بهبود الگوریتم رمزنگاری مبتنی بر هویت و بهره‌وری آن در فراهم‌کردن محرمانگی سیستم‌های سلامت الکترونیک ابری

مجید علی‌پور، شقایق بختیاری چهل‌چشمه و شهرام حیدریان

چکیده: در این مقاله ابتدا یک روش جدید رمزنگاری مبتنی بر هویت ارائه می‌گردد و نشان داده می‌شود در مقایسه با روش‌های پیشین دارای سربار محاسباتی کمتری است. در این راستا، روش مبتنی بر هویت پیشنهادی، شبیه‌سازی شده و نتایج حاصل با نمایندگان برتر رمزنگاری مبتنی بر هویت مورد مقایسه قرار می‌گیرد. سپس در ادامه پژوهش با استفاده از پروکسی رمزنگاری مجدد و روش رمز مبتنی بر هویت ارائه‌شده در این مقاله، یک سیستم سلامت الکترونیک ابری پیشنهاد می‌گردد. این سیستم علاوه بر فراهم‌کردن محرمانگی و افزایش قابلیت دسترسی، در کلیه مراحل راه‌اندازی، تولید کلید خصوصی، رمزگذاری، تولید کلید رمز مجدد، رمزنگاری مجدد و رمزگشایی دارای زمان اجرای کمتری است و منجر به کاهش هزینه محاسباتی و سربار ارتباطی فرایند رمزنگاری در سیستم سلامت الکترونیک می‌شود.

کلیدواژه: ***سیستم سلامت الکترونیک، فضای ابر، رمزنگاری مبتنی بر هویت، پروکسی رمزنگاری مجدد.***

۱- مقدمه

امروزه سیستم‌های سلامت الکترونیک[1] به دلیل ارائه خدماتی مانند یکپارچه‌سازی یکنواخت داده‌ها و تسهیل فرایند تشخیص پزشکی در جهت ارتقای سطح بهداشت جامعه بیش از پیش مورد توجه قرار گرفته‌اند. در جوامع پیشرفته سیستم‌های سلامت به سرعت در حال توسعه و کاربردی‌شدن هستند چرا که به کارگیری و توسعه سیستم‌های سلامت الکترونیک نقش اساسی در ارتقای سطح بهداشت، تسریع در ارائه خدمات بهداشتی و کاهش خطاهای انسانی در فرایند ارائه خدمات بهداشتی، تشخیص بیماری و تجویز دارو دارند [۱].

از مهم‌ترین چالش‌های پیش رو در توسعه و پیشبرد سیستم‌های سلامت الکترونیک می‌توان به تأمین سرویس محرمانگی[2] و حفظ حریم خصوصی اشاره نمود چرا که هر گونه حمله در این سیستم‌ها منجر به خسارات جبران‌ناپذیری خواهد شد. از این رو در سال‌های گذشته پیشنهادهای بسیاری برای تأمین امنیت و حفظ محرمانگی در سیستم‌های سلامت الکترونیک ارائه شده است. بسیاری از این روش‌ها مبتنی بر پروتکل‌های سنتی زیرساخت کلید عمومی (PKI)[3] هستند. در این سیستم‌ها مشکلاتی از قبیل مدیریت کلید عمومی[4] و احراز اصالت کاربران باعث می‌شود تا امکان استفاده از این سیستم‌ها برای همه کاربران به آسانی صورت نپذیرد [۲]. سیستم‌های مبتنی بر زیرساخت کلید عمومی نیاز به یک موجودیت با عنوان طرف سوم مورد اعتماد[5]، جهت صدور گواهینامه‌های[6] امضاشده دارند تا کاربران به وسیله گواهینامه‌های ارائه‌شده از اصالت[7] کلید عمومی کاربران دیگر اطمینان حاصل کنند. این مسأله علاوه بر افزایش پیچیدگی سیستم، موجب افزایش هزینه در سیستم‌های سلامت الکترونیک می‌شود. مشکلاتی از قبیل پیچیدگی مدیریت کلید عمومی و احراز اصالت کاربران در سیستم‌های سنتی کلید عمومی همواره هزینه‌های ناشی از به کارگیری این روش‌ها در سیستم‌های سلامت الکترونیک را افزایش می‌دهد.

در سال ۱۹۸۴ مفهوم رمزنگاری مبتنی بر هویت (IBE)[8] با هدف تسهیل مدیریت گواهینامه و کاهش پیچیدگی در سیستم‌های کلید عمومی سنتی معرفی شد. در الگوی رمزنگاری مبتنی بر هویت کلید عمومی کاربران، اطلاعات هویتی کاربران (مانند آدرس ایمیل، شناسه‌های ملی، شماره تلفن، عوامل ژنتیکی[9] و غیره) است. به این ترتیب از آنجایی که کلید عمومی گیرنده پیام مطابق با الگوریتم رمزنگاری مبتنی بر هویت توسط خود فرستنده ایجاد می‌شود از اصالت کلید گیرنده اطمینان خواهد داشت. در نتیجه در سیستم رمزنگاری مبتنی بر هویت نیاز به موجودیت سوم شخص مورد اعتماد نیست. استفاده از سیستم‌های رمزنگاری مبتنی بر هویت علاوه بر تأمین امنیت و حفظ محرمانگی اطلاعات [۳]، سهولت در کاربری سیستم‌های سلامت را برای استفاده‌کنندگان از این سیستم‌ها به همراه دارد. بهره‌مندی از مزایای رمزنگاری مبتنی بر هویت در سیستم‌های سلامت الکترونیک استفاده از این سیستم‌ها را برای مخاطبان سیستم آسان و هزینه‌های این قبیل سیستم‌ها را به طور چشم‌گیری کاهش می‌دهد. استفاده مستقیم از برخی رشته‌ها مانند آدرس ایمیل کاربران به عنوان کلید عمومی باعث کاهش بار کاری کاربران و سربار ارتباطی در سیستم سلامت الکترونیک خواهد شد [۲].

پروکسی رمزنگاری مجدد[10] یکی دیگر از روش‌های رمزنگاری است که هدف آن تبدیل[11] متن رمزشده[12] با استفاده از شناسه هویتی کاربر اول به متن رمزشده دیگری با استفاده از شناسه هویتی کاربر دوم است. به

این مقاله در تاریخ ۶ فروردین ماه ۱۳۹۷ دریافت و در تاریخ ۱۰ بهمن ماه ۱۳۹۷ بازنگری شد.

مجید علی‌پور، گروه کامپیوتر، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران، (email: m.alipour.6689@gmail.com).

شقایق بختیاری چهل‌چشمه (نویسنده مسئول)، گروه کامپیوتر، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران، (email: sh.bakhtiari@iaushk.ac.ir).

شهرام حیدریان، گروه ریاضی، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران، (email: heidarianshm@iaushk.ac.ir).

1. E-Health System
2. Confidentiality
3. Public Key Infrastructure
4. Public Key
5. Trusted Third Party
6. Certificate
7. Authenticity
8. Identity/ID Based Encryption
9. Biometric
10. Proxy Re-Encryption
11. Translate
12. Cipher-Text

گونه‌ای که امکان رمزگشایی[1] متن رمزشده ضمن حفظ محرمانگی برای کاربر دوم نیز فراهم باشد. از آنجا که در سیستم سلامت الکترونیک نیاز است تا اطلاعات رمزشده توسط بیمار با استفاده از شناسه هویتی تیم پزشکی در اختیار دیگر بخش‌های مجاز قرار گیرد، استفاده از پروکسی رمزنگاری مجدد در سیستم‌های سلامت الکترونیک موجب تسهیل فرایند خدمت‌رسانی به بیماران و کاهش هزینه ناشی از رمزنگاری می‌شود.

در این مقاله، یک نمونه جدید از رمزنگاری مبتنی بر هویت با هدف بهره‌مندی در پروکسی رمزنگاری مجدد مطرح خواهد شد. طرح پیشنهادی ضمن حفظ ویژگی‌های طرح‌های پیشین قابلیت به کارگیری در پروکسی رمزنگاری مجدد را دارد. نتایج ارزیابی‌های انجام‌شده در این پژوهش نشان می‌دهد که ترکیب روش پیشنهادی با پروکسی رمزنگاری مجدد موجب فراهم‌نمودن محرمانگی و کاهش هزینه در سیستم سلامت الکترونیک در فضای ابر می‌شود.

بخش‌های بعدی این مقاله بدین شرح است: در بخش دوم نوآوری پژوهش بیان می‌گردد. در بخش سوم کلیات پژوهش و مروری بر روش‌های گذشته تشریح می‌گردد. در بخش چهارم طرح پیشنهادی به همراه جزئیات آن ارائه شده و ارزیابی آن در بخش پنجم مطرح می‌شود. در بخش ششم نیز نتیجه‌گیری مقاله بیان می‌گردد.

۲- نوآوری پژوهش

با توجه به این که از یک طرف، روش‌های فعلی ارائه‌شده جهت فراهم‌کردن امنیت سیستم‌های سلامت الکترونیک، مبتنی بر زیرساخت کلید عمومی هستند که علاوه بر هزینه بالا و پیچیدگی زیاد، کاربری سیستم‌های سلامت الکترونیک را دشوار ساخته‌اند و از طرفی با روی کار آمدن رمزنگاری مبتنی بر هویت، مسایل مربوط به مدیریت گواهینامه‌های دیجیتالی و پیچیدگی زیرساخت کلید عمومی حل شده است، لذا در این پژوهش یک روش جدید رمزنگاری مبتنی بر هویت ارائه می‌شود که تنها در مرحله رمزگشایی از زوج‌سازی دوخطی استفاده می‌کند و پارامتر زوج‌سازی استفاده‌شده در فاز رمزگذاری، یک پارامتر از پیش تعیین شده است. همین امر موجب کاهش هزینه محاسبات و در نتیجه کاهش زمان اجرای الگوریتم شده است. طرح پیشنهادی، در این مفهوم و البته از نظر معماری بی‌شباهت با طرح ارائه‌شده توسط بونه و بوین در سال ۲۰۰۴ نیست اما نقطه قوت طرح ارائه‌شده، توانایی به کارگیری طرح مذکور در رمزنگاری مجدد است. از دیگر نقاط قوت طرح ارائه‌شده، کوتاه‌کردن پارامترهای ارسالی در عین حفظ امنیت طرح است به طوری که از آنجایی که طرح ارائه‌شده توسط وانگ و همکاران در سال ۲۰۱۷ بر مبنای روش رمزنگاری مبتنی بر هویت بونه و فرانکلین در سال ۲۰۰۱ است، لذا اثبات طرح در روش اوراکل تصادفی می‌باشد. در حالی که از آنجایی که مبنای طرح پیشنهادی بر اساس روش ارائه‌شده توسط بونه و بوین در سال ۲۰۰۴ است اثبات روش مذکور در مدل استاندار فراهم آمده است. این مسأله با استفاده از پیاده‌سازی بخش ارزیابی در نمودارهای جداگانه نشان داده می‌شود. سپس از ترکیب اثربخش این روش با رمزنگاری مجدد، سیستم سلامت الکترونیک ابری پیشنهاد می‌شود که ضمن فراهم‌نمودن محرمانگی، کاهش هزینه و افزایش قابلیت دسترسی را در بر دارد. همچنین در بخش ارزیابی به شبیه‌سازی ترکیب ارائه‌شده و مقایسه آن با مرتبط‌ترین پژوهش موجود با روش پیشنهادی پرداخته شده و نشان داده می‌شود که طرح پیشنهادی دارای سربار محاسباتی کمتری است.

1. Decryption

۳- کلیات پژوهش و پیشینه‌ها

در این بخش، مفاهیم رمزنگاری مبتنی بر هویت، سیستم سلامت الکترونیک، پیشینه آنها و همچنین مفهوم پروکسی رمزنگاری مجدد بیان می‌شود.

۳-۱ رمزنگاری مبتنی بر هویت و پیشینه آن

پیدایش مفهوم رمزنگاری مبتنی بر هویت در سده اخیر شکل گرفته است. در این طرح، شناسه هویتی کاربر (مانند رایانامه[2]، شماره تلفن، عوامل ژنتیکی و غیره) به عنوان کلید عمومی استفاده می‌شود. همچنین احراز هویت کاربران بر عهده مرکز تولید کلید[3] است که شناسه‌ها در آن به ثبت رسیده‌اند. مرکز تولید کلید، کلید خصوصی متناظر با شناسه هویتی را ایجاد می‌کند و به کاربران تحویل می‌دهد. همچنین چند پارامتر عمومی ایجاد می‌کند و آن را به اطلاع همه می‌رساند. کاربری که قصد ارسال پیام را دارد، پیام را با کلید عمومی گیرنده که مستقیماً از شناسه او به دست آورده و پارامترهای عمومی که مرکز تولید کلید در اختیار او قرار داده رمز می‌کند. گیرنده پیام با استفاده از کلید خصوصی خود و پارامترهای عمومی که از مرکز تولید کلید دریافت کرده است متن رمزشده را رمزگشایی می‌کند [۴]. ایده رمزنگاری مبتنی بر هویت برای اولین بار توسط شامیر[4] در سال ۱۹۸۴ به همراه اولین روش امضای دیجیتالی ارائه شد [۵]. البته شامیر موفق به ارائه رمزنگاری مبتنی بر هویت نشد تا این که بونه[5] و فرانکلین[6] در سال ۲۰۰۱ اولین ساختار عملی رمزنگاری مبتنی بر هویت را بر مبنای گروه‌های تزویج دوخطی با اثبات در مدل اوراکل تصادفی[7] ارائه کردند [۳].

این طرح به دلیل معقول‌بودن طول کلید متن رمزشده و هزینه محاسبات برای مرکز تولید، رمزگذاری و رمزگشایی به یک روش پایه برای ایجاد روش‌های رمزنگاری مبتنی بر هویت تبدیل شد. در سال ۲۰۰۳ بونه و فرانکلین رمزنگاری مبتنی بر هویت دیگری را ارائه کردند. این طرح با تغییرات اندکی نسبت به طرح اول خودشان، نظیر استفاده از تزویج دوخطی نامتقارن و بهره‌مندی از دو تابع درهم‌ساز به عنوان پارامتر عمومی مرکز تولید کلید با اثبات در مدل اوراکل تصادفی ارائه شد [۶].

در سال ۲۰۰۳ ساکای و کاساهارا[8] یک طرح رمزنگاری و امضای دیجیتالی مبتنی بر هویت را با ساختار تزویج دوخطی ارائه کردند که از لحاظ رمزگذاری و رمزگشایی و تولید کلید عملکرد مناسبی داشت [۷]. پس از آن روش‌های دیگری با ساختار نسبتاً متفاوتی ارائه شدند که در میان آنها روش ساکای و کاساهارا ۲۰۰۳ و همچنین روش بونه و بوین ۲۰۰۴ [۸] دارای کارایی بهتری بود. علت این امر استفاده‌نکردن از تزویج دوخطی در زمان رمزگذاری بود که موجب کاهش هزینه می‌شد. در سال ۲۰۰۶ جنتری یک طرح رمزنگاری مبتنی بر هویت بر پایه روش بونه و بوین ارائه داد که نیاز به محاسبه تزویج بیشتری به صورت پارامترهای از پیش محاسبه شده توسط مرکز تولید کلید داشت [۹]. طرح جنتری در مقایسه با طرح بونه و بوین دارای مقاومت بیشتری است اما نسبت به طرح ساکای و کاساهارا و نسخه بدون اوراکل تصادفی بونه و بوین کارایی

2. Email
3. Key Generation Center
4. Shamir
5. Boneh
6. Franklin
7. Random Oracle Model
8. Kasahara

کمتر و علاوه بر این، نیاز به مفروضات پیچیده‌ای دارد [۴].

بوین در سال ۲۰۰۸ پس از بررسی و مقایسه روش‌های رمزنگاری موجود نشان داد که طرح‌های رمزنگاری مبتنی بر هویتی با ساختار تزویج دوخطی کاراتر از روش‌های رمزنگاری مبتنی بر هویتی با ساختار دیگر مسایل سخت از جمله لگاریتم گسسته دریچه‌دار، باقیمانده درجه دوم و مشبّکه[1] هستند و از بین طرح‌های رمزنگاری مبتنی بر هویت با ساختار تزویج دوخطی طرح ساکای و کاساهارا و طرح بونه و بوین کاراترین روش‌های رمزنگاری مبتنی بر هویتی هستند که تا سال ۲۰۰۸ ارائه شده‌اند [۴]. در سال ۲۰۱۱ بونه و بوین سیستم رمزنگاری مبتنی بر هویت بدون اوراکل تصادفی را که در مقابل حمله شناسه انتخابی[2] مقاوم بود ارائه نمودند. در این ساختار نیازی به محاسبه تزویج دوخطی در رمزگذاری نیست و در رمزگشایی تنها نیاز به محاسبه دو تابع تزویج است [۱۰]. در سال ۲۰۱۰ گالیندو[3] طرح رمزنگاری مبتنی بر هویت با محرمانگی متن رمزشده انتخابی با اندازه متن رمزشده ثابت تحت مفروضات محاسباتی دوخطی دیفی هلمن[4] در مدل استاندارد ارائه نمود [۱۱]. در سال ۲۰۱۱ چن و همکاران طرح جدیدی از رمزنگاری مبتنی بر هویت را برگرفته از طرح بونه و بوین ۲۰۰۴ مطرح نموده‌اند [۱۲]. پارک[5] و همکاران طرح رمزنگاری مبتنی بر هویت با محرمانگی متن رمزشده انتخابی را برای به دست آوردن محرمانگی قوی در مسأله دیفی هلمن دوخطی ارائه نموده‌اند [۱۳].

سوسیلو[6] و همکاران طرح رمزنگاری مبتنی بر هویت با آستانه پویا و اندازه متن رمزشده ثابت را ارائه نمودند. در طرح آنها فرستنده با انتخاب تعداد گیرندگان متن رمزشده را با طول ثابت به نحوی فراهم می‌آورد که تنها با حضور همه گیرندگان امکان بازگشایی متن رمزشده فراهم باشد [۱۴]. در سال ۲۰۱۷ بختیاری و حسین‌زاده روش رمز مبتنی بر هویتی ارائه نمودند که علاوه بر رمزنگاری، قادر به امضای پیام نیز است. آنها روش خود را در احراز هویت بدون گواهینامه به کار بردند [۱۵]. در همان سال وانگ[7] و همکاران سیستم سلامت الکترونیک کارایی را با استفاده از طرح رمزنگاری مبتنی بر هویت ارائه نمودند [۲]. این طرح برای استفاده در پروکسی رمزنگاری مجدد بهینه شده است. طول پارامترهای عمومی زیاد و استفاده از توابع تزویج دوخطی زیاد در رمزگذاری و رمزگشایی از معایب این روش است.

الگوریتم‌های رمزنگاری مبتنی بر هویت دارای چهار مرحله به شرح زیر هستند [۴]:

۳-۱-۱ راه‌اندازی سیستم

در این مرحله با دریافت پارامتر محرمانگی k به عنوان ورودی سیستم، شاه‌کلید[8] و پارامترهای عمومی سیستم[9] به عنوان دو خروجی تولید می‌شود. کلیه کاربران سیستم از پارامترهای عمومی مطلع هستند در حالی که شاه‌کلید تنها در اختیار مرکز تولید کلید خصوصی[10] قرار دارد

$$setup() = params, msk \quad (۱)$$

۳-۱-۲ ایجاد کلید خصوصی برای کاربران

در این مرحله، مرکز تولید کلید، پارامترهای عمومی سیستم $(params)$ و شاه‌کلید msk را به همراه شناسه کاربر $ID_i \in \{0,1\}^*$ که قصد تولید کلید را برای آن دارد به عنوان ورودی، دریافت و کلید خصوصی d_i مربوط به شناسه مورد نظر را به عنوان خروجی تولید می‌کند

$$KeyGen(params, ID_i, msk) = d_i \quad (۲)$$

۳-۱-۳ رمزگذاری

در این مرحله فرستنده پیام با استفاده از پارامترهای عمومی $(params)$ و شناسه کاربری که قصد ارسال پیام به آن را دارد، متن آشکار M را رمزگذاری می‌کند. فرستنده از کلید عمومی کاربر مقصد (e_i) که مستقیماً از شناسه او به دست آمده برای رمزگذاری متن آشکار استفاده می‌کند و متن رمزشده CT با استفاده از کلید عمومی گیرنده را در خروجی تولید می‌نماید

$$Enc(params, e_i, M) = CT \quad (۳)$$

۳-۱-۴ رمزگشایی

در این مرحله گیرنده پیام پارامترهای عمومی سیستم $(params)$، کلید خصوصی مربوط به شناسه خود و متن رمزشده را به عنوان ورودی دریافت کرده و پس از رمزگشایی متن رمزشده CT، متن آشکار M را به عنوان خروجی تولید می‌نماید

$$Dec(params, CT, d_i) = M \quad (۴)$$

۳-۲ سیستم سلامت الکترونیک ابری و پیشینه آن

مفهوم e-Health (به صورت E-Health هم نوشته می‌شود) فرایند الکترونیکی و ارتباطی با هدف پشتیبانی از مراقبت‌های بهداشتی بیماران است که در سال ۱۹۹۹ معرفی شد [۱۶]. به طور کلی، تکنولوژی یکپارچه‌سازی داده‌ها به منظور تسهیل در فرایند تشخیص پزشکی، دسترسی همه‌جانبه به اطلاعات سلامت، امکان دسترسی سریع و به موقع به ارزیابی‌های دقیق علمی، افزایش کارایی ارائه خدمات بهداشت و سلامت، تسهیل انتقال و اشتراک داده‌ها در میان کلیه گروه‌های کاربران شامل بیماران، متخصصان سلامت و روابط مدیریتی، مراکز تحقیقاتی و غیره را سیستم سلامت الکترونیک گویند [۱۷]. سوابق الکترونیک سلامت (EHR)[11] نقش اساسی در سیستم‌های سلامت الکترونیک ایفا می‌کنند [۲]. پرونده الکترونیک سلامت، فرایند مکانیزه‌کردن وظایف و تکالیف واحدهای ارائه‌دهنده خدمات بهداشت و درمان است یعنی پیاده‌سازی سامانه اطلاعاتی به صورت کاملاً یکپارچه که قابلیت کاربری و استفاده در طیف گسترده‌ای از مراکز بهداشتی و درمانی را داشته باشد [۱۸].

اسناد الکترونیک سلامت یک مجموعه جامع و سازماندهی‌شده الکترونیکی داده‌ها و اطلاعات بالینی، اجتماعی و مالی است که مراقبت‌های بهداشتی و درمانی ارائه‌شده به یک فرد را مستند می‌کند [۱۹]. یکی از عمده‌ترین اهداف اجرای پرونده الکترونیک سلامت، توسعه و پیاده‌سازی یک سامانه اطلاعاتی مؤثر، کارا و منطبق بر استانداردهای خاص، اطلاعاتی، پویا و انعطاف‌پذیر در راستای مواجهه با نیازهای جدید و کاهش هزینه‌ها در همه ابعاد حوزه سلامت است [۲۰]. این اسناد توسط

1. Lattice
2. Adaptive Identity Attack
3. Galindo
4. Computational Bilinear Diffie-Hellman
5. Park
6. Susilo
7. Wang
8. Master Key
9. Public System Parameters
10. Private Key Generator
11. Electronic Health Record

پزشکان، پرستاران و مجموعه‌ای از حسگرها در شبکه حسگر بی‌سیم و مانند اینها ثبت می‌شوند. با استفاده از سیستم‌های سلامت الکترونیک، پزشکان به آسانی امکان تغییر اسناد سلامت را دارند، بیماران نیز به سادگی از طریق رابط‌های کاربری که به منظور رؤیت اطلاعات پزشکی طراحی شده به اسناد پزشکی خود دسترسی دارند. به علاوه سازمان‌های ارائه‌دهنده خدمات بهداشتی نیز می‌توانند در مواقع حیاتی به اطلاعات بیمار دسترسی پیدا کنند. این سیستم‌ها تاریخچه‌ای از سوابق پزشکی و اطلاعات حیاتی بیمار را در خود ذخیره می‌کنند که به عنوان منبع اطلاعاتی برای پزشکان، سازمان‌های ارائه‌دهنده خدمات سلامت و مراکز تحقیقاتی به حساب می‌آید. متخصصان خلاصه‌ای از رویدادهای کاربران را در اسناد سلامت الکترونیک ثبت می‌کنند. این اسناد به متصدیان بیمارستان‌ها و ارائه‌دهندگان خدمات برای بررسی عمیق‌تر وضعیت بیماران مانند آزمایشات پزشکی کمک می‌کنند.

به عنوان نمونه در گذشته زمانی که بیمار برای تشخیص بیماری خود به بیمارستان مراجعه می‌کرد پزشک می‌بایست وضعیت بدن بیمار را به طور کلی بررسی می‌کرد تا بیماری فرد را به بهترین صورت تشخیص دهد. این فرایند شامل دسته‌بندی و بررسی عکس‌ها، مراجع، اسناد پزشکی می‌شد که امری زمانبر و خسته‌کننده بود. سیستم‌های سلامت الکترونیک با انجام خودکار فرایند فوق مراحل تشخیص را تسهیل می‌کنند و موجب کاهش خطای انسانی می‌شوند [۲]. محرمانگی و حفظ حریم خصوصی از چالش‌های اصلی در گسترش سیستم سلامت به منظور ثبت سوابق سلامت بیماران به حساب می‌آید [۲۱].

در حال حاضر پیشنهادهای بسیاری در خصوص چگونگی فرایند رمزنگاری و ایجاد محرمانگی برای سیستم‌های سلامت وجود دارد که شامل استفاده از کلید متقارن و الگوی کلید عمومی و یا روش‌های مشابه شناسه ناشناس[1] و غیره است. یک باور رایج برای ایجاد محرمانگی و حفظ حریم خصوصی در سیستم‌های سلامت الکترونیک رمزنگاری اسناد سلامت الکترونیک در این سیستم‌ها است [۲]. به این ترتیب داده‌ها، شناسه‌ها (نام‌های مستعار) و کلیدهای داده‌های ویژگی (فراداده[2]) همگی قبل از ذخیره‌سازی در مرکز تصدیق و یا منبعی در فضای ابر باید رمزنگاری شوند. علاوه بر این چگونگی برقرارنمودن کنترل دسترسی و مسایل مربوط به مدیریت کلید و هزینه اجرای آن همواره از حیاتی‌ترین مسایل سیستم‌های سلامت هستند. از این رو تکنیک‌های رمزنگاری می‌توانند برای اجرای مکانیزم کنترل دسترسی امن و یا خواص مدیریت کلید مورد استفاده قرار بگیرند [۲۲] تا [۲۴]. با وجود ارائه کاربردها و قابلیت‌های رمزنگاری مبتنی بر هویت در سال‌های گذشته مقالات بسیار کمی از این تکنیک‌ها برای ایجاد محرمانگی و حفظ حریم خصوصی در سیستم‌های الکترونیکی سلامت در فضای ابر استفاده نموده‌اند. در نتیجه در این قسمت آثار نزدیک به موضوع بیان می‌شود.

بنالوه[3] و همکاران در سال ۲۰۰۹ ضمن بررسی چالش‌های حفظ حریم خصوصی بیماران در سیستم ثبت اسناد الکترونیک سلامت، بیان می‌کنند امنیت در چنین سیستم‌هایی باید از طریق رمزگذاری و کنترل دسترسی اعمال شود. آنها همچنین چگونگی استفاده از رمزنگاری برای ثبت اسناد الکترونیک پزشکی را با اطمینان از محرمانگی توسط الگویی با نام رمزنگاری کنترل‌شده توسط بیمار مطرح نمودند [۲۵]. در این طرح، بیمار قادر به تولید و ذخیره‌سازی کلید رمزنگاری است به طوری که حریم خصوصی بیماران در مرکز داده‌های رایانه‌ای به خطر نیفتد. در همین سال ژو[4] و همکاران یک سیستم احراز هویت مبتنی بر رمزنگاری مبتنی بر هویت برای حفظ حریم خصوصی شبکه‌های الکترونیکی سلامت مطرح نموده‌اند [۲۶]. در سال ۲۰۱۱ باروا[5] و همکاران طرح محرمانگی و کنترل دسترسی بیمارمحور سیستم‌های سلامت الکترونیک در فضای ابر را ارائه کردند [۲۷]. در این طرح به منظور اطمینان از حفظ حریم خصوصی اطلاعات سلامت شخصی، تکنیک EDPAC مطرح شده که سیستم را قادر می‌سازد تا درخواست‌کنندگان داده بر اساس نقش خود در سیستم دارای سطوح متفاوت دسترسی باشند.

در سال ۲۰۱۲ گوا و همکاران سیستم تأیید هویت را با حفظ محرمانگی مبتنی بر ویژگی در سیستم سلامت الکترونیک مطرح نموده‌اند [۲۸]. در این طرح برای حفظ اطلاعات شخصی بیماران در حین دریافت خدمات پزشکی چارجوبی با عنوان PAAS مطرح شده که قادر به تصدیق ویژگی کاربران در فرایند تأیید هویت کاربران در سیستم سلامت الکترونیک با قابلیت حفظ حریم خصوصی است. در سال ۲۰۱۳ لی[6] و همکاران اشتراک‌گذاری مقیاس‌پذیر و امن اسناد سلامت شخصی[7] در فضای ابر را با استفاده از روش رمزنگاری مبتنی بر ویژگی مطرح نموده‌اند [۲۹]. در این طرح، چارچوب بیمارمحور جدیدی با مجموعه‌ای از مکانیزم‌های کنترل دسترسی به داده‌ها برای ذخیره‌سازی اسناد سلامت شخصی با استفاده از تکنیک رمزنگاری مبتنی بر ویژگی در سرویس‌دهندگان نیمه‌معتمد بیان شده است. در سال ۲۰۱۶ یان[8] و همکاران طرح دسترسی جدیدی را برای تحقق‌بخشیدن به کنترل دسترسی امن به اسناد سلامتی شخصی در سیستم‌های سلامت الکترونیک بر مبنای طرح اولیه رمزنگاری مبتنی بر ویژگی مطرح کردند [۳۰].

به عنوان تنها اثر مرتبط با موضوع پیشنهادی، وانگ[9] و همکاران در سال ۲۰۱۷ طرح محرمانگی سیستم‌های سلامت الکترونیک را با تمرکز بر کاهش هزینه مطرح نموده‌اند. در این طرح، سیستم رمزنگاری مبتنی بر هویت جدیدی به منظور بهره‌وری در سیستم سلامت ارائه‌شده و چگونگی به کارگیری این طرح در جهت کاستن معایب روش‌های استفاده‌شده در سیستم سلامت الکترونیک بیان گردیده است. ولی استفاده از طرح رمزنگاری مبتنی بر هویت پیشنهادی در این طرح ضمن افزایش هزینه محاسباتی در مراحل رمزگذاری و رمزگشایی، قابلیت انعطاف‌پذیری و توسعه‌پذیری طرح را تحت شعاع قرار می‌دهد به طوری که طرح رمزنگاری مبتنی بر هویت مطرح‌شده در مقایسه با دیگر طرح‌های پیشین به مراتب پرهزینه‌تر است، با این حال، قابلیت کاربردی‌شدن در سیستم سلامت الکترونیک به عنوان نقطه عطف طرح مذکور می‌باشد.

۳-۳ پروکسی رمزنگاری مجدد

مفهوم پروکسی رمزنگاری مجدد در سال ۱۹۹۸ توسط بلیز[10] و همکاران ارائه شد [۳۱]. در این طرح، پروکسی نیمه‌معتمد با در اختیار داشتن اطلاعاتی مانند کلید رمزنگاری مجدد، متن رمزشده را با استفاده از

1. Anonymous ID Technique
2. Metadata
3. Benaloh
4. Xue
5. Barua
6. Li
7. Personal Health Records
8. Yan
9. Wang
10. Blaze

جدول ۱: شرح نمادهای به کار گرفته شده در طرح پیشنهادی.

نماد	شرح نماد
$h()$	تابع درهم‌ساز
G, G_T	گروه چرخشی
$e: G \times G \to G_T$	تابع تزویج دوخطی بر روی خم بیضوی
ID_i	شناسه هویتی مربوط به کاربر i
$msk = \{\}$	کلید مخفی اصلی، مرکز تولید کلید
g_1, g_2	پارامترهای عمومی
Z_P	گروه اول به پیمانه p
Z_p^*	گروه اولی که شامل تمام اعداد صحیح مثبت اول کوچک‌تر از p است که این گروه $p-1$ عضو دارد.
g	مولد گروه Z_p^*
d_i	کلید خصوصی مربوط به کاربر i
m	متن آشکار
CT	متن رمزشده
SE	عنصر رمزنگاری متقارن
δ	الگوی امضای دیجیتالی در زمان

کلید عمومی نماینده اول به متن رمزشده دیگری تبدیل می‌کند به طوری که امکان بازگشایی متن رمزشده توسط کلید خصوصی نماینده دوم فراهم باشد. در این طرح، پروکسی امکان دست‌یابی به متن پیام را نخواهد داشت.

٤- طرح پیشنهادی

در این بخش ابتدا طرح رمزنگاری مبتنی بر هویت جدیدی بر مبنای تزویج دوخطی، پیشنهاد و پس از آن، مدل سیستم پروکسی رمزنگاری مجدد مطابق با الگوی روش رمزنگاری پیشنهادی مطرح می‌شود.

در طرح پیشنهادی از نمادهایی استفاده می‌گردد که شرح این نمادها در جدول ۱ بیان می‌شود.

٤-۱ روش پیشنهادی رمزنگاری مبتنی بر هویت

تمرکز طرح رمزنگاری مبتنی بر هویت پیشنهادی، حفظ قابلیت انعطاف‌پذیری در به کارگیری مستقل روش، در عین برقراری تأمین امنیت در کاربردهای دیگر است. در طرح پیشنهادی با کوتاه‌شدن پارامترهای مورد استفاده در مراحل رمزنگاری و استفاده از زوج‌سازی از پیش محاسبه شده در فاز رمزگذاری، سربار محاسباتی به شدت کاهش یافته است. علاوه بر این، نقطه قوت روش پیشنهادی را می‌توان قابلیت استفاده در سیستم پروکسی رمزنگاری مجدد دانست. به این ترتیب با کاهش محاسبات تزویج دوخطی در مراحل رمزگذاری و رمزگشایی به مراتب میزان محاسبات در مقایسه با طرح‌های پیشین کاهش یافته که در نتیجه سربار محاسباتی سیستم کاهش می‌یابد.

٤-۱-۱ راه‌اندازی سیستم

ابتدا الگوریتم $\wp(1^n)$ برای به دست آوردن چندتایی (G, G_T, e) اجرا می‌شود. در این سیستم g عنصر مولد گروه دوخطی G به پیمانه p است و شناسه هویتی ID به عنوان عنصری از گروه Z_p^* فرض می‌شود. همچنین متن رمزشده به عنوان عنصری در گروه G_T در نظر گرفته می‌شود. برای تولید پارامترهای عمومی و شاه‌کلید، مرکز تولید کلید دو عدد تصادفی $a_1, a_2 \in Z_p^*$ انتخاب می‌کند. پس از آن پارامترهای عمومی سیستم و شاه‌کلید توسط مرکز تولید کلید به صورت زیر تعریف می‌شود

$$g_1 = g^{a_1} \quad (۵)$$

$$g_2 = g^{a_2} \quad (۶)$$

$$Vo = e(g, g_2) \quad (۷)$$

$$params = \{g, g_1, g_2, Vo, G, G_T, e, h\} \quad (۸)$$

$$msk = \{a_1, a_2\} \quad (۹)$$

٤-۱-۲ تولید کلید

با در اختیار داشتن پارامترهای عمومی $(params)$، شاه‌کلید msk و شناسه هویتی ID، مرکز تولید کلید عدد تصادفی r را انتخاب نموده و کلید خصوصی را به شکل زیر تولید می‌کند

$$d_{ID} = (d_1, d_2, d_3, d_4) = ((a_1 ID + a_2)^{-1}, g_1^{ID\, r}, g_1^r) \quad (۱۰)$$

٤-۱-۳ رمزگذاری

به منظور رمزکردن متن آشکار $m \in G_1$ با استفاده از شناسه هویتی $ID \in Z_p^*$، یک عدد تصادفی s انتخاب می‌شود و متن رمزشده C_T به صورت زیر محاسبه می‌گردد

$$C_T = (C_1, C_2, C_3) = ((g_1^{ID} g_2)^s, mVo^s, g^{IDs}) \quad (۱۱)$$

٤-۱-۴ رمزگشایی

کاربر نهایی به منظور رمزگشایی متن رمزشده $C_T = (C_1, C_2, C_3)$ با استفاده از کلید خصوصی خود و پارامترهای عمومی به صورت زیر عمل می‌نماید

$$M = \frac{C_2 e(C_3, d_2)}{e(C_1^{d_1}, g_2 d_2)} \quad (۱۲)$$

٤-۱-۵ اثبات درستی

اثبات درستی طرح پیشنهادی در این زیربخش بیان می‌شود

$$M = \frac{C_2 e(C_3, d_2)}{e(C_1^{d_1}, g_2 d_2)} = \frac{mVo^s e(g^{IDs}, g_1^r)}{e((g_1^{ID} g_2)^{s(a_1 ID + a_2)^{-1}}, g_2 g_1^{ID\, r})} = \frac{me(g, g_2)^s}{e(g^s, g_2)} = M \quad (۱۳)$$

٤-۲ طرح پروکسی رمزنگاری مجدد پیشنهادی

در این بخش چگونگی به کارگیری طرح رمزنگاری مبتنی بر هویت پیشنهادی در سیستم پروکسی رمزنگاری مجدد بیان می‌شود.

٤-۲-۱ راه‌اندازی سیستم

در ابتدا الگوریتم $\wp(1^n)$ برای به دست آوردن چندتایی (G, G_T, e)، اجرا و پس از آن g به طوری که مولد گروه دوخطی G به پیمانه p باشد تولید می‌شود. در ادامه الگوی امضای دیجیتالی در زمان δ و یک عنصر رمزنگاری متقارن که در اینجا با نماد SE شناخته شده انتخاب می‌گردد. همچنین سه تابع درهم‌ساز $H_1 : S \to G$، $G : \{0,1\}^* \to Z_p^*$ و $H_2 : G_T \to K$ که در آن K کلید ویژه SE است انتخاب می‌گردد [۲]. در اینجا متن رمزشده به عنوان یک عنصر در گروه G_T فرض می‌شود. اعداد تصادفی $a_1, a_2, f, f' \in Z_p^*$ برای تولید پارامترهای عمومی و شاه‌کلید انتخاب می‌شوند. پس از آن پارامترهای عمومی سیستم و شاه‌کلید توسط مرکز تولید کلید به صورت زیر تعریف می‌شود

$$g_1 = g^{a_1} \quad (۱۴)$$

$$g_2 = g^{a_2} \quad (۱۵)$$

$$Vo = e(g, g_2) \quad (۱۶)$$

$$A = g^f \quad (۱۷)$$

$$params = \{g, g_1, g_2, Vo, G, G_T, e, h\} \quad (۱۸)$$

$$msk = \{a_1, a_2, f, f'\} \quad (۱۹)$$

٤-۲-۲ تولید کلید

با در اختیار داشتن پارامترهای عمومی $(params)$،کلید مخفی اصلی msk و شناسه هویتی ID، مرکز تولید کلید اعداد تصادفی $r, r', n, n', z, \mu \in Z_p^*$ را انتخاب نموده و کلید خصوصی کاربر A را به شکل زیر تولید می‌کند

$$\begin{aligned} &r, rsk_{ID} = (d_{ID}^A, d_{ID}^B, d_{ID}^C) \\ &d_{ID}^A = (d_1, d_2, d_3, d_4, d_5, d_6) = \\ &\quad ((a_1 ID + a_2)^{-1}, g_1^{IDr}, g^{IDr}, \\ &\quad \mu + fr, g_1^n, A^r (g_1^{ID} g_2)^{-n} g^{\mu}) \\ &d_{ID}^B = (d_1', d_2', d_3') = \\ &\quad (\frac{fr'}{a_1 ID + a_2}, g_1^{n'} g^{f' ID}, A^{r'} (g_1^{ID} g_2)^{-n'}) \\ &d_{ID}^c = (d_7, d_8) = g_3^{a_1^{-1}} (g_1^{ID} g_2)^{zID}, g_1^{zID} g^{f' ID} \end{aligned} \quad (۲۰)$$

٤-۲-۳ رمزگذاری

به منظور رمزکردن متن آشکار $m \in G_T$ با استفاده از شناسه هویتی $ID \in Z_p^*$، یک عدد تصادفی s و نمونه امضای دیجیتالی در زمان با کلیدهای خصوصی/عمومی ssk و svk انتخاب می‌گردد و متن رمزشده C_{ID} به صورت زیر محاسبه می‌شود

$$\begin{aligned} &C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6) = \\ &\quad ((g_1^{ID} g_2)^s, SE.Enc(h_2(V_o)^s, m), g_1^s, h_1(svk)^s, svk, \sigma) \\ &\sigma = \delta.sig(ssk, C_1, C_2, C_3, C_4, C_5) \end{aligned} \quad (۲۱)$$

٤-۲-٤ تولید کلید رمز مجدد

گیرنده، دارای شناسه هویتی ID می‌باشد و تنها فردی است که به اطلاعات رمزشده با شناسه هویتی خود دسترسی دارد. پس از دریافت درخواست رمزگشایی از سمت کاربر دیگر با شناسه هویتی ID'، کلید رمزنگاری مجدد برای مرکز تولید کلید را ایجاد می‌کند به طوری که مرکز تولید کلید بدون این که از محتوای متن رمزشده مطلع شود، اطلاعات را با کلید رمزنگاری مجدد، رمز می‌نماید. اطلاعات رمزشده جدید قابلیت بازگشایی سطح یک و تنها توسط کلید رمزگشایی کاربر دوم را دارند. در مراحل فوق دو نکته قابل توجه است: اول این که کلید رمزنگاری مجدد $rk_{ID \to ID'}$ در بستر فراهم‌آمده توسط رمزنگاری مبتنی بر هویت برای پروکسی رمزنگاری مجدد ارسال می‌شود. دوم این که مرکز تولید کلید اطلاعاتی را مجدد رمز می‌کند که خود از محتوای آن آگاه نیست و به خطر افتادن کلید رمز مجدد، به تنهایی امنیت اطلاعات را به خطر نمی‌اندازد. علاوه بر این چون کلید رمز مجدد، تنها برای رمزنگاری مجدد طراحی شده و بر روی پیام رمزنشده کاربرد ندارد، در نتیجه دشمن نمی‌تواند تنها با داشتن کلید رمز مجدد و بدون در اختیار داشتن کلید خصوصی گیرنده پیام (کاربر A) به محتوای پیام‌ها دست یابد. برای تولید کلید رمز مجدد، گیرنده پس از انتخاب یک عدد تصادفی k، کلید رمز مجدد $rk_{ID \to ID'}$ را به صورت زیر تولید کرده و در اختیار پروکسی رمز مجدد قرار می‌دهد

$$\begin{aligned} &rk_{ID \to ID'} = (rk_1, rk_2, rk_3) \\ &rk_1 = \frac{1}{k}((d_1 d_4) ID' + d_1') = \frac{\mu ID' + f(rID' + r')}{k(a_1 ID + a_2)} \\ &rk_2 = d_5^{ID'} d_2' = g^{f' ID} g_1^{(nID' + n')} \\ &rk_3 = d_6^{ID'} d_3' = \frac{g^{f(rID' + r')} g^{f \mu ID'}}{g_1^{ID} g_2^{(nID' + n')}} \\ &rk_4 = g_1^k \end{aligned} \quad (۲۲)$$

٤-۲-۵ رمزگذاری مجدد

پروکسی رمز مجدد با در اختیار داشتن متن رمزشده $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6)_{ID}$ و پارامترهای عمومی، اقدام به رمزگذاری مجدد متن رمزشده می‌کند. نکته قابل توجه در این بخش، عدم توانایی پروکسی در رمزگشایی متن است، در نتیجه پروکسی برای اطمینان از اصالت پیام درستی زیر را بررسی می‌کند

$$\begin{aligned} &\delta Verify(C_5, C_6) = Yes \\ &e(g_1, C_4) = e(C_3, h_1(C_5)) \end{aligned} \quad (۲۳)$$

در صورت برقراری درستی تساوی (۲۳)، متن رمزنگاری مجدد به صورت زیر تولید می‌گردد و در صورت عدم برقراری درستی آن، متن دریافت‌شده دور انداخته می‌شود

$$\begin{aligned} &\hat{C}_{ID} = (C_1', C_2', C_3', C_4', C_5', C_6') = \\ &\quad (C_1, C_2, C_3, e(C_1^{rk_1}, rk_4), rk_2, rk_3) \end{aligned} \quad (۲۴)$$

٤-۲-٦ رمزگشایی سطح دوم

گیرنده پیام با در اختیار داشتن متن رمزشده $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6)_{ID}$ که با استفاده از شناسه خود او رمزشده و کلید خصوصی $sk_{ID} = (d_{ID}^A, d_{ID}^B, d_{ID}^C)$ که در آن $sk_{ID}^A = (d_1, d_2, d_3, d_4, d_5, d_6)$ است و پارامترهای عمومی، اقدام به رمزگشایی متن رمزشده می‌کند.

گیرنده جهت بررسی اصالت پیام ابتدا درستی (۲۳) را بررسی می‌کند. در صورت برقرارنبودن درستی این رابطه، پیام دور انداخته شده و در صورت برقراری (۲۳) متن رمزشده به شکل زیر رمزگشایی می‌شود

$$\begin{aligned} &K = h_2(\frac{e(C_1^{d_1}, g_2 d_2)}{e(C_3, d_3)}) \\ &m = SE.Dec(K, C_2) \end{aligned} \quad (۲۵)$$

در پایان با استفاده از خواص عنصر SE متن آشکار m تصدیق می‌گردد.

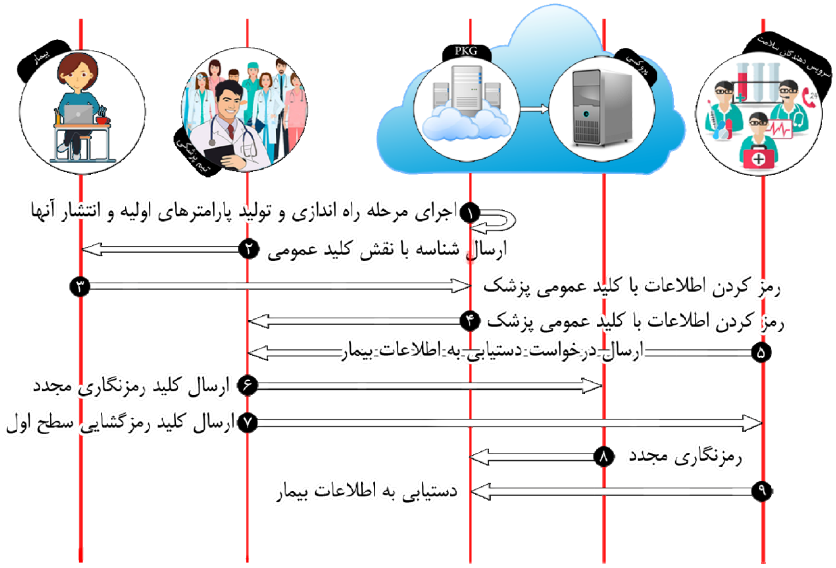
٤-۲-۷ رمزگشایی سطح یک

در این مرحله کاربر B با در اختیار داشتن پارامترهای عمومی و کلید مخفی $d_{ID}^C = (d_7, d_8)$، متن رمزشده مجدد $\hat{C}_{ID} = (C_1', C_2', C_3', C_4', C_5', C_6')$ را به صورت زیر رمزگشایی می‌کند

$$\begin{aligned} &K = h_2(\frac{e(C_1', C_5') e(C_3', C_6') e(C_1', d_7)}{C_4' e(C_1', d_8)}) \\ &m = SE.Dec(K, C_2) \end{aligned} \quad (۲۶)$$

٤-۲-۸ اثبات درستی

اثبات درستی به کارگیری روش رمزنگاری مبتنی بر هویت پیشنهادی و ترکیب آن با پروکسی رمز مجدد به صورت زیر است



شکل ۱: مدل سیستم سلامت الکترونیک پیشنهادی.

$$T=\frac{e(C_1',C_5')e(C_3',C_6')e(C_1',d_7)}{C_4'e(C_1',d_8)}=\frac{e(C_1',rk_2)e(C_3',rk_3)e(C_1',d_7)}{e(C_1^{rk_1},rk_4)e(C_1',d_8)}=$$
$$\frac{e((g_1^{ID}g_2)^s,g^{f'ID}g_1^{(nID'+n')})e(g_1^s,\frac{g^{f(rID'+r')}g^{f\mu ID'}}{g_1^{ID}g_2^{(nID'+n')}})}{e((g_1^{ID}g_2)^{s\frac{\mu ID'+f(rID'+r')}{k(a_1ID+a_0)}},g_1^k)}\times$$
$$\frac{e((g_1^{ID}g_2)^s,g_2^{a_1}(g_1^{ID}g_2)^{zID})}{e((g_1^{ID}g_2)^s,g_1^{zID}g^{fID})}=$$
$$\frac{e((g_1^{ID}g_2)^s,g^{fID}g_1^{(nID'+n')})e(g_1^s,g^{f(rID'+r')}g^{f\mu ID'})}{e(g_1^s,(g_1^{ID}g_2)^{(nID'+n')})e(g^s,g_1)^{\mu ID'}}\times$$
$$\frac{e((g_1^{ID}g_2)^s,g_2^{a_1}(g_1^{ID}g_2)^{zID})}{e(g^s,g_1)^{f(rID'+r')}e((g_1^{ID}g_2)^s,g_1^{zID}g^{fID})}=$$
$$\frac{e((g_1^{ID}g_2)^s,g^{fID})e((g_1^{ID}g_2)^s,g_2^{a_1}(g_1^{ID}g_2)^{zID})}{e((g_1^{ID}g_2)^s,g_1^{zID}g^{f'ID})}$$
$$K=h_2(T)\ ,\ m=SE.Dec(K,SE.Enc(h_2(V_o)^s,m)) \qquad (۲۷)$$

۴-۳ سیستم سلامت الکترونیک ابری پیشنهادی

همان طور که در شکل ۱ نشان داده شده است در مدل سیستم سلامت الکترونیک پنج موجودیت بیمار، تیم پزشکی، مرکز تولید کلید، پروکسی رمزگذاری مجدد و سرویس‌دهندگان سلامت به ایفای نقش می‌پردازند. با به کارگیری پروکسی رمزنگاری مجدد و ترکیب آن با ساختار طرح رمزنگاری پیشنهادی، در مدل سیستم سلامت سناریوی زیر برقرار است (لازم به ذکر است که تمامی مراحل رمزنگاری در این سناریو، مطابق با مراحل روش پیشنهادی انجام می‌شود که در بخش ۴ به طور کامل بیان شد).

در ابتدای سناریو و در مرحله ۱، مرکز تولید کلید، پارامترهای عمومی سیستم و کلید عمومی و خصوصی هر بخش را تولید کرده و در اختیار آنها قرار می‌دهد. این فرایند پس از ثبت شناسه مخاطبان در سیستم سلامت و احراز اصالت افراد صورت می‌پذیرد.

در مرحله ۲، بیمار A برای اولین بار به تیم پزشکی مراجعه می‌کند و تیم پزشکی شناسه هویتی خود را که همان کلید عمومی است برای بیمار ارسال می‌کند تا هر دو بتوانند با استفاده از روش رمزنگاری مبتنی بر هویت، بر روی یک کلید رمز متقارن جهت رمزکردن اسناد پزشکی بیمار توافق کنند.

در مرحله ۳، بیمار با استفاده از کلید متقارن توافق‌شده و رمزنگاری AES (و یا مانند آن)، اسناد سلامت الکترونیک خود را جهت فراهم‌کردن محرمانگی رمز کرده و طبق الگوی مدل سیستم، این اسناد پزشکی را به همراه کلید توافقی متقارنی که به روش مبتنی بر هویت رمز کرده است، در فضای غیر قابل اعتماد ابر برون‌سپاری می‌کند.

در مرحله ۴، هر زمان که تیم پزشکی به اسناد سلامت الکترونیک بیمار A نیاز داشته باشد اسناد رمزشده را از فضای ابری دریافت می‌کند. در این مرحله، تیم پزشکی با داشتن کلید رمز متقارن از قبل توافق شده، اسناد دریافت‌شده در مرحله ۲ را به راحتی رمزگشایی می‌کند.

در مرحله ۵ فرض می‌شود کاربر A مدتی بعد دوباره بیمار گردد و به خدمات مرکز پزشکی دیگری نیاز پیدا کند. گروه خدمات سلامت و بهداشت جامعه برای تشخیص بهتر بیماری و انجام اقدامات لازم، نیاز به اطلاعات سلامت کاربر A پیدا می‌کنند. بنابراین آنها جهت دسترسی به اطلاعات بیمار شناسه هویتی خود را برای تیم پزشکی ارسال می‌کنند.

در مرحله ۶، تیم پزشکی با داشتن کلید خصوصی متعلق به خود و همچنین شناسه هویتی گروه خدمات سلامت و بهداشت، کلید رمز مجددی را از طریق اجرای الگوریتم تولید کلید رمزمجدد در سیستم پروکسی رمز مجدد، تولید می‌کند و در اختیار پروکسی رمزنگاری مجدد قرار می‌دهد.

در مرحله ۷، تیم پزشکی علاوه بر ارسال کلید رمز مجدد به پروکسی رمزنگاری، کلید رمزگشایی متن رمزشده سطح اول را برای درخواست‌کننده اطلاعات کاربر A ارسال می‌کند.

در مرحله ۸، پروکسی رمزگذاری مجدد، کلید توافقی متقارنی را که به روش مبتنی بر هویت رمز شده و در فضای ابری قرار دارد با استفاده از کلید رمز مجددی که تیم پزشکی تولید و ارسال کرده است، مجدداً رمز می‌کند و برای استفاده گروه خدمات سلامت و بهداشت در فضای ابر ذخیره می‌کند.

در مرحله ۹، گروه خدمات سلامت و بهداشت با داشتن کلید توافقی مجدد رمزشده (همان متن رمزشده سطح اول) که پروکسی در مرحله ۸ ذخیره نموده بود و همچنین کلیدی که تیم پزشکی در مرحله تولید کلید

مجدد در اختیار آنها قرار داده است، اطلاعات پزشکی بیمار A را رمزگشایی می‌کنند.

٤-٤ اثبات امنیت طرح رمزنگاری مبتنی بر هویت پیشنهادی

با توجه به عدم وابستگی طرح پیشنهادی به پارمتر تولید توسط اوراکل تصادفی می‌توان طرح مذکور را در مدل استاندارد BDDH اثبات نمود. در این بخش مدل امنیتی IND-ID-CCA را بیان می‌کنیم. این مدل در سال ۲۰۰۱ برای اولین بار جهت اثبات امنیت روش‌های رمزنگاری شناسه‌گرا توسط بونه و فرانکلین استفاده شد. در این مدل حمله‌کننده و چالشگر[1]، بازی خاصی را در پنج مرحله انجام می‌دهند. در ادامه این بخش در ابتدا مراحل بازی بین حمله‌کننده و چالشگر بیان شده است.

بازی بین حمله‌کننده و چالشگر در مدل IND-ID-CCA در طی پنج مرحله به شرح زیر انجام می‌شود:

٤-٤-١ برپایی

در این مرحله چالشگر ورودی‌های مسئله سختی را دریافت و بر اساس آنها پارامترهای عمومی سیستم را ایجاد می‌کند و به حمله‌کننده می‌دهد.

٤-٤-٢ مرحله ١

حمله‌کننده پارامترهای عمومی سیستم را دریافت کرده و با استفاده از آنها، به صورت وفقی[2] k درخواست از چالشگر می‌پرسد، در حالی که هر یک از این درخواست‌ها یکی از پرسش‌های زیر است:

درخواست‌های تولید کلید خصوصی

حمله‌کننده از چالشگر درخواست ایجاد کلید خصوصی d_i برای شناسه‌هایی می‌نماید که خود او به صورت وفقی انتخاب می‌کند. چالشگر باید کلید خصوصی مورد نظر حمله‌کننده را ایجاد کند و در اختیار او بگذارد.

درخواست‌های رمزگشایی

حمله‌کننده از چالشگر درخواست رمزگشایی برای متن رمزشده (CT) با شناسه (ID) که توسط خود او به صورت وفقی انتخاب می‌شود، می‌کند و در نهایت چالشگر نتیجه رمزگشایی را در اختیار حمله‌کننده قرار می‌دهد.

٤-٤-٣ چالش

حمله‌کننده، کلید عمومی e_* را که متعلق به کاربری با شناسه ID_* است و دو متن آشکار m_0 و m_1 با اندازه یکسان، انتخاب و برای چالشگر ارسال می‌کند. کلید عمومی انتخابی نباید در هیچ یک از پرسش‌های مرحله ۱ وجود داشته باشد. چالشگر بیت تصادفی $\gamma \in \{0,1\}$ را انتخاب می‌کند، سپس متن رمزشده $CT^* = Enc(PP, e_*, m_\gamma)$ را ایجاد کرده و به عنوان یک چالش[3] در اختیار حمله‌کننده قرار می‌دهد.

٤-٤-٤ مرحله ٢

این مرحله شبیه به مرحله ۱ است با این تفاوت که حمله‌کننده اجازه پرسش درخواست ایجاد کلید خصوصی برای شناسه‌ای که در مرحله چالش انتخاب کرده و همچنین درخواست رمزگشایی برای متن رمزشده CT^* را ندارد.

٤-٤-٥ حدس

حمله‌کننده بیت $\gamma' \in \{0,1\}$ را حدس می‌زند و اگر $\gamma = \gamma'$ باشد بازی را برده است.

چالشگر با استفاده از بیتی که حمله‌کننده حدس زده، توانایی حل نمونه مسئله سختی را که دریافت کرده است دارد. اگر حمله‌کننده به طور تصادفی بیت جواب را تولید کند، جواب چالشگر نیز به این مسئله سخت، کاملاً تصادفی خواهد بود. اما اگر حمله‌کننده توانایی شکست طرح پیشنهادی را داشته باشد و به طریقی توانایی ایجاد جواب درست را داشته باشد، چالشگر نیز می‌تواند به مسئله سخت، جواب درست بدهد. به این حمله‌کننده، دشمن IND-ID-CCA گفته می‌شود [۹].

٤-٤-٦ مسئله دیفی- هلمن تصمیمی دوخطی[4] (BDDH)

اگر a، b و c سه عدد تصادفی در گروهی به پیمانه N و g مولد گروه باشد، حمله‌کننده A با دانستن مقادیر (g, g^a, g^b, g^c, T) نمی‌تواند مقدار $e(g,g)^{abc}$ را از مقدار تصادفی T تمیز دهد.

٤-٥ اثبات محرمانگی طرح پیشنهادی

مدل امنیتی IND-ID-CCA بر پایه یک بازی بین چالشگر و حمله‌کننده در ۵ مرحله راه‌اندازی، مرحله ۱، چالش، مرحله ۲ و مرحله حدس است. بر اساس قضیه ۱، طرح رمزنگاری پیشنهادی در برابر حمله‌کننده IND-ID-CCA امن است. در ادامه به توضیح مراحل مذکور پرداخته خواهد شد.

قضیه ۱: اگر فرضیات BDDH در چندتایی (G, G_T, e) برقرار باشد آن گاه طرح رمزنگاری مبتنی بر هویت پیشنهادی در برابر حمله‌کننده IND-ID-CCA امن است.

اثبات: فرض کنید حمله‌کننده A وجود دارد که توانایی حمله به طرح پیشنهادی را دارد. در این صورت نشان می‌دهیم ساختاری با نام الگوریتم B وجود دارد که قادر به حل مسئله BDDH در چندتایی (G, G_T, e) است. الگوریتم B چندتایی (g, g^a, g^b, g^c, T) را در اختیار دارد در حالی که T برابر با $e(g,g)^{acb}$ یا یک عدد تصادفی است. هدف الگوریتم B تولید عدد یک بیت خروجی ۱ در صورت برقراری تساوی $T = e(g,g)^{abc}$ است و در غیر این صورت تولید عدد صفر در صورتی که T برابر با یک عدد تصادفی باشد، به عنوان خروجی است. فرض کنید $a = a_1$ و $b = a_2$ باشد. الگوریتم B برای حل مسئله پیش روی با حمله‌کننده A وارد تعامل می‌شود. بازی شناسه انتخابی با اولین خروجی شناسه ID^* که حمله‌کننده A قصد حمله به آن را دارد آغاز می‌شود.

٤-٥-١ راه‌اندازی

برای تولید پارامترهای سیستم الگوریتم B با انتخاب دو عدد تصادفی a و b پارامترهای عمومی $params = \{g, g_1, g_2, Vo\}$ را تولید می‌کند و در اختیار حمله‌کننده A قرار می‌دهد.

٤-٥-٢ مرحله ١

در این مرحله حمله‌کننده A درخواست کلید خصوصی و یا رمزگشایی برای شناسه ID که خود او به صورت وقفی ایجاد کرده است را منتشر می‌کند. الگوریتم B متن رمزگشایی‌شده معتبر مربوط به متن رمزشده درخواستی حمله‌کننده و کلید خصوصی مربوط به شناسه مورد نظر حمله‌کننده را در اختیار او قرار می‌دهد.

1. Challenger
2. Adaptively
3. Challenge
4. Bilinear Decisional Diffie-Hellman

جدول ۲: مقایسه میزان نیاز به محاسبه تزویج دوخطی.

روش پیشنهادی رمزنگاری مبتنی بر هویت	نیاز به محاسبه تابع تزویج دوخطی				بهینه‌شده برای استفاده در پروکسی رمزنگاری مجدد
	سال ارائه طرح	مرکز تولید کلید	رمزگذاری	رمزگشایی	
بونه و فرانکلین [۳]	۲۰۰۱		✓	✓	
بونه و فرانکلین [۶]	۲۰۰۳		✓	✓	
ساکای و کاساهارا [۷]	۲۰۰۳	✓		✓	
بونه و بوین [۸]	۲۰۰۴	✓		✓	
جنتری [۹]	۲۰۰۶	✓		✓	
بونه و بوین [۱۰]	۲۰۱۱	✓		✓	
بختیاری و حسین‌زاده [۱۵]	۲۰۱۶		✓	✓	
وانگ [۲]	۲۰۱۷		✓	✓	✓
طرح پیشنهادی	۲۰۱۷	✓		✓	✓

٤-٥-٣ چالش

پس از ان که حمله‌کننده A تصمیم به پایان‌رساندن فاز یک می‌گیرد دو متن آشکار m_0 و m_1 را با طول یکسان و شناسه ID_* برای الگوریتم B ارسال می‌کند. سپس الگوریتم B، بیت تصادفی $\gamma \in \{0,1\}$ را انتخاب و متن رمزشده $CT_* = (g_1^{ID_*} g_2)^c, MT, g^{ID_*}$ را ایجاد می‌کند. سپس متن رمزشده CT_* را به عنوان چالش برای حمله‌کننده A ارسال می‌کند. توجه داشته باشید که الگوریتم B مقدار c را نمی‌داند اما مقدار g^c را به عنوان یکی از ورودی‌های مسئله BDDH دریافت کرده است.

٤-٥-٤ مرحله دوم

این مرحله شبیه مرحله ۱ است به غیر از این که حمله‌کننده اجازه درخواست کلید خصوصی برای شناسه ID^* و درخواست رمزگشایی را برای CT_* ندارد.

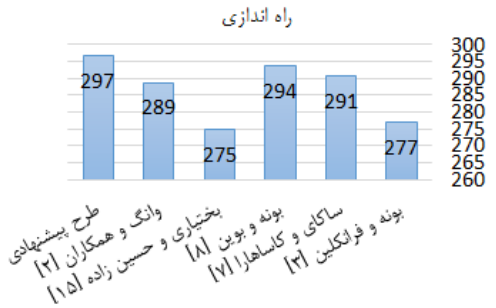
٤-٥-٥ حدس

در مرحله پایانی، حمله‌کننده A مقدار $\gamma' = \{0,1\}$ را حدس می‌زند. اگر مقدار $\gamma' = \gamma$ باشد الگوریتم B مقدار یک را به عنوان خروجی نشان می‌دهد. بدین معنی که $T = e(g,g)^{acb}$ است و در غیر این صورت مقدار صفر را نشان می‌دهد یعنی T برابر با عددی تصادفی است.

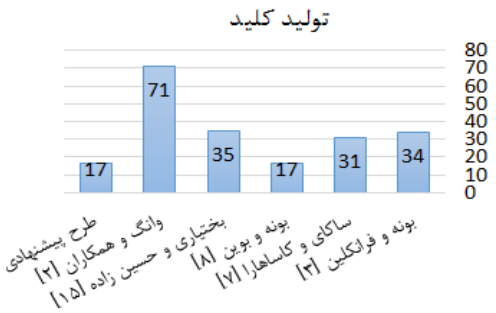
در صورت برقراری $T = e(g,g)^{acb}$، حمله‌کننده A قادر به شکست طرح پیشنهادی می‌باشد و این یعنی الگوریتم B باید وجود داشته باشد که قادر به حل مسأله سخت BDDH است. در نتیجه تا زمانی که الگوریتم B که قادر به حل مسئله سخت BDDH است وجود نداشته باشد، طرح رمزنگاری پیشنهادی دارای محرمانگی IND-ID-CCA است.

۵- ارزیابی طرح پیشنهادی

در نسخه‌های ابتدایی رمزنگاری مبتنی بر هویت با ساختار تزویج دوخطی، در هر دو مرحله رمزنگاری و رمزگشایی از تزویج دوخطی استفاده شده است در حالی که روش‌های جدید فقط برای رمزگشایی از تزویج دوخطی استفاده می‌کنند. این تغییرات باعث کاهش هزینه محاسباتی و زمان اجرای روش‌های پیشنهادی می‌شود و از این رو در طرح پیشنهادی سعی بر حفظ قابلیت مذکور با تمرکز بر بهبود آن جهت استفاده در الگوریتم پروکسی رمزنگاری مجدد شد. جدول ۲ میزان نیاز روش‌های رمزنگاری مبتنی بر هویت به اجرای تابع تزویج دوخطی در سه مرحله



شکل ۲: مقایسه زمان اجرای مرحله راه‌اندازی.



شکل ۳: مقایسه زمان اجرای مرحله تولید کلید خصوصی.

تولید کلید، رمزنگاری، رمزگشایی و مقایسه آنها با روش پیشنهادی را نشان می‌دهد.

در این بخش، زمان اجرای روش‌های رمزنگاری مبتنی بر هویت برتر با طرح پیشنهادی مقایسه می‌شود. نتایج درج‌شده حاصل از پیاده‌سازی طرح‌های مورد نظر با استفاده از کتابخانه JPBC در زبان برنامه‌نویسی جاوا [۳۲] در محیط Eclipse با استفاده از دستگاه با مشخصات Intel Core i۷ ۳٫۵ GHz و RAM ۸ GB حاصل شده است.

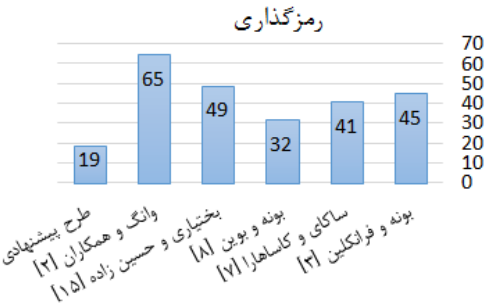
در شکل ۲، مدت زمان اجرای مرحله راه‌اندازی روش‌ها بر حسب میلی‌ثانیه نمایش داده شده است. در این بخش از شبیه‌سازی ساختار یکسانی در تولید خم بیضوی به کار گرفته شد و در تمامی روش‌های مورد ارزیابی شبیه‌سازی، از تزویج دوخطی متقارن استفاده شده است. این نوع در کتابخانه JPBC با نوع A[1] شناخته می‌شود. این بخش از سیستم که شامل تولید پارامترهای عمومی سیستم و شاه‌کلید سیستم است در یک جریان رمزنگاری تنها برای یک بار محاسبه می‌شود و در دفعات بعدی اجرای مراحل تولید کلید، رمزگذاری و رمزگشایی از پارامترهای از پیش محاسبه شده در بخش راه‌اندازی استفاده می‌شود.

شکل ۳، زمان اجرای مرحله تولید کلید خصوصی را برای کاربران سیستم در روش‌های رمزنگاری مبتنی بر هویت نمایش می‌دهد.

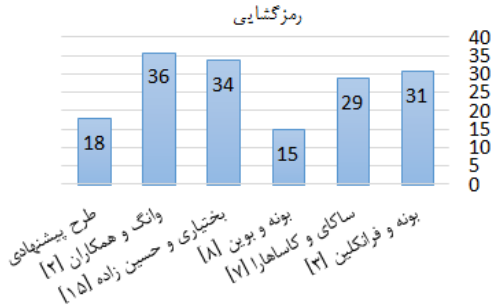
شکل ۴، زمان اجرای رمزگذاری در سیستم رمزنگاری مبتنی بر هویت را نمایش می‌دهد. در نسخه‌های ابتدایی ارائه‌شده در مرحله رمزگذاری از تابع تزویج دوخطی استفاده می‌شد. در این صورت با هر بار اجرای رمزنگاری نیاز به محاسبه توابع تزویج دوخطی وجود دارد و در نتیجه منجر به افزایش هزینه سیستم رمزنگاری مبتنی بر هویت می‌شود. اما در نسخه‌های جدیدتر، تنها در مرحله رمزگشایی از محاسبات تزویج دوخطی استفاده شده که این امر موجب کاهش قابل توجه هزینه در سیستم‌های جدید رمزنگاری مبتنی بر هویت است.

شکل ۵، زمان اجرای رمزگشایی در روش‌های مورد ارزیابی را نمایش می‌دهد.

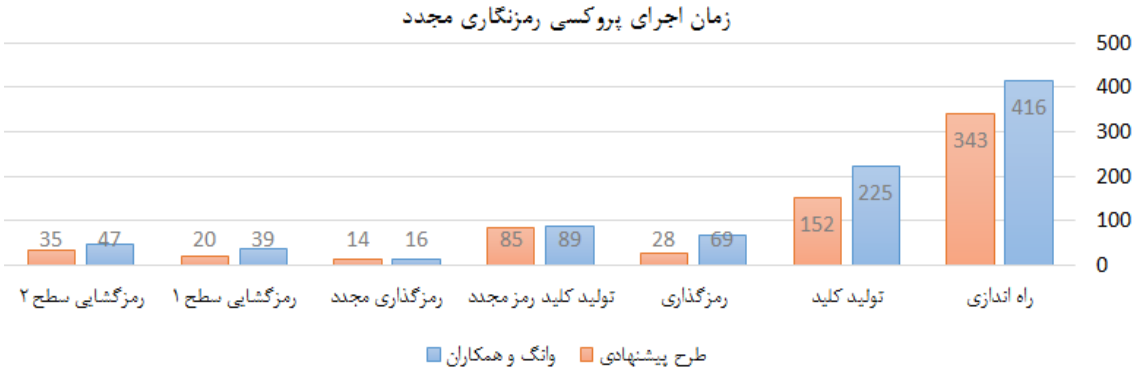
1. Type A



شکل ۴: مقایسه زمان اجرای مرحله رمزگذاری.



شکل ۵: مقایسه زمان اجرای مرحله رمزگشایی.



شکل ۶: مقایسه زمان اجرای پروکسی رمزنگاری مجدد.

همان طور که در شکل‌های ۲ و ۳ مشاهده می‌شود، روش رمزنگاری مبتنی بر هویت پیشنهادی در مرحله راه‌اندازی و تولید کلید دارای زمان اجرای مشابهی در مقایسه با طرح بونه و بوین ۲۰۰۴ [۸] است. در شکل ۴، زمان اجرای مرحله رمزگذاری نمایش داده شده است. همان طور که مشخص است طرح پیشنهادی دارای برتری ۱۳ میلی‌ثانیه در مقایسه با طرح بونه و بوین ۲۰۰۴ است.

در شکل ۵، زمان اجرای مرحله رمزگشایی در طرح‌های رمزنگاری مبتنی بر هویت نمایش داده شده است. واضح است که طرح بونه و بوین دارای برتری ۳ میلی‌ثانیه‌ای در مقایسه با روش پیشنهادی است. به این ترتیب در مجموع زمان اجرای رمزگذاری و رمزگشایی طرح پیشنهادی دارای زمان اجرای کمتری (حدود ۱۰ میلی‌ثانیه) است که باعث کاهش هزینه سیستم می‌شود. علاوه بر این روش پیشنهادی قابلیت استفاده در پروکسی رمزنگاری مجدد را دارد. در مقایسه روش پیشنهادی با روش وانگ و همکاران [۲] که دارای ویژگی‌های یکسانی با روش پیشنهادی است، تغییرات قابل توجهی در کاهش زمان اجرا در هر یک از سه مرحله تولید کلید، رمزگذاری و رمزگشایی قابل مشاهده است.

شکل ۶ زمان اجرای پروکسی رمزنگاری مجدد را با استفاده از روش رمزنگاری پیشنهادی و همچنین طرح پروکسی رمزنگاری مجدد وانگ و همکاران ۲۰۱۷ مقایسه می‌کند. همان طور که مشاهده می‌کنید بهبودهای صورت‌گرفته در روش پیشنهادی باعث بهبود زمان اجرا و کاهش میزان محاسبات و در نتیجه کاهش هزینه در طرح پروکسی رمزنگاری مجدد شده است.

۶- نتیجه‌گیری

در این مقاله تعریف مختصری از سیستم سلامت الکترونیک ارائه شد و با معرفی روش‌های رمزنگاری مبتنی بر هویت و پروکسی رمزنگاری مجدد، چگونگی استفاده از این روش‌ها در سیستم سلامت الکترونیک و بهره‌مندی از مزایای آن بیان شد. در ادامه طرح رمزنگاری مبتنی بر هویت جدیدی پیشنهاد شد. پس از آن پروکسی رمزنگاری مجدد مبتنی بر روش رمز پیشنهادی ارائه گردید و چگونگی استفاده از پروکسی رمزنگاری مجدد در مدل سیستم سلامت الکترونیک و چگونگی محرمانه‌ماندن اسناد پزشکی بیماران بیان شد. همچنین طرح پیشنهای شبیه‌سازی و نتایج حاصل با نمایندگان برتر رمزنگاری مبتنی بر هویت مورد مقایسه قرار گرفت. نتایج حاصل از شبیه‌سازی انجام‌شده نشان‌دهنده کاهش هزینه طرح پیشنهادی است. علاوه بر این، طرح پیشنهادی قابلیت به کارگیری در پروکسی رمزنگاری مجدد را دارد. مقایسه طرح پروکسی رمزنگاری مجدد مبتنی بر هویت جدید با تنها طرح ارائه‌شده در سیستم سلامت الکترونیک نشان می‌دهد که طرح پروکسی رمزنگاری مجدد مبتنی بر هویت پیشنهادی، در کلیه مراحل راه‌اندازی، تولید کلید خصوصی، رمزگذاری، تولید کلید رمز مجدد، رمزگذاری مجدد، رمزگشایی سطح ۱ و ۲ دارای زمان اجرای بهتری است که در نتیجه کاهش محاسبات در کلیه مراحل مذکور می‌باشد و منجر به کاهش هزینه محاسباتی و سربار ارتباطی در سیستم سلامت الکترونیک می‌شود.

مراجع

[1] Z. A. Khan, S. Sivakumar, W. Phillips, and N. Aslam, "A new patient monitoring framework and Energy-aware Peering Routing Protocol (EPR) for body area network communication," *J. Ambient Intell. Humaniz. Comput.*, vol. 5, no. 3, pp. 409-423, Jun. 2014.

[2] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure E-health cloud system using identity based cryptographic techniques," *Futur. Gener. Comput. Syst.*, vol. 67, pp. 242-254, Feb. 2017.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. 21st Annual Int. Cryptology Conf.*, pp. 213-229, 19-23 Aug. 2001.

[4] X. Boyen, "A tapestry of identity-based encryption: practical frameworks compared," *Int. J. Appl. Cryptogr.*, vol. 1, no. 1, pp. 3-21, Feb. 2008.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. of CRYPTO 84 on Advances in Cryptology*, vol. 84, pp. 47-53, Santa Barbara, CA, USA, 1984.

[6] D. A. N. Boneh and M. Franklin, "Downloaded 12/27/12 to 138.26.31.3. Redistribution subject to SIAM license or copyright, see http://www.siam.org/journals/ojsa.php," vol. 32, no. 3, pp. 586-615, 2003.
[7] R. Sakai and M. Kasahara, "ID based cryptosystems with pairing on elliptic curve," *IACR Cryptol. ePrint Arch.*, Article 54, 2003.
[8] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in *Proc. Int. Conf. on the Theory and Applications of Cryptographic Techniques*, pp. 223-238, Aarhus, Denmark, 22-25 May 2005.
[9] C. Gentry, "Practical identity-based encryption without random oracles," in *Proc. Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, pp. 445-464, St. Petersburg, Russia, 28 May-1 Jun. 2006.
[10] D. Boneh and X. Boyen, "Efficient selective identity-based encryption without random oracles," *Journal of Cryptology*, vol. 24, no. 4, pp. 659-693, Oct. 2011.
[11] D. Galindo, "Chosen-ciphertext secure identity-based encryption from computational bilinear Diffie-Hellman," in *Pairing*, pp. 367-376, 2010.
[12] Y. Chen, S. Luo, J. Hu, and Z. Chen, "A novel commutative blinding identity based encryption scheme," in *Proc. Int. Symp. on Foundations and Practice of Security*, pp. 73-89, Paris, France, 12-13 May 2011.
[13] J. H. Park, K. Lee, and D. H. Lee, "New chosen-ciphertext secure identity-based encryption with tight security reduction to the bilinear Diffie-Hellman problem," *Inf. Sci.*, vol. 325, pp. 256-270, 20 Dec. 2015.
[14] W. Susilo, F. Guo, and Y. Mu, "Efficient dynamic threshold identity-based encryption with constant-size ciphertext," *Theor. Comput. Sci.*, vol. 1, no. 1, pp. 49-59, Jan. 2015.
[15] S. Bakhtiari-Chehelcheshmeh and M. Hosseinzadeh, "A new certificateless and secure authentication scheme for ad hoc networks," *Wirel. Pers. Commun.*, vol. 94, no. 4, pp. 2833-2851, Jun. 2017.
[16] V. Della Mea, "What is e-Health (2): the death of telemedicine?," *J. Med. Internet Res.*, vol. 3, no. 2, Article 22, Apr.-Jun. 2001.
[17] H. Lohr, A. R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proc. of the 1st ACM Int. Health Informatics Symp.*, *IHI'10*, pp. 220-229, Arlington, VA, USA, 10-11 Nov. 2010.
[18] W. T. Riley, *et al*., "Health behavior models in the age of mobile interventions: are our theories up to the task?," *Transl. Behav. Med.*, vol. 1, no. 1, pp. 53-71, Mar. 2011.
[19] R. Istepanian, S. Laxminarayan, and C. S. Pattichis, *M-Health*, Springer, 2014.
[20] H. Yan, H. Huo, Y. Xu, and M. Gidlund, "Wireless sensor network based e-health system-implementation and experimental results," *IEEE Trans. Consum. Electron.*, vol. 56, no. 4, pp. 2288-2295, Nov. 2010.
[21] J. O'donoghue and J. Herbert, "Data management within mHealth environments: patient sensors, mobile devices, and databases," *J. Data Inf. Qual.*, vol. 4, no. 1, Article 5, Oct. 2012.
[22] L. Neuhauser and G. L. Kreps, "Online cancer communication: meeting the literacy, cultural and linguistic needs of diverse audiences," *Patient Educ. Couns.*, vol. 71, no. 3, pp. 365-377, Jun. 2008.
[23] L. Neuhauser and G. L. Kreps, "E-health communication and behavior change: promise and performance," *Soc. Semiot.*, vol. 20, no. 1, pp. 9-27, 2010.
[24] G. L. Kreps, "Strategic use of communication to market cancer prevention and control to vulnerable populations," *Health Mark. Q.*, vol. 25, no. 1-2, pp. 204-216, 2008.
[25] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *Proc. of the ACM Workshop on Cloud Computing Security*, *CCSW'09*, pp. 103-114, Chicago, IL, USA, 13- 13 Nov. 2009.
[26] Y. Xue, X. Mao, Y. Guo, and S. Lv, "The research advance of facial expression recognition in human computer interaction," *J. Image Graph.*, vol. 5, pp. 764-772, 2009.
[27] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: enabling security and patient-centric access control for e-health in cloud computing," *Int. J. Secur. Networks*, vol. 6, no. 2-3, pp. 67-76, Nov. 2011.
[28] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: a privacy-preserving attribute-based authentication system for ehealth networks," in *Proc. IEEE 32nd Int. Conf. on Distributed Computing Systems, ICDCS'12*, pp. 224-233, Macau, China, 18-21 Jun. 2012.
[29] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131-143, Jan. 2013.
[30] H. Yan, J. Li, X. Li, G. Zhao, S. Y. Lee, and J. Shen, "Secure access control of E-health system with attribute-based encryption," *Intell. Autom. Soft Comput.*, vol. 22, no. 3, pp. 345-352, 2016.
[31] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proc.* 5th Int. Conf. on *Applied Cryptography and Network Security*, pp. 288-306, Zhuhai, China, 5-8 Jun. 2007.
[32] A. De Caro, V. Iovino, and A. Renato, *JPBC : Java Pairing Based Cryptography*, pp. 850-855, 2011.

مجید علی‌پور در سال ۱۳۹۰ مدرک کارشناسی مهندسی تکنولوژی‌های سخت افزار رایانه خود را از دانشگاه جهاد دانشگاهی شعبه اصفهان و در سال ۱۳۹۶ مدرک کارشناسی ارشد مهندسی نرم افزار کامپیوتر خود را از دانشگاه آزاد واحد شهرکرد دریافت نمود. از سال ۱۳۸۹ الی ۱۳۹۸ نام‌برده به عنوان کارشناس سیستم‌های سخت افزاری در موسسه سام کلینیک به کار مشغول بوده و درسال ۱۳۹۸ ایشان در مرکز تکنونیک مشغول به کار می‌باشد. زمینه‌های علمی مورد علاقه وی متنوع بوده و شامل موضوعاتی مانند طراحی بردهای الکترونیک هوشمند، سیستم‌های رباتیک و سیستم‌های رمزنگاری مبتنی بر مشبّکه و ابر می‌باشد.

شقایق بختیاری چهل‌چشمه تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد کامپیوتر به‌ترتیب در سال‌های ۱۳۸۵ و ۱۳۸۷ از دانشگاه آزاد اسلامی واحد نجف آباد و دکتری نرم‌افزار کامپیوتر در سال ۱۳۹۵ از دانشگاه علوم و تحقیقات تهران به پایان رسانده است و هم‌اکنون استادیار دانشکده مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد شهرکرد می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: رمزنگاری، امنیت داده، سایر پروتکل‌های امنیتی از قبیل احراز هویت، سیستم‌های پرداختی، شبکه‌های کامپیوتری و پایگاه داده پیشرفته.

شهرام حیدریان در سال ۱۳۷۵ مدرک کارشناسی ریاضی محض خود را از دانشگاه پیام نور شهرکرد و در سال ۱۳۷۸ مدرک کارشناسی ارشد ریاضی خود را از دانشگاه صنعتی اصفهان دریافت نمود و از سال ۱۳۷۹ تاکنون به عنوان عضو هیأت علمی دانشگاه آزاد شهرکرد مشغول به کار است. وی در سال ۱۳۸۵ دوره دکتری ریاضی را در دانشگاه کاشان آغاز و در سال ۱۳۸۹ از این دانشکاه با دریافت مدرک دکتری ریاضی در نظریه گروه‌ها فارغ التحصیل شد. زمینه‌های تحقیقاتی مورد علاقه ایشان نظریه گروه‌های نامتناهی و نظریه گراف می‌باشند.