19th International Power System Conference
نوزدهمین کنفرانس بین المللی برق
PSC 2004
98-F-DTC-598

پیاده‌سازی انواع بهینه شده توابع درهم مبتنی بر CBC-MAC و ارائه طرح جدید ترکیبی FCBC-XCBC-ECBC جهت حصول امنیت بالاتر در سیستم اتوماسیون توزیع نیروی برق

مهدی خادمیان[۱]، مروارید صحت‌کار[۲]، فرامرز فقیهی[۳]
دانشجوی کارشناسی مهندسی صنایع، دانشکده مهندسی صنایع / دانشگاه علم و صنعت ایران
دانشجوی کارشناسی ارشد هوش ماشین و رباتیک، گروه برق و کامپیوتر دانشکده فنی / دانشگاه تهران
دانشجوی دکتری برق، دانشکده مهندسی برق، مرکز تحقیقات فشارقوی و موادمغناطیسی / دانشگاه علم و صنعت ایران

واژه‌های کلیدی: سیستم اتوماسیون توزیع نیروی برق – تابع درهم – CBC-MAC – تصدیق اطلاعات، رمزنگاری

چکیده

با توجه به گسترش روزافزون ارتباطات و مخابرات، استفاده از فن‌آوری اطلاعات در سیستم‌های گوناگون به شدت مورد توجه است. از بحث‌های بسیار مهم در به کارگیری فن‌آوری اطلاعات، تصدیق داده‌های ارسالی - دریافتی است. به ویژه در سیستم‌های اتوماسیون توزیع با قابلیت‌های جمع‌آوری و پردازش اطلاعات و اعمال فرمان‌های کنترلی، امنیت و اعتبار اطلاعات بسیار ضروری به نظر می‌رسد. استفاده از طرح‌های کلید عمومی مبتنی بر خم بیضوی و الگوریتم‌های پر قدرت توابع درهم نظیر UMAC و MD5 برای این سیستم به عنوان پیشنهادهای کاراً مطرح شده است [۳-۱]. این مقاله برای دستیابی به سطح نسبی امنیت و حصول الگوریتم‌های با کارآیی مناسب از لحاظ سرعت، پیاده‌سازی توابع درهم بازبینی شده ECBC، FCBC، XCBC و مقایسه آن‌ها انجام شده است. در نهایت تابع ترکیبی آن‌ها به عنوان یک الگوریتم جدید جهت استفاده از همین توابع و رسیدن به امنیت بیشتر با توجه به خصوصیات سیستم اتوماسیون توزیع نیروی برق ارائه شده است.

۱- مقدمه

نیل به وابستگی روزافزون زندگی بشر به انرژی الکتریکی، قابلیت اطمینان و تداوم سرویس، کیفیت مطلوب و ایمنی کافی همراه با هزینه کم برای مشترکین برق اهمیت بیشتری یافته، تقریبا برای تمام مصرف کنندگان کیفیت برق و عدم قطعی آن از اهمیت زیادی برخوردار است. به‌دلایل مختلف تا قبل از دهه‌ی اخیر همواره توجه بیشتری به فعالیت‌های تولید و انتقال معطوف شده بود، اما در حال حاضر نیل به خصوصی

سازی‌های صورت گرفته و تجدید ساختار در شبکه برق به ویژه در حوزهٔ توزیع، روش‌های بهره‌برداری از شبکه‌ها با گرایش به سمت سرویس‌دهی کارآ به مشترکین، اولویت مهمی را در صنعت برق به خود اختصاص داده است [۸-۴].

سیستم اتوماسیون توزیع یکی از روش‌هایی است که به منظور دستیابی به این اهداف و کاهش مدت زمان خاموشی‌ها مورد توجه خاص شرکت‌های توزیع برق قرار گرفته است.

تبدیل شدن سیستم اتوماسیون توزیع به شبکه‌ای وسیع و پهناور و آمادگی آن برای پذیرفتن و اجرای دستورهایی که از هرجای شبکه برای آن ارسال می‌شود، از یک سو قدرت انعطاف پذیری فراوان به شبکه برای بالا بردن توان آن و از سوی دیگر ضعفی بزرگ از لحاظ امکان فراوان سرقت اطلاعات و ره‌یافت تغییر ناخواسته اطلاعات برای آن به وجود می‌آورد. این ضعف فقط با تصدیق اطلاعات در قسمت‌های مختلف شبکه قابل حل می‌باشد که ضرورت هرچه بیشتر امنیت و تصدیق اطلاعات روشن می‌گردد. چه بسا که با ارائه اطلاعات غلط، بسیاری از عملکردهای لحظه‌ای و برنامه‌های آنی تحت‌الشعاع قرار گیرد. عملکرد لحظه‌ای می‌تواند قطع و وصل ناصحیح دژنکتور یا سکسیونر باشد و عملکرد آینده را می‌توان برنامه‌ریزی رشد بار و میزان مصرف سالیانه و ... در نظر گرفت که هرکدام درجای خود خسارات فراوانی را به بار می‌آورد. در این راستا روش‌های گوناگون تایید اعتبار اعم از روش‌های امضای دیجیتال متکی بر کلید عمومی [۹] و توابع درهم[۹] در سیستم اتوماسیون توزیع قابل به کارگیری است. در کارهای تحقیقی انجام شده تاکنون ایدهٔ تئوریک خم بیضوی به عنوان یک الگوریتم فوق‌العاده امن با سرعت پایین مطرح شده است [۱] که حتی الگوریتم سریع شده آن [۱۱و۱۰] حداکثر بهبود زمانی تا دو برابر را خواهند داشت که فقط در مقاصد خاص امنیتی نظیر اتوماسیون پست‌های برق در مناطق مرزی در حال جنگ که دشمن سعی را در اختیار گرفتن کنترل برق خواهد داشت توجیه‌پذیر است. الگوریتم‌های تابع درهم MD5 که مبتنی بر تکرار توابع ساده غیر خطی است از امنیت خوب برخوردارند و در ارسال اطلاعات با حجم کم مناسب هستند که این الگوریتم[۳] و نوع بهینه شدهٔ آن [۱۲] برای سیستم اتوماسیون توزیع پیشنهاد شده‌اند. تابع درهم UMAC که از پیچیدگی خاص برخوردار است و زمان اجرای مناسبی دارد نیز برای این سیستم پیشنهاد وبا توجه به این کاربرد بهینه‌سازی و پیاده‌سازی شده است [۲].

در این مقاله به استفاده از توابع درهم ECBC – FCBC – XCBC و انواع ترکیبی آن‌ها به عنوان ایده جدید جهت حصول به امنیت بالاتر ضمن برخورداری از سرعت نه چندان کمتر و مقایسه و پیاده‌سازی آن‌ها پرداخته می‌شود.

۲- سیستم کلید عمومی

یکی از روش هایی که جهت تامین امنیت و اعتبار پیام استفاده می شود سیستم کلید عمومی است. در این روش متن اصلی توسط یک کلید عمومی رمز می شود و توسط یک کلید خصوصی گشوده می شود. هر منبع دارای یک کلید عمومی (e) و یک کلید خصوصی (d) است. فرض می کنیم که منبع A بخواهد پیام امن و معتبر M را برای B ارسال نماید، در این حالت ابتدا A پیام M را توسط کلید خصوصی خود، d_A، رمز کرده و $d_A(M)$ را به دست می آورد. برای امنیت پیام منبع A مقدار $d_A(M)$ را توسط کلید عمومی B یعنی e_B رمز می کند ومتن رمز شده $C = e_B(d_A(M))$ را برای B می فرستد. منبع B با دریافت C و با استفاده از کلید خصوصی خود یعنی d_B ابتدا متن $d_A(M)$ را به دست می آورد، آنگاه با استفاده از کلید عمومی A یعنی e_A متن اصلی M را آشکار می کند. از مهمترین مزیت‌های سیستم کلید عمومی این است که نیازی به ارسال کلید از طریق یک کانال امن نمی باشد.

$$e_A(d_B(C)) = e_A(d_B(e_B(d_A(M)))) = e_A(d_A(M)) = M$$

از جمله روش‌های مبتنی بر کلید عمومی امضای دیجیتال است، در امضای دیجیتال جهت اعتبار اطلاعات دریافتی شرایطی لازم است: گیرنده باید مطمئن باشد که پیام از منبع فرستنده است، امکان تغییر پیام توسط گیرنده و یا دیگری نباشد و همچنین فرستنده نیز بعدا نتواند ارسال پیام را انکار کند، با توجه به ویژگیهای سیستم کلید عمومی این

شرایط برقرارمی باشد. در حقیقت کلید خصوصی A یعنی d_A نقش امضا را خواهد داشت. از جمله روش‌های امضای دیجیتال می‌توان به امضای RSA، امضای شامیر، امضای ELGAMAL و امضای GMR اشاره کرد [۱۳].

امروزه خم های بیضوی در رمز نگاری کلید عمومی کاربرد وسیعی پیدا کرده اند. خم بیضوی یک سیستم رمزی منحصر به فرد کلید عمومی و مبتنی بر اصول ریاضی عملکرد گروه آبلی است که جوابی را با استفاده از اعداد کوچکتر برای دستیابی به سطح بالای امنیت ارائه می دهد[۹].

اگر F یک میدان باشد، مجموعه‌ای از نقاط $(x,y)\in F^2$ که در معادله

$$y^2+axy+by = x^3+cx^2+dx+e;\ a, b, c, d, e \in F$$

صدق کنند به همراه نقطه در بی‌نهایت، تشکیل یک خم بیضوی روی این میدان می دهند. از ویژگی جمع خم بیضوی برای رمزنگاری استفاده می شود. عملیات خم بیضوی مستلزم جمع، ضرب، مجذور کردن و وارونگی در میدان واقعی است که این امر زمان اجرای خم بیضوی را طولانی می‌کند. برای رفع این مشکل روش‌های مختلفی وجود دارد، استفاده از روش کاهش مدولار و بهینه سازی این روش تاثیر بسزایی در افزایش کارایی خم بیضوی دارد[۱۱]. ترکیب map و جدول فروبینیوس در میدانهای خاص، استفاده از روشهای بهینه دودویی و دستگاه مختصات مناسب حداکثر تا دو برابر سرعت الگوریتم را افزایش می دهند [۱۰].

خروجی‌های امضاهای دیجیتال و روش خم بیضوی دارای خروجی‌های نسبتا بزرگ و زمان اجرای طولانی می‌باشند که این موضوع سبب عدم کارایی آنها در بسیاری از کاربردها - از جمله کاربرد مورد نظر ما در شرایط معمول- می‌شود.

۳- توابع درهم

تابع درهم، یک تابع یک‌طرفه است که ورودی با طول دلخواه را به خروجی با طول ثابت تبدیل می‌کند[۹]. یک تابع درهم که به صورت H=h(M) تعریف می‌شود، دارای ویژگی‌های زیر است:

- به‌دست آوردن مقدار تابع H، از پیام ورودی M آسان است.
- به‌دست آوردن پیام ورودی از روی تابع مشکل است.
- با داشتن یک پیام M، به‌دست آوردن پیام دیگر M' که در شرط h(M)=h(M') صدق کند مشکل است.

در تعاریف مذکور آسانی و مشکلی از لحاظ محاسباتی عنوان شده‌اند. (اگر بیش از ۲۱۲۸ عملیات برای محاسبه تابعی نیاز باشد، گوییم محاسبه مشکل است).

اگر تابع درهم دارای خواص مناسبی باشد، به‌جای ارسال معتبر پیام می‌توان تابع درهم را به پیام اعمال و خروجی آن را به صورت معتبر همراه پیام برای گیرنده ارسال نمود، گیرنده نیز با در دست داشتن پیام و تابع درهم، خروجی تابع درهم را محاسبه و بررسی اعتبار را روی آن انجام می‌دهد. به دلیل این‌که طول خروجی تابع درهم از طول ورودی آن بسیار کوچک‌تر است ارسال آن از طریق کانال‌های مخابراتی به راحتی امکان‌پذیر است.

برای این‌که به‌جای پیام، خلاصه آن به صورت معتبر ارسال شود، به‌نظر می‌رسد که این خلاصه باید یکتا باشد، اما در عمل این خلاصه نمی‌تواند یکتا باشد زیرا به دلیل کوچکتر بودن طول خروجی از طول ورودی، تعداد زیادی پیام با خلاصه یکسان وجود دارند که به آنها تصادم[i] گفته می‌شود. اگر احتمال وجود تصادم کم باشد این مساله در به‌کار بردن تابع درهم اشکالی ایجاد نمی‌کند. در این مورد می‌توان به پارادوکس روز تولد[ii] اشاره نمود. مطابق پارادوکس مذکور، تعداد پیام‌هایی که باید برای پیدا کردن تصادم، مقدار درهم آنها را محاسبه نمود به صورتی که با احتمال نزدیک به ۵۰٪ تصادم پیدا شود $2^{\frac{n}{2}}$است که n طول خروجی تابع درهم است که به تبع آن، حداقل طول خروجی توابع درهم برای لحاظ امنیت باید ۱۲۸ بیت باشد [۱۳].

۴- الگوریتم‌های MAC

توابع MAC[iii] از دسته توابع درهم مبتنی بر سیستم‌های رمزنگاری قالبی هستند. از نمونه‌های رایج MAC، روش

MAC تکراری است. در این روش، پیام‌ها به قالب‌های کوچکتری تقسیم شده، سپس یک تابع کلیددار کوچک، به دفعات روی این قالب‌ها اعمال می‌گردد.

ورودی‌های تابع کلیددار، قالب‌های پیام و مقدار نتیجه قبلی تابع است که از آن‌ها برای تولید نتیجه بعدی استفاده می‌گردد. این‌کار برای هر قالب پیام تکرار شده، نتیجه نهایی به‌دست می‌آید.

تابع MAC شامل سه الگوریتم زیر است:

الگوریتم تولید کلید تصادفی که یک کلید را از فضای $\sum k$ به عنوان نتیجه بر می‌گرداند که $\sum=\{0,1\}$ و k طول کلید K است. $\sum k$ مجموعه همه رشته‌هایی از ۰و۱ به طول k است.

الگوریتم برچسب[iv] که کلید K و پیام M را به عنوان ورودی می‌گیرد و یک برچسب σ از $\sum t$ برمی‌گرداند.

الگوریتم Vf، که کلید K، پیام M و برچسب σ را گرفته و یک بیت برمی‌گرداند. در صـــورتی که رابطه‌ی Vf(M, σ,K) = 1 برقرار باشد، σ یک برچسب معتبر خواهد بود.

MAC4، CBC-MAC، ECBC، FCBC، XCBC، PMAC و UMAC همگی نمونه‌هایی از تابع MAC می‌باشند که در این مقاله توابع CBC-MAC، ECBC، FCBC و XCBC مورد بررسی، تحلیل و پیاده‌سازی قرار می‌گیرند.

۵- پیاده‌سازی توابع MAC

- روش CBC-MAC

ساده‌ترین و رایج‌ترین روش برای ساختن یک MAC است. برای این منظور پیام به قالب‌های m بیتی تقسیم و عملیات بازگشتی زیر انجام می‌شود:

$M = M_1M_2\ldots M_t$
$H_0 = I$
$H_i = e_K(H_{i-1} \oplus M_i)$, $i=1,\ldots,t$
$H(M) = H_t$

- روش ECBC

در روش CBC-MAC لایه‌گذاری[v] پیام به صورت دلخواه و قراردادی برای پیام انجام شده، پیام را به‌صورت مضرب صحیحی از n تبدیل می‌کند. در این روش هم برای پیام‌ها با مضرب n و هم برای پیام‌های لایه‌گذاری شده یک نوع کلید اعمال می‌شود که حالتی نامطلوب است. در ECBC پیام در صورتی که مضرب صحیحی از n نباشد به صورت لایه‌گذاری شده و در ازای لایه‌گذاری شدن تابع e_K اعمال شده تغییر پیدا می‌کند. این کار یک مرحله پیچیدگی به تابع اضافه می‌کند. الگوریتم به شکل زیر است:

if $M \in (\sum^n)^+$
then return $e_{K2}(CBC_{e_{K1}}(M))$
else return $e_{K3}(CBC_{e_{K1}}(M|\,|10^i))$, where i=n-1-|M| mod n

- روش FCBC

در روش ECBC برای بلوک آخر یک بار e_{K1} اعمال می‌شود و یک بار e_{K2} یا e_{K3} اعمال خواهد شد. این‌مورد می‌تواند برای کاهش زمان اعمال شده به حالتی که در آن e_{K1} دیگر اعمال نشود، تغییر پیدا کند که روش جدید را FCBC نامیده‌اند. الگوریتم آن به صورت زیر است.

if $M \in (\sum^n)^+$
then return $K \leftarrow K_2$ and $P \leftarrow M$
else return $K \leftarrow K_3$ and $P \leftarrow M|\,|10^i$, where i=n-1-|M| mod n

P=P1…Pm , | P1 | = … = | Pm | = n
$H_0 \leftarrow 0^n$
for $H_0 \leftarrow 0^n$ to m-1 do
$H_i \leftarrow e_{K1}(P_i \oplus H_{i-1})$
return $H_m \leftarrow e_K(P_m \oplus H_{m-1})$

- روش XCBC

وقتی یک کلید به یک سری زیر کلید تبدیل می‌شود بیشتر رمزهای بلوکی هزینه تنظیم کردن کلیدها را دارا می‌باشند. زیرکلیدها اغلب از کلید اصلی بزرگتر هستند و محاسبه‌ی آن‌ها ممکن است مستلزم هزینه باشد. بنابراین کلیددار کردن رمزهای بلوکی با کلیدهای چندگانه مانند آنچه در ECBC و FCBC انجام شد چندان مطلوب نیست. بهتر است که از همان کلید برای همه رمز بلوکی استفاده شود. الگوریتم XCBC این کار را انجام می‌دهد.

if $M \in \left(\sum^n\right)^+$
then return $K \leftarrow K_2$ and $P \leftarrow M$
else return $K \leftarrow K_3$ and $P \leftarrow M \mid 10^i$, where i=n-1-|M| mod n

P=P1…Pm , | P1 | = … = | Pm | = n
$H_0 \leftarrow 0^n$
for $H_0 \leftarrow 0^n$ to m-1 do
$H_i \leftarrow e_{K1}(P_i \oplus H_{i-1} \oplus K)$
return $H_m \leftarrow e_{K1}(P_m \oplus H_{m-1} \oplus K)$.

۶- ارائه یک MAC ترکیبی جدید - راهکاری برای افزایش امنیت ضمن توازن سرعت در سیستم اتوماسیون توزیع

توابع MAC استاندارد و تایید شده توابعی بودند که معرفی شدند. حال برای افزایش پیچیدگی خروجی و تولید خروجی‌هایی امن‌تر از ترکیبی پیشنهادی برای توابع فوق مبتنی بر ویژگی‌های مثبت MAC های استاندارد و تابع درهم قوی HMAC [۹].استفاده می‌کنیم. تابع جدید را آلفا MAC نامیده‌ایم و آن را به صورت زیر تعریف می‌کنیم.

M = P1P2…Pm
αMAC =
FCBC(XCBC(P1⊕ K1)||ECBC(P2 ⊕ K_2)||M)

تابع ارائه شده دارای ویژگی‌های زیر است:

۱- در این تابع از هر سه تابع استاندارد MAC بهینه شده استفاده می‌شود. لذا از لحاظ پیچیدگی الگوریتم به مرتبه بالاتری دست یافته‌ایم.
۲- طراحی الگوریتم جدید از لحاظ ساختار کلی بسیار شبیه به ساختار کلی HMAC است که از کارآترین الگوریتم‌ها از لحاظ امنیت است، لذا انتظار بر آن است از لحاظ امنیت دارای ویژگی‌های این تابع باشد.
۳- علاوه بر آن به دلیل وجود MAC های بهینه در ساختار تابع درهم جدید پیشنهادی، لم محدوده تصادم را ارضا می‌کند و برای دو پیام متفاوت M و M' که دارای $m = |M|/n$ و $m' = |M'|/n$ بلوک باشند، با فرض $m, m' \le N/4$ که $N=2^n$ داریم:

$$V_n(m, m') \le \frac{(m+m')^2}{2^n}$$

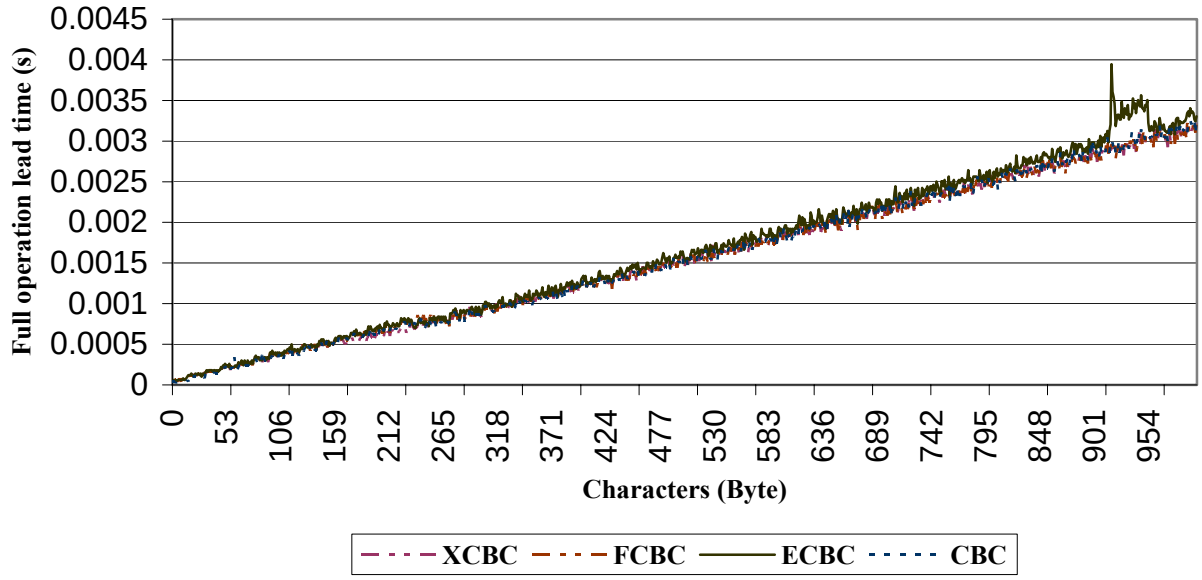
۴- این تابع در اجراهای با طول بسیار بزرگ از لحاظ زمانی مشکل‌ساز خواهد بود، حال آن‌که در سیستم اتوماسیون توزیع محدوده‌ای کوچک مدنظر است و حجم پیام‌ها به دو گروه اطلاعات آماری و اطلاعات آنی تقسیم‌بندی می‌شود که برای آن‌ها هم‌چنان زمان اجرا با اختلاف ناچیزی با زمان اجرای سه تابع استاندارد برابری می‌کند که در قسمت بعدی به تفصیل آمده‌است. به عنوان مثال درهم‌سازی متن نسبتا بزرگ ۱۳۶۹۸ بایتی برای سیستم اتوماسیون توسط این تابع پیشنهادی در ۰,۰۰۰۹۱۴۹۸۲۶ ثانیه انجام می‌پذیرد.

۷- مقایسه توابع

به‌منظور مطالعه کارآیی زمانی توابع مورد بحث، این موضوع با استفاده از نمودارها و اطلاعات به‌دست آمده ازپیاده‌سازی نرم‌افزاری توابع بررسی شده‌است.

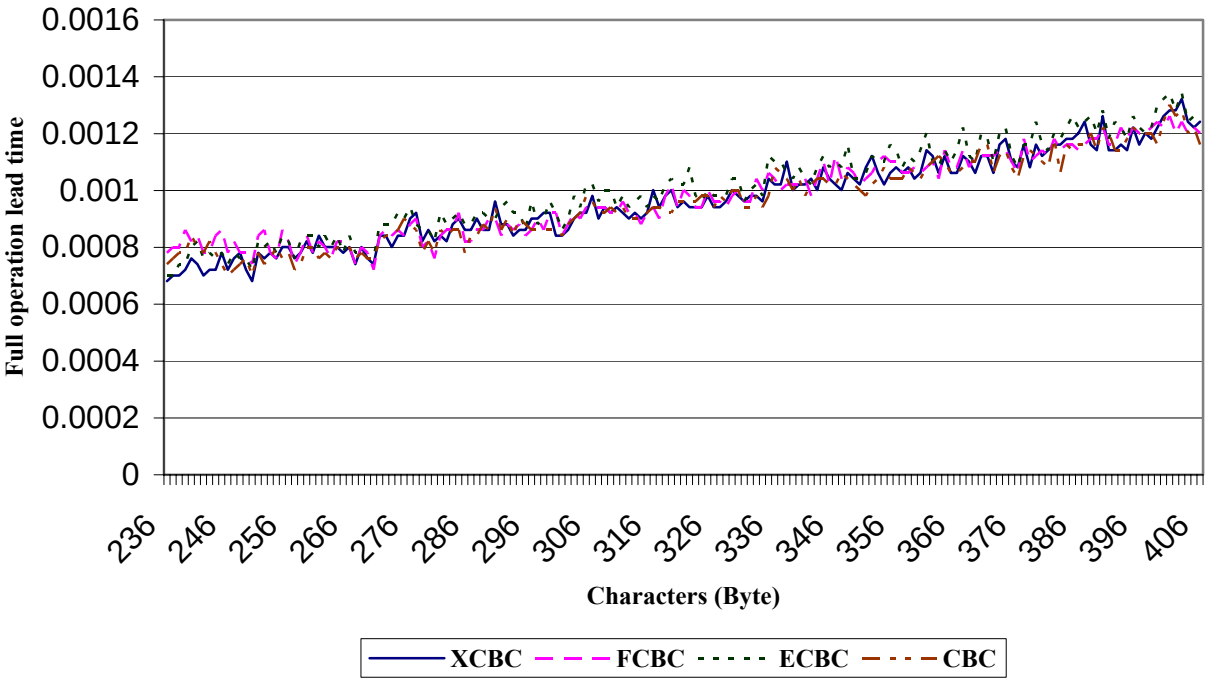
در توابعی از جمله توابع درهم میزان زمان انجام عملیات توسط تابع از موارد بسیار مهم می‌باشد. زیرا اگر در یک بازه‌ی زمانی خاص نیاز به تعداد زیادی عملیات با تابع درهم باشد، آن موقع تلفات زمان حتی به میزان چند صدم ثانیه برای یک بار عمل، در چندین بار اجرا بسیار دیده می‌شود. از سوی دیگر در سیستم اتوماسیون توزیع نیروی برق که موضوع مطالعه ماست زمان‌هایی نظیر دستور قطع و وصل برای دژنگتورها باید تا حد امکان آنی و بدون وقفه صورت گیرد، چرا که یک لحظه زمانی کوچک در حالات بروز خطا قادر است سبب به‌بار آوردن خسارات فراوان در سیستم توزیع شود. در نمودارهایی که ارائه شده است، زمان‌های منتج شده در حالت‌های مختلف استفاده از این چهار تابع درهم بررسی می‌شود.

بررسی زمان‌های انجام عملیات برای طول رشته تا ۱۰۰۰ کاراکتر



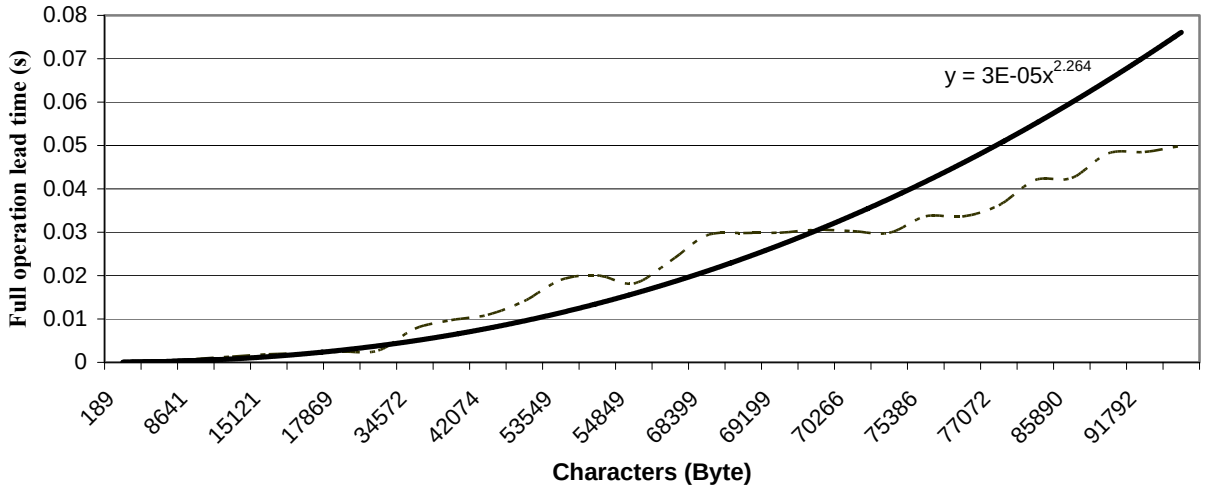
شکل ۱- زمان‌های اجرا برای چهار تابع استاندارد MAC

مدت زمان اجرا برای بازه ۲۳۶ تا ۴۰۶ کاراکتر



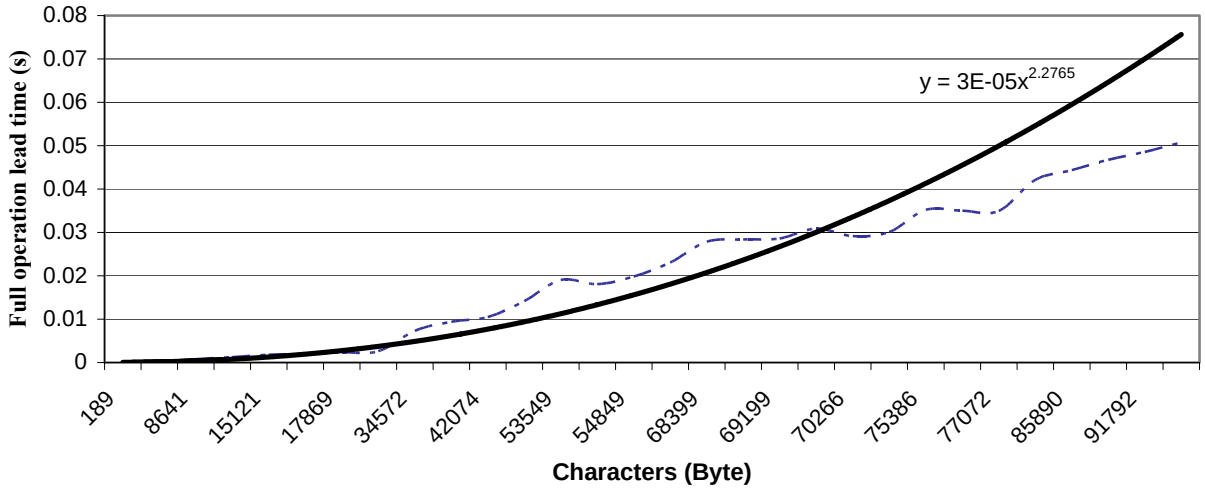
شکل ۲- تحلیل دقیق زمان‌های اجرا برای چهار تابع استاندارد MAC در یک بازه محدود

بررسی زمان انجام عملیات در تابع XCBC برای حجم‌های زیاد



شکل ۳ - مطالعه زمانی بهترین نوع استاندارد MACبرای درهم سازی اطلاعات آماری سیستم اتوماسیون توزیع

بررسی زمان انجام عملیات در تابع αMAC برای حجم‌های زیاد



شکل ۴ - مطالعه زمانی تابع درهم پیشنهادی برای درهم سازی اطلاعات آنی و آماری سیستم اتوماسیون توزیع

- اطلاعات به‌دست آمده بر مبنای الگوریتم‌های ارائه شده در قسمت‌های قبل وپیاده‌سازی نرم‌افزاری، استخراج شده است. پردازنده‌ی سیستمی که اطلاعات با استفاده از آن تولید شده Athlon XP 2500 بوده که دارای Clock 1.84GHz می‌باشد.
- در استخراج اطلاعات دو نمودار اولیه اطلاعات زمانی پس از ۵۰۰ بار انجام عملیات به‌دست آمده است. هم‌چنین برای به‌دست آمدن اطلاعات زمانی هر تعداد کاراکتر از نمودار سوم ۱۰۰ بار تابع XCBC اجرا شده است.

- به‌دست آمدن تعداد کاراکترها برای تولید رشته اولیه به صورت تصادفی انجام شده و سپس طبق تعریف تابع مورد نظر لایه‌گذاری بر روی آن انجام شده است.

از نتایج اجرا به‌طور خلاصه می‌توان گفت:

۱- در توابع درهم مورد مطالعه برای بازه‌ای از ۱ تا ۱۰۰۰ بایت عملیات درهم‌سازی اجرا و اندازه‌گیری زمانی شده‌است که می‌تواند بیان‌گر اطلاعات لحظه‌ای ولتاژ (ولت)، جریان (آمپر)، ضریب قدرت، توان اکتیو و راکتیو(کیلووات و کیلووار)، میزان مصرف انرژی(کیلووات ساعت و کیلووار ساعت) و ... باشد که تجهیزات اندازه‌گیری در پست‌های توزیع اعم از ولت‌متر، آمپرمتر، وات‌متر و یا یک انرژی مولتی‌متر این مقادیر را به‌طور دائمی نشان می‌دهند (شکل (۱)).

۲- در راستای مطالعه دقیق‌تر بازه زمانی ۲۳۴ تا ۴۰۶ بایت که محدوده مناسبی از لحاظ ارسال و دریافت اطلاعات – و تقریبا چند برابر معمول است- را جداگانه در شکل (۲) آورده‌ایم.

۳- در نگاهی دیگر در راستای برداشت اطلاعات آماری از پست‌های توزیع و در راستای صحت اطلاعات دریافتی به مرکز کنترل، تایید اعتبار ضروری است تا پس از پردازش اطلاعات به نتایج قابل استناد و صحیح دست یابیم. از این‌رو در این گروه اطلاعات که دارای حجم بزرگتری نسبت به فرمان‌های اعمالی لحظه‌ای می‌باشند زمان اجرا برای رشته با طول ۱۸۹ الی ۹۱۷۹۲ بایت را به دست آورده‌ایم که تنها نتایج را برای بهترین نوع یعنی XCBC آورده‌ایم(شکل (۳)).

۴- برای تابع جدید پیشنهادی در حجم‌های تا ۱۰۰۰ بایت همان‌طور که انتظار می‌رفت زمان اجرا بسیار نزدیک به زمان اجرا سایر انواع استاندارد بود. اما زمان اجرا برای حجم‌های بزرگ (اطلاعات آماری سیستم توزیع) با توجه به استفاده از توابع سه‌گانه در بدنه الگوریتم پیشنهادی ما را دچار شبهه می‌کند که با اجرای انجام شده از ۱ الی ۹۱۷۹۲ در شکل (۴) مطابقت زمانی در این حجم از ارسال و دریافت داده کماکان تفاوت چندانی نکرده است که حاکی از موفقیت زمانی در ارائه جدید این مقاله ضمن بالا بردن امنیت دارد.

۵- در شکل‌های (۳) و (۴) بر زمان‌های به‌دست‌آمده منحنی‌هایی برازش شده‌است که این منحنی‌ها نمایی می‌باشند.

۶- منحنی نمایی حکایت از آن دارد که این درهم‌سازی فقط در سیستم‌هایی جوابگو ست که حجم ارسال و دریافت اطلاعات‌زیادنباشد و یا اینکه سرعت نقش مهمی را ایفا نکند.

۷- توان متغیر X در منحنی‌های برازش شده بسیار به یکدیگر نزدیک بوده، نشان می‌دهد از لحاظ اجرا تابع پیشنهادی هیچ مشکلی پیدا نکرده است.

۸- در محدوده مورد نظر –همان‌طور که از شکل (۱) پیداست- از لحاظ زمانی توابع دارای رفتاری نزدیک به یکدیگر می‌باشند.

۹- از شکل (۲) می‌توان تحلیل دقیق زمان‌های اجرا را برای یک بازه کوچک ارائه نمود:

الف) در محدوده مورد نظر توابع بسیار از لحاظ زمانی نزدیک به یکدیگر بوده، نمی‌توان هیچ یک را سریع‌تر از دیگران دانست.

ب) در یک اظهار نظر کلی و تقریبی XCBC را که از لحاظ الگوریتم نسبت به بقیه انواع مناسب‌تر است (مطابق تحلیل انجام شده در قسمت پنجم) از لحاظ زمانی نسبت به دیگران وضعیت متوسط مناسبی دارد.

ج) اظهار نظر قسمت (ب) خیلی قابل استناد نیست، زیرا اول، در همه مواقع اینچنین نیست. دوم، این مقادیر بسیار به یکدیگر نزدیک بوده آنچنانکه حتی در نمودار ارائه شده قابل تشخیص نیستند.

د) در نمودار شکل (۲) دیده می‌شود که برای یک نوع تابع درهم، زمان خروجی دقیقا روندی صعودی ندارد. به عبارتی برای پیام با طول کمی بیشتر زمان کمتری به‌دست می‌آید. علت را در مورد زیر می‌توان یافت:

اول آن‌که میزان منابعی که سیستم در بازه‌های زمانی مختلف در اختیار برنامه قرار می‌دهد بر اساس کارآیی پردازنده، میزان حافظه موجود و منابع دیگر متفاوت است.

دوم، با توجه به الگوریتم‌های ارائه شده طول پیام در میزان عملیات مورد نیاز در پردازش آن عامل مهمی است مانند نیاز یا عدم نیاز به لایه گذاری.

۱۰- تابع ارائه شده برای سیستم اتوماسیون توزیع با توجه به حجم اطلاعات انتقالی، نبود تفاوت قابل توجه در سرعت و امنیت بهتر آن نسبت به سایر انواع استاندارد را می‌توان در کلاس بالاتری جای داد.

۸- نتیجه‌گیری

در این مقاله برای دست یافتن به یک سیستم کارآمد برای تایید اطلاعات در سیستم اتوماسیون توزیع مطالعه انواع جدید توابع درهم MAC انجام شد. شرح الگوریتم‌های مذکور با تحلیل میزان کارآیی آن‌ها انجام شد و انواع CBC-MAC ، E-CBC ، F-CBC و X-CBC مورد پیاده‌سازی نرم‌افزاری گرفت. با توجه به حجم کوچک اطلاعات مبادله شده در سیستم اتوماسیون توزیع و میزان مجاز اتلاف زمانی، این توابع از نقطه نظر زمانی مناسب می‌باشند که نتایج زمانی را در محدوده ۰/۰۰۰۵ الی ۰/۰۰۴۵ ثانیه برای حجم تا ۱ کیلوبایت مقدار قابل قبولی است. اما در راستای حصول به امنیت بالاتر تابع درهم جدیدی بر پایه این سه تابع پیشنهاد نمودیم که از هر سه آن‌ها در بدنه خود بهره می‌برد، ضمن آن‌که از لحاظ ساختار کلی مبتنی و نزدیک به الگوریتم تابع بسیار امن HMAC بود که ویژگی های مناسب امنیتی آن را در الگوریتم ما القا نماید. تابع ارائه شده ضمن حصول امنیت بالاتر، دارای زمان اجرای در محدوده توابع قبلی تا حدود ۱ کیلو بایت بوده، حتی برای اطمینان از وضعیت زمانی آن تا حجم ۹۰ کیلوبایت برای ارسال اطلاعات آماری شبکه مورد مطالعه قرار گرفت که تا این محدوده همچنان زمان اجرا بسیار نزدیک به زمان اجرای هر یک از توابع سه‌گانه است. علت این امر را در انباشت اطلاعات در حافظه از اجراهای یک تابع MAC و استفاده از آن در توابع مشابه بعدی است که زمان را چندان دستخوش تغیر نمی‌کند و همین‌طور اصول کلی ساختار که مبتنی بر HMAC است، در حالی‌که پیچیدگی به مراتب بالاتر رفته و مقاومت در مقابل حمله‌های بازیابی کلید، تصادم L و جعلی بالا می‌رود.

مراجع

[1] F. Faghihi, M. esmaeili and M. Sehatkar, "information security in distribution automation system by Elliptic curve", *17th International power system conference*, 28-30 Oct. 2002 Tehran – Iran – proceeding (4), control & protection _Telecommunication – IT – pp.89-97

[2] H. Heydari, F. Faghihi, M. Sehatkar , "UMAC hash function for data authentication in power electric distribution automation system", *18th International power system conference*, – proceeding (4), control & protection _Telecommunication – IT, 2003.

[3] F. Faghihi and M. Esmaeili, "Message Authentication in Distribution Automation System by MD5 Hash function", *8th Electric power distribution conference (IPDC)*, IAEEE 2003, Tehran, Iran, Vol.1, pp. 39-45

[4] Z. Alaywan and J. Allen, "California Electric Restructuring: a Broad Description of the Development of the California ISO," *IEEE Transactions on Power System*, Vol. 13, No. 4, November, pp 1445-1450, 1998.

[5] Y. Hong, S. W. Tsia, and M. T. Weng, "Bidding Strategy Based on Artificial Intelligent for a Competitive Electric Market," *IEE Proceeding,* General Transmission and Distribution, Vol. 148, No. 2, pp 159-164, March 2001.

[6] M. Apprill, "Regulations Impact on Restructuring," *IEEE Potentials*, pp. 11-13, December 1997 / January 1998.

[7] M. Ilic and P. Skantze, "Electric Power Systems Operation by Decision and Control," *IEEE Control Systems Magazine*, pp25-38, August 2000.

[8] Q. Feng , X. Bai, "Model of Electric Market Operation Support System Based on UML," *Proceeding of the IEEE Conferences*, pp.13-17, 2001.

[9] D. Stinson, "*Cryptography, Theory and Practice*," CRC press,2002.

[10] T. Kobayashi, H. Morita, and F. Hoshine, "Fast Elliptic Curve Algorithms Combining Ferrobenius Map and Table Reference to Adapt to Higher Characteristic," *EUROCRYPT 99*, Vol. LNCS 1592, 1999, pp. 176-189.

[11] Y. Han, P. Leong, and T. J. Zhang, "Fast Algorithms for Elliptic Curve

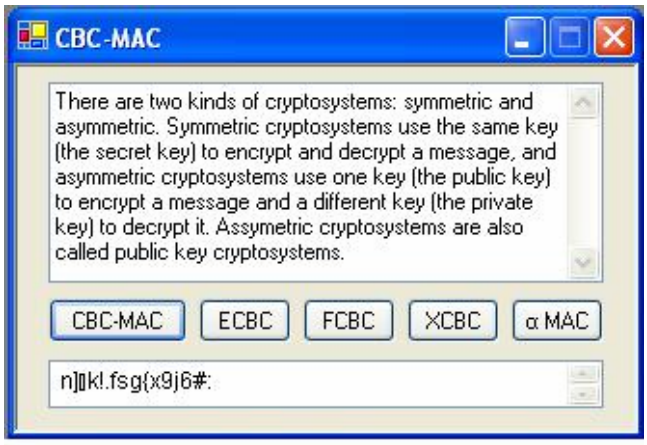
Cryptosystem over Binary Finite Field," *Crypto 2000*, pp. 75-85.
[12] M. Sehatkar and F. Faghihi, "Data Authentication in Distribution Automation System Using Optimized MD5 Hash Function," *Wseas Transaction on communication*, Issue 2, Vol. 3, April 2004, pp. 622-625
[13] A. J. Menezes, P. Cvan, O. Scott and A.Vanstone, "*Handbook of applied Cryptography*," CRC press, 1996.

[i] Collision
[ii] Birthday paradox
[iii] Message Authentication Code
[iv] Tag
[v] Padding

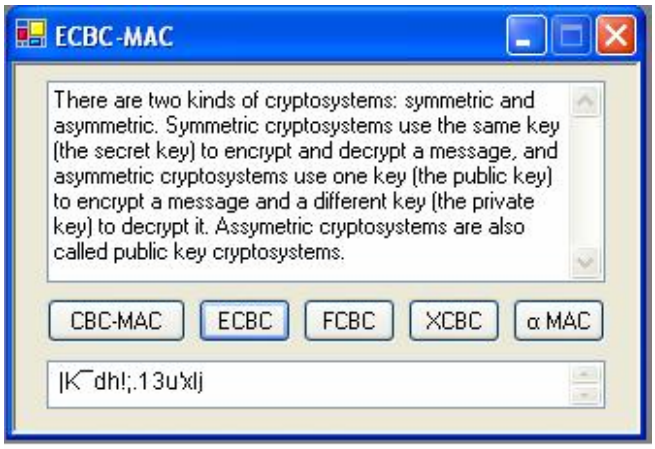
پیوست:

ذیلا نتایج اجرای نمونه‌ای توابع درهم مورد بحث در مقاله آمده است.

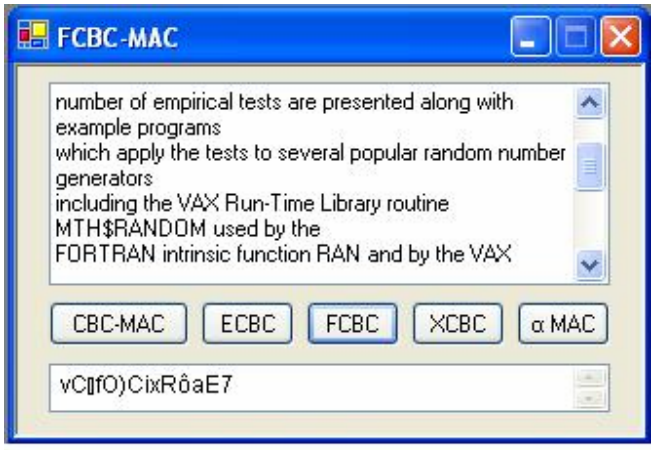
الف) اجرای نرم‌افزاری CBC-MAC:



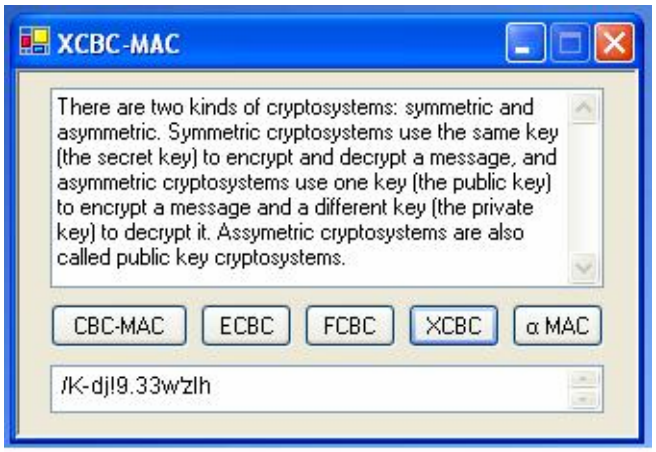
ب) اجرای نرم‌افزاری E- CBC:



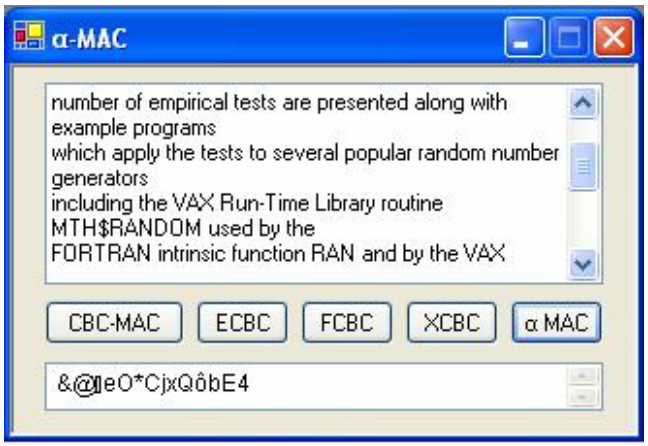
ج) اجرای نرم‌افزاری F-CBC:



د) اجرای نرم‌افزاری X-CBC:



ه) اجرای نرم‌افزاری تابع درهم جدید پیشنهادی ترکیبی:



#