنعتی اصفهان، اصفهان، ایران

[۳]پژوهشکده ریاضیات، پژوهشگاه دانشهای بنیادی(IPM)، تهران، ایران

در این مقاله دو روش موثر پیاده‌سازی ضرب کننده بیت-موازی سریع و خط لوله با پایه چند جمله‌ای بر روی میدان $GF(2^m)$ به وسیله سه جمله‌ای و پنج جمله‌ای‌های تحویل‌ناپذیر ارائه شده است. معماری اولین ضرب کننده براساس محاسبات موازی و مستقل توان‌های متغیر چند جمله‌ای می‌باشد. در دومین ساختار تنها محاسبات مربوط به توان‌های زوج متغیر چند جمله‌ای بکار گرفته شده‌اند. انجام محاسبات به‌صورت موازی، ساختاری منظم با هزینه سخت افزاری و تاخیر مسیر بحرانی کم فراهم ساخته است. علاوه براین در ساختارهای پیشنهادی از تکنیک خط لوله به‌منظور کوتاه کردن مسیر بحرانی و انجام محاسبات در دو سیکل ساعت استفاده شده است. پیاده‌سازی روش‌های پیشنهادی با موفقیت برای دو میدان متناهی $GF(2^{163})$ و $GF(2^{233})$ توسط نرم افزار Xilinx ISE 11 بر روی FPGA XC4VLX200 از خانوده Virtex-4 انجام گرفته است.

واژه‌های کلیدی: ضرب کننده بیت-موازی، رمزنگاری خم های بیضوی، سه جمله‌ای تحویل ناپذیر، پنج جمله‌ای تحویل ناپذیر، تکنیک خطا لوله‌ای.

The ISC Int'l Journal of Information Security
ISeCure

July 2015, Volume 7, Number 2 (p. 169)
http://www.isecure-journal.org

Persian Abstract

EEH: یک سامانه رمزنگاری مشبکه-مبنای شبه GGH روی اعداد صحیح آیزنشتاین بر اساس نمایش چندجمله‌ای‌ها

رضا ابراهیمی آتانی[۱]، شهاب‌الدین ابراهیمی آتانی[۲] و امیر حسنی کرباسی[۱]

[۱]دانشکده ریاضی، دانشگاه گیلان، رشت، ایران

[۲]دانشکده فنی، دانشگاه گیلان، رشت، ایران

در سال‌های اخیر، تحقیقات در حوزه رمزنگاری مشبکه-مبنا بسیار فعال و چشمگیر بوده است و نظریه مشبکه‌ها نقش مهمی را در طراحی، تحلیل و پیاده‌سازی طرح‌ها و سامانه‌های جدید و پیشرفته دارد. یک خانواده از این طرح‌ها، سامانه‌های رمزنگاری مشبکه-مبنای شبه GGH هستند که از دید امنیتی به مسائل محاسباتی مبتنی بر مسئله کوتاهترین بردار (CVP) در مشبکه‌ها وابسته‌اند. در این مقاله، سامانه رمزنگاری EEH را که یک سامانه شبه GGH بوده و مبتنی بر اعداد صحیح آیزنشتاین $\mathbf{Z}[z_3]$ است، ارائه داده‌ایم به‌طوری‌که $[z_3]$ ریشه سوم واحد است. همچنین به اندازه کلید و نحوه انتخاب پارامترها پرداخته و نمایش چندجمله‌ای‌ها را بکار می‌گیریم. بعلاوه، نتایج نظری و تجربی را برای مقایسه امنیت و کارایی بین طرح‌های EEH و GGH فراهم کرده و نشان می‌دهیم که EEH یک سامانه بهبود یافته‌ای GGH از نظر امنیتی و کارایی است.

واژه‌های کلیدی: رمزنگاری مشبکه-مبنا، GGH، Dedekind domain، نمایش چندجمله‌ای‌ها.

The ISC Int'l Journal of Information Security
ISeCure

July 2015, Volume 7, Number 2 (p. 170)
http://www.isecure-journal.org

Persian Abstract

تحلیل و ارزیابی برخی نامزدهای دور اول مسابقه CAESAR

جواد علیزاده[۱]، محمدرضا عارف[۲]، نصور باقری[۳]، علیرضا رحیمی[۱] و حسن صادقی[۴]

[۱]مرکز تحقیقات فتح، دانشکده و پژوهشکده مهندسی فاوا، دانشگاه جامع امام حسین (ع)، تهران، ایران
[۲]آزمایشگاه نظریه اطلاعات و امنیت (ISSL)، دانشگاه صنعتی شریف، تهران، ایران
[۳]دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
[۴]دانشکده علوم، دانشگاه قم، قم، ایران

AES-CMCCv1، AVALANCHEv1، CLOCv1 و SILCv1 چهار نامزد دور اول مسابقه CAESAR هستند. CLOCv1 در FSE 2014 ارائه شده و SILCv1 نیز بر اساس آن و با هدف بهبود هزینه پیاده‌سازی سخت‌افزاری طراحی شده است. در این مقاله، ضعف‌های ساختاری نامزدهای ذکر شده مورد مطالعه و بررسی قرار می‌گیرد و حملات تمایز برای AES-CMCCv1، با پیچیدگی دو درخواست و احتمال موفقیت تقریباً برابر با ۱، برای CLOCv1 و SILCv1 با پیچیدگی $O(۲^{n/۲})$ درخواست و احتمال موفقیت ۰/۶۳ ارائه می‌شود که در آن n طول بیتی قالب‌های پیام است. علاوه بر این، یک حمله جعل در مورد AVALANCHEv1 توضیح داده می‌شود که تنها یک درخواست لازم داشته و احتمال موفقیت برابر ۱ دارد. حملات ارائه شده در این مقاله، برخی ضعف‌ها در ساختار چهار نامزد دور اول مسابقه CAESAR و نادرست بودن ادعاهای امنیتی طراحان آن‌ها را نشان می‌دهند.

واژه‌های کلیدی: رمزگذاری احراز اصالت شده، CAESAR، CMCCv1، AVALANCHEv1، CLOCv1، SILCv1، حمله تمایز، حمله جعل.

The ISC Int'l Journal of Information Security
ISeCure

July 2015, Volume 7, Number 2 (p. 171)
http://www.isecure-journal.org

Persian Abstract

افزایش محرمانگی طرح‌های احرازهویت اخیر برای سامانه‌های RFID ارزان‌قیمت

کریم باقری[۱]، بهزاد عبدالملکی[۱]، بهاره اخباری[۲] و محمدرضا عارف[۱]

[۱]آزمایشگاه نظریه اطلاعات و امنیت (ISSL)، دانشگاه صنعتی شریف، تهران، ایران

[۲]دانشکده مهندسی برق، دانشگاه صنعتی خواجه نصیر طوسی، تهران، ایران

امروزه سامانه‌های RFID به صورت وسیعی در کاربردهای شناسایی و احرازهویت به کار گرفته شده است. در برخی از کاربردهای حساس، فراهم کردن یک مخابره‌ی امن و غیرقابل ردیابی برای کاربران بسیار حائز اهمیت است. به این منظور، پروتکل‌های احرازهویت گوناگونی برای سامانه‌های RFID پیشنهاد شده است که سعی در فراهم کردن امنیت و محرمانگی کاربران سامانه‌های RFID هستند. در این مقاله به آنالیز محرمانگی دو پروتکل جدید RFID که در سال‌های ۲۰۱۲ و ۲۰۱۳ پیشنهاد شده است، می‌پردازیم. برروی پروتکل اول انواع حمله‌های محرمانگی، از جمله ردیابی، ردیابی پیشرو و ردیابی پسرو را ارایه می‌کنیم و همچنین نشان می‌دهیم که پروتکل دوم نه تنها از حمله‌ی DoS رنج می‌کشد، بلکه در مقابل حمله‌های ردیابی و ردیابی پسرو آسیب‌پذیر است. تحلیل‌های محرمانگی را بر اساس یک مدل شناخته‌شده‌ی رسمی سامانه‌های RFID که توسط اوفی و فان در سال ۲۰۰۸ ارایه شده است، ارایه کرده‌ایم. در ادامه، به منظور غلبه به تمام ضعف‌های اشاره شده، برخی اصلاحات در ساختار پروتکل‌های ارایه شده اعمال می‌کنیم و دو نسخه‌ی اصلاح شده از پروتکل‌های آنالیز شده را پیشنهاد می‌کنیم.

واژه‌های کلیدی: پروتکل‌های احرازهویت سامانه‌های RFID، امنیت، محرمانگی، مدل اوفی–فان، استاندارد EPC C1 G2.

The ISC Int'l Journal of Information Security
ISeCure

July 2015, Volume 7, Number 2 (p. 172)
http://www.isecure-journal.org

Persian Abstract

یک روش مقابله با تبانی در سیستم‌های شهرت

مینا نیک‌نفس[۱]، صادق دری نوگورانی[۱] و رسول جلیلی[۱]

[۱]آزمایشگاه امنیت داده و شبکه، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

امروزه از مدیریت شهرت به طور گسترده‌ای برای تعدیل و تنظیم همکاری‌ها در سامانه‌های مشارکتی استفاده می‌شود. تبانی یکی از مخرب‌ترین حملات در این گونه سامانه‌هاست که در آن تبانی‌کنندگان به دنبال تأثیرگذاری ناعادلانه روی سامانه هستند. بسیاری از سامانه‌های مدیریت شهرت در برابر این حمله آسیب‌پذیرند، و برخی دیگر نیز راهکاری مختص خود را برای مقابله با این حمله دارند. نشان داده شده است که مسئله تشخیص تبانی در حالت کلی یک مسئله ان-پی-کامل است. در این مقاله ما یک معیار شباهت (سی-اس-ام) را ارائه، و از آن در یک الگوریتم اکتشافی خوشه‌بندی (سی-دی-ای) استفاده کرده‌ایم. پیچیدگی این الگوریتم از مرتبه n^2m+n^4 است که در آن m و n به ترتیب تعداد کل گره‌ها و تعداد تبانی‌کنندگان می‌باشد. به علاوه، برای پیاده‌سازی توزیع شده این الگوریتم معماری نیز پیشنهاد کرده‌ایم که در کنار بسیاری از مدل‌های شهرت قابل استفاده است. نتایج پیاده‌سازی و مقایسه آن با سایر روش‌ها نشان می‌دهد که روش پیشنهادی در مقابل تبانی‌کنندگانی که ناعادلانه قصد بالا بردن شهرت خود و پایین بردن شهرت دیگران را دارند، مؤثر واقع می‌شود.

واژه‌های کلیدی: مقاومت در برابر حمله، شهرت، تبانی، اعتماد.