دوفصلنامه محاسبات و سامانه های توزیع شده
سال پنجم، شماره۲، شماره پیاپی ۱۰، صفحه ۴۳ تا ۴۸، سال ۱۴۰۱

رمزگذاری و احرازهویت ایمن مبتنی بر مشبکه

فرشته حیدری
دانشکده علوم پایه، دانشگاه شاهد، تهران، ایران

چکیده

با تکامل اینترنت اشیا، تبادل اطلاعات همراه با رمزگذاری ایمن صورت می گیرد. با توجه به توسعه ی کامپیوتر های کلاسیک به کامپیوتر های کوانتومی در آینده ی نزدیک و به دنبال آن ظهور حملات کوانتومی، نیاز به رمزگذاری ایمن اطلاعات و حفظ امنیت در برابر آن افزایش یافت. در این پژوهش ضمن معرفی مشبکه ها، طرح دقیق و جامع رمزگذاری مبتنی بر مشبکه NTRU که طراحی کامل رمزگذاری و رمزگشایی آن سال ها به طول انجامید می پردازیم و ارایه کاملی از ترسیم هندسی رمزگذاری NTRU، تولید کلیدعمومی، خصوصی و رمزگشایی آن انجام می شود. در ادامه احراز هویت مبتنی بر مشبکه و چگونگی اثبات امنیت اطلاعات رمزگذاری شده در برابر حملات کوانتومی و سرعت رمزگذاری و رمز گشایی طرح نسبت به طرح های معرفی شده مشابه نتیجه می شود.

کلمات کلیدی: رمزگذاری، مشبکه، امنیت.

Secure Lattice-based Encryption And Authentication

Fereshte Heydari.

Shahed University, Tehran, Iran.

Abstract

With the evolution of the Internet of Things, the exchange of information is accompanied by secure encryption. Due to the development of classical computers to quantum computers in the near future and the emergence of quantum attacks, the need to securely encrypt information and maintain security against it has increased. In this research, along with the introduction of lattices, the detailed and comprehensive encryption plan based on the NTRU lattice, the complete design of the encryption and decryption of which took years, and a complete presentation of the geometric drawing of the NTRU encryption, public and private key generation, and its decryption are made. In the following, network-based authentication and how to prove the security of encrypted information against quantum attacks and the speed of encryption and decryption of the plan compared to the similar introduced plans are concluded.

تاریخچه مقاله:

تاریخ ارسال: ۱۴۰۱/۹/۱۷
تاریخ اصلاحات: ۱۴۰۱/۱۱/۲۵
تاریخ پذیرش: ۱۴۰۱/۱۲/۲۵
تاریخ انتشار: ۱۴۰۱/۱۲/۲۹

Keywords:

Encryption, Lattice, Security

*ایمیل نویسنده مسئول:
Fereshteh.heydari216@gmail.com

۱ – مقدمه

طراحی سنتی شبکه های حسگر بی سیم، سیستم های کنترل و سایر موارد همگی به امکان دسترسی به اینترنت در همه اشیا کمک می کنند. با تکامل اینترنت اشیا، به اشتراک گذاری متقابل اطلاعات در میان دستگاه های هوشمند مختلف در سراسر جهان آسان می شود[10]. اینترنت اشیا به طور فزاینده ای در حال تبدیل شدن به یک سرویس رایانه ای فراگیر است که به حجم گسترده ای از ذخیره سازی و پردازش داده ها نیاز دارد. تکامل اینترنت زمینه را برای فناوری های مختلف جدیدی از جمله محاسبات کوانتومی و اینترنت اشیا برای ارائه کیفیت خدمات به کاربران فراهم کرده است. به دلیل ویژگی های منحصر به فرد محدودیت منابع، خود سازماندهی و ارتباط کوتاه برد در اینترنت اشیا، برای ذخیره سازی و محاسبه به ابر متوسل می شود که این امر تهدیدات امنیتی و حریم خصوصی چالش برانگیزی را ایجاد کرده است. ابر عمومی یک موجود نا امن است و ذخیره داده ها در آن به صورت متن پیام خطرناک است زیرا می توان از طریق یک مهاجم بر روی ابرهای عمومی شانس زیادی برای شنود را ایجاد کرد[1]. بنا براین با اعمال مکانیزم های رمزگذاری این دسترسی باید محدود شود.

با توجه به اینکه در رمزگذاری داده همواره امنیت، سرعت انتقال و ساده بودن محاسبات کلید از اهمیت بالایی برخوردار است، سعی بر آن شده تا حد مطلوبی این نیاز برطرف شود. رمز گذاری مبتنی بر مشبکه را نمی توان در زمان چند جمله ای حتی با یک کامپیوتر کوانتومی رمزگشایی کرد و در برابر حملات سایبری سنتی شناخته شده مقاومتی ثابت شده دارد[2].

۲ – پیشینه تحقیق

علم رمزنگاری از دیرباز مورد توجه بود و امروزه با توسعه کامپیوتر ها و انتقال اطلاعات بیش از پیش مورد اهمیت قرار گرفته است. ابتدایی ترین شکل آن رمزگذاری کلید خصوصی(متقارن) که یک کلید خصوصی میان طرفین توافق شده و اطلاعات بوسیله ی آن رمز شده و منتقل می شود و در انتها رمزگشایی می شود. در رمز گذاری کلید عمومی(نامتقارن)، کلید مجزای خصوصی برای رمزگشایی و کلید عمومی برای رمزگذاری استفاده می شود[7]. محققان در گذشته برای تأمین امنیت در حوزه های مختلف مانند شبکه هوشمند و تأیید اعتبار برچسب های RFID مورد استفاده قرار گرفته اند. برخلاف رایانه های کلاسیک قدیمی که بیت ها در هر حالت ۰یا۱ نشان داده می شوند، طراحی رایانه کوانتومی به گونه ای است که از بیت ها در حالت کوانتوم استفاده می کند (معروف به کیوبیت). این کیوبیت ها ترکیبی از ۰ و ۱ بیت قدیمی است که هم زمان کار می کنند. علاوه بر این فقط یک جهت چرخش، عمودی یا افقی، برای شناسایی بیت ها انتخاب می شود. درکنار سرعت، نیاز به امنیت شدید یک نگرانی عمده در عصر کامپیوتر های کوانتومی است که با کمک رمزنگاری مبتنی بر مشبکه می توان اطمینان حاصل کرد. این روش پسا کوانتومی برای امنیت رمزگذاری کلید عمومی مناسب است که مبتنی بر مشبکه ساخته شده است. این رمزگذاری در برابر حملات رایانه ای کلاسیک و کوانتومی انعطاف پذیر است.

مشبکه ازقرن هجدهم در ریاضیات استفاده شده است. هر زیرگروه جمعی گسسته در R^n با عمل جمع را یک مشبکه می‌نامند.

نگاشت خطی π به صورت زیر است:

$$\pi : \quad \mathbb{Z}_q{}^n \rightarrow \quad = \frac{\mathbb{Z}_q[x]}{\langle x^n-1\rangle}$$

$$(a_0,a_1,\dots,a_{n-1}) \rightarrow \ a_0 + a_1x + \dots + a_{n-1}x^{n-1}$$

زیر مجموعه ناتهی از $F \subseteq \mathbb{Z}_q^n$ مشبکه ایده آل است هرگاه $\pi(F)$ ایده آلی ازحلقه ی خارج قسمتی $\frac{\mathbb{Z}_q[x]}{\langle x^n-1\rangle}$ باشد.

فرض کنید $h(x)=h_{n-1}x^{n-1}+ \dots + h_0$ باشد. اگر $r(x)=x^n - 1$ آنگاه ماتریس چرخشی به صورت زیر محاسبه می شود:

ستون اول و ستون دوم ماتریس عبارت است از نمایش $x^0h(x)$ و $xh(x)$ برحسب پایه ی مرتب B به شرح

$x^0h(x)=h_{n-1}x^{n-1}+ \dots + h_0$

و

$xh(x)=h_{n-1}x^n+h_{n-2}x^{n-1}+\dots+h_0x = h_{n-2}x^{n-1}+\dots+h_0x +h_{n-1}$

و بدین ترتیب سایر ستون های ماتریس $\varphi(h)$ تا ستون n ام که ضرایب x درضرب x^n در $h(x)$ در پیمانه n ساخته می شود. بیشترین درجه مجاز برای x، $n-1$ است.

$x^i h(x)$ به ازای $0 \le i \le n-1$ برحسب پایه ی مرتب B می نویسیم و به ترتیب درماتریس $\varphi(h)$ قرار می دهیم. نمایش ماتریس به صورت

$$\begin{bmatrix} h_0 & \cdots & h_1 \\ \vdots & \ddots & \vdots \\ h_{n-1} & \cdots & h_0 \end{bmatrix}$$

در دهه ۹۰ از یک روش رمزگذاری مبتنی بر ویژگی ABE برای ذخیره سوابق سلامت بیماران در سرورهای نیمه ابری استفاده کردند. با این حال، معایب کلی استفاده از طرح های ABE این است که از عملیات با هزینه محاسبه بالا استفاده می کنند[6].

در اوایل ۲۰۰۰محققانی مانند رگو[1] و میکیانسیو[2] کارهای نظری اولیه را با به دست آوردن ضمانت های امنیتی بسیار قوی تر و کارآیی چشمگیر بهبود بخشیدند. پس از آن چندین محقق یک جعبه ابزار شگفت آور غنی از ساختارهای رمزنگاری مبتنی بر مشکبه ساخته اند، از جمله اشیا قدرتمند مانند طرح های امضا، هویت و ویژگی های رمزگذاری، رمزگذاری تماماً هوموروفیک و موارد دیگر.

۳- معرفی رمزگذاری طرح

رمزگذاری مبتنی بر مشبکه در حال حاضر کاندیدای مهم رمزگذاری پس از کوانتوم می باشد. برخلاف طرح های کلید عمومی پرکاربرد و شناخته شده مانند RSA، دیفی هلمن یا سیستم های رمزگذاری منحنی بیضوی، که از نظر تئوریک به راحتی توسط یک کامپیوتر کوانتومی مورد حمله قرار می گیرند، به نظر می رسد برخی از ساختارهای مبتنی بر مشبکه در برابر حمله رایانه های کلاسیک و کوانتومی مقاوم هستند. علاوه بر این، بسیاری از سازه های مبتنی بر مشبکه با این فرض که برخی از مسائل مشبکه محاسباتی کاملاً مطالعه شده را نمی توان به طور کارآمد حل کرد، ایمن در نظر گرفته می شوند[9].

طرح رمزگذاری مبتنی بر مشبکه یNTRUبه یک رمزگذاری کلید عمومی مبتنی بر حلقه بستگی دارد[11][3]. ابتدا مرحله ی راه اندازی طرح است که با انتخاب پارامتر های مدنظر همراه است که در مرحله ی تولید کلید با استفاده از این پارامتر ها ساخت کلید انجام می شود.

در مرحله ی تولید کلید، الگوریتم اقلیدسی توسعه یافته یک روش کارآمد برای محاسبه وارون ضربی است. الگوریتم اقلیدسی توسعه یافته که در کنار محاسبه ی بزرگترین تقسیم کننده مشترک (gcd) اعداد صحیح a و b ، ضرایب قضیه ی بزو را نیز محاسبه می کند که $a\,x + b\,y = gcd\,(a,b)$ می باشد.

در حالت خاص اگردو عدد a و b نسبت به هم اول باشند داریم $ax+by=1$ که اگر به پیمانه bکاهش دهیم،$ax \equiv 1 \pmod b$ می باشد. در ابتدا مرکز تولید کلید(KGC) پارامترهای امنیتی را بر اساس بردارهای چند جمله ای مشبکه ای به عنوان ورودی انتخاب می کند. این پارامترها بین KGC و پایگاه داده (DS) برای شروع نشست به اشتراک گذاشته می شوند. مجموعه چند جمله ای های استفاده شده در مراحل رمزگذاری و رمزگشایی $\{k\ (x), g(x), m\ (x), r\ (x)\}$است. توجه داریم که بر اساس پارامترهای امنیتی تعریف شده در مرحله راه اندازی، مرحله تولید کلید شروع می شود.

مشبکه های حلقه ای چند جمله ای هایR_p, R و R_q به شکل $R=\frac{\mathbb{Z}\,[x]}{\langle x^s-1\rangle}$, $R_p=\frac{\mathbb{Z}_p\,[x]}{\langle x^s-1\rangle}$, $R_q=\frac{\mathbb{Z}_q\,[x]}{\langle x^s-1\rangle}$ تعریف می شود. اعداد صحیح s , p , q و مجموعه چندجمله ای های $\{k\ (x), g(x), m\ (x), r\ (x)\}$ با درجه حداکثر (s-1) را انتخاب کرده که در آنs یک عدد اول است و pرا به گونه ای انتخاب می کنیم که $k(x),p)=1$ وq توانی از ۲ به طوری که $q> p$ و $gcd\ (s,p) = 1$ و $gcd\ (q,p) = 1$و $k(x),p)=1$است. سپس در مرحله تولید کلید، مرکز تولیدکلید KGC زوج کلید عمومی و خصوصی را تولید می کند که با DS به اشتراک گذاشته می شود.

حال با استفاده از الگوریتم توسعه یافته اقلیدسی محاسبه مقدار $k_p(x)$ به شرح زیر است:

$$(k(x),p)=1 \rightarrow k\ (x)\ k_p(x) = 1 \pmod p$$
$$k\ (x) = k_p^{-1}(x) \pmod p$$

و $k_p\ (x) = k^{-1}\ (x) \pmod p$ می باشد. با استفاده از همین روش $k_q(x)$ را به صورت $k_q(x) = k^{-1}(x) \pmod q$ محاسبه می کنیم.

محاسبه ی کلید عمومی به شرح زیر است :

$$h(x) =[pk_q(x)g(x)](\text{mod } q)=[pk^{-1}\ (x)g(x)](\text{mod } q)$$

(فرمول-۱):

که در آن $h(x)$ چند جمله ای به پیمانه q است.

کلید خصوصی نیزعبارت است از $\{k\ (x)\ ,\ g(x)\}$که هرکدام دارای ضرایب{۰،۱،-۱}می باشد. با تایید اعتبار کاربر توسط شنونده مورد اعتماد (TPA) پس از دریافت کلید عمومی، DS پارامترهای ورودی را به عنوان پیام $m(x)$ انتخاب می کند و آن را با چند جمله ای تصادفی$r(x)$ ادغام می کند. از آن جا که حسگرهای مختلف انواع مختلفی از داده (یا پیام) را تولید می کنند، $m\ (x)$ ابتدا به قالب باینری تبدیل شده است. متن رمز شده سپس با استفاده از پارامترهای ورودی و کلید عمومی به صورت زیر محاسبه می شود.

پارامترهای ورودی $m\ (x)$ و $r(x)$ بردارهای چند جمله ای هستند. با درجه حداکثرp-1 که$m(x)\in R_p$ و $r(x)\in R_p$ است. متن رمزشده

$$t\ (x) = [m\ (x) + r(x)h\ (x)] \pmod q$$ **(فرمول-۲):**

می باشد.

[1] Regev

[2] Micciancio

داده های رمزگذاری شده$t(x)$در فضای ابر ذخیره می شود. هنگامی که کاربر درخواست جدیدی برای دسترسی به داده ها می فرستد، KGC زوج کلیدخصوصی را ازطریق یک کانال امن (/ SSL TLS) به DSمی فرستد و متن پیام مدنظر رمزگشایی می شود.

۵_۳_رمزگشایی:

پس از تایید اعتبار کاربر که توسط TPA این کار صورت می گیرد، درخواست رمزگشایی توسط کاربر به KGC ارسال می شود و با تولید کلید خصوصی درخواست رمز گشایی همراه با کلید خصوصی به DS ارسال می شود. پیام ارسال شده $t(x)$ از کاربر پس از ارسال به DS در فضای ابر دخیره می شود و سپس DS پیام متن اصلی را با استفاده از پارامترهای ورودی $t(x)$، $k(x)$ و زوج کلید خصوصی محاسبه می کند. درنهایت، داده های متن اصلی بهKGCارسال می شود که اجازه دسترسی داده را از طریق کانال امن همراه با پیام اصلی به کاربر ارسال می کند.

الگوریتم رمزگشایی، $t(x)$ را به عنوان ورودی دریافت می کند و$m(x) = k(x)t(x) \pmod q$ را محاسبه می کند و قرار می دهیم $a(x) = k(x)t(x) \pmod q$ و اکنون نشان می دهیم $a(x)$ همان پیام اصلی$m(x)$ است. با استفاده از تعریف

(فرمول-۳): $a(x) = k(x)[m(x)+ r(x)\, h(x)] \pmod q$

و

(فرمول-۱): $h(x) = [p\, k_q(x)\, g(x)] \pmod q$

نتیجه می گیریم

$$a(x)=k_q(x)t(x)(\mathrm{mod} q)$$
$$=k_q(x)(m(x)+h(x)r(x))(\mathrm{mod}\ q)$$
$$= k_q(x)m(x) + pg(x)r(x)(\mathrm{mod} q)$$

بنابراین بردار $a(x)$برابر$k_q(x)m(x) + pg(x)r(x)$ و

$$a(x)=k^{-1}(x)(k_q(x)m(x)+pg(x)r(x))\ (\mathrm{mod} p) = m(x)(\mathrm{mod}\ p)$$

(فرمول-۴):

در رمزگذاری معرفی شده به دلیل ضرب های چند جمله ای با درجهs، متن های رمزدار با طول بیشتر را ایجاد می کند. از این رو برای کاهش بار اضافی بر منابع شبکه، مقدار s در طرح پیشنهادی کوچک نگه داشته شده است. با این حال می توان این مقدار را افزایش داد تا متن رمز پیچیده تری ایجاد کند، بدین ترتیب شکستن متن رمز برای یک مهاجم دشوار است[8].

۴- معرفی تعبیر هندسی رمزگذاری طرح

کلیدخصوصی درطرح NTRU توسط بردارکوتاه v ارائه شده است که با روش کاهش مشبکه یا روش ترکیبی آن را بدست می آوریم. مشبکه ی مربوط به v شامل کوچکترین مشبکه دو-دوری شامل v می شود. یک مولد برای این مشبکه باتمام چرخش های دوتایی$(i = 0, \dots, n-1)\ \mathrm{rot}^{i}_{2}(v)$ و تمام بردارهای به شکل $(i = 0, \dots, 2n-1)\ qe_i$ بدست می آید.

کلید عمومی در پایه ی HNFکه با روش حذف گاوسی محاسبه می شود، مشبکه qپیمانه ای دو-دوری است که توسط v تولید شده است. جالب است که اگر $v=[pg^T\ k^T]^T$ آنگاه کلید عمومی به صورت $H=\begin{bmatrix} qI & M_h \\ 0 & I \end{bmatrix}$است. به عبارت دیگر مشبکه می تواند به عنوان کوچکترین مشبکه ی q پیمانه ای دو-دوری شامل $[h^T, e_1^T]$ در نظر گرفته شود.

پیام ورودی به صورت بردار $m \in \{-1, 0, 1\}^n$ به همراه بردار تصادفی $r \in \{-1, 0, 1\}^n$ به صورت بردار $[m^T, -r^T]^T$در نظر می گیریم. حال با توجه به ساختار اصلی تعریف شده رمز گذاری یعنی، $t=(m+hr)\ (\mathrm{mod}\ q)$رمزگذاری به صورت

$$R=[0, r^T]^T, M=[m^T,-r^T]^T, H=\begin{bmatrix} qI & M_h \\ 0 & I \end{bmatrix}$$

پارامترگذاری می شود. بنابراین

$$T=\begin{bmatrix} m \\ -r \end{bmatrix}+\begin{bmatrix} qI & M_h \\ 0 & I \end{bmatrix}\begin{bmatrix} 0 \\ r \end{bmatrix}=\begin{bmatrix} m \\ -r \end{bmatrix}+\begin{bmatrix} M_{hr} \\ r \end{bmatrix}$$

(فرمول-۵):

که با توجه، $t=(m+hr)\ (\mathrm{mod}\ q)$ برابر با$[t^T, 0^T]^T$ است.

متن رمزگذاری شده t با ضرب آن در ماتریس M_k در پیمانه q، رمزگشایی می شود که عبارت است از

$$M_k\, t \pmod q = M_k\, m + M_k\, M_h\, r \pmod q$$
$$= M_k\, m + M_g\, r \pmod q$$

حال با کاهش عبارت $M_k\, m + M_g\, r$ در$\mathrm{mod}\ p$ داریم

(فرمول-۶): $M_k\, m + M_g\, r \pmod p = I.m+O.r=m$

بدین ترتیب پیام اصلی m بازیابی می شود.

۵-احرازهویت افراد برای برقراری ارتباط با یکدیگر

قبل از ارسال پیام با مشخص کردن فرد یا نهادی تحت عنوان شنونده ی مورد اعتماد می توان اطلاعات افراد شرکت کننده برای دریافت یا ارسال پیام را قرارداد. به طور کلی هدف معرفی و طراحی احراز هویت کاربر ارزیابی آن است و رمزگذاری هیچ گونه اصالت پیام از فرد اصلی ارسال کننده را تضمین نمی کند[12]. مراحل احراز هویت شامل ۴ مرحله میان کاربر و شنونده مورد اعتماد می باشد. در ابتدا پارامتر های کاربر را تعیین می کنیم. فرض می کنیم Gگروه ضربی و g مولد آن است. L مشبکه ی p ترکیب خطی بردار های مستقل به صورت $\{a_0x^0, a_1x^1, \dots, a_{p-1}x^{p-1}\}$ که a_i ها متعلق به $\mathbb{Z}_p$ هستند. کاربر کلید خصوصی a_xرا انتخاب می کندکه برحسب رمزکاربر می باشد. کاربر با استفاده از کلید

خصوصی a_x مولفه ی اول کلید عمومی (A_x,B_x)را با فرض بردار تصادفی انتخابی d_x به صورت

$$A_X = g^{ax} \pmod p \text{ و } B_X = g^{dx} \pmod p$$

می سازد. در انتها زوج کلید عمومی (A_x,B_x) را به همراه ID_x به شنونده ی مورد اعتماد می فرستد. دراین جا شنونده ی مورد اطمینان پارامترهای G, p, s, R_p را درنظر می گیرد و بردار تصادفی b_Y را به عنوان کلید خصوصی انتخاب می کند که برحسب رمز خود می باشد. با توجه به b_y مولفه های کلید عمومی (C_Y,D_Y) را با فرض بردار تصادفی d_y که توسط شنونده مورد اعتماد انتخاب می شود به صورت

$$C_Y = g^{by} \pmod p \text{ و } D_Y = g^{dy} \pmod p$$

محاسبه می کند. همچنین با استفاده از آیدی دریافتی از کاربر و آیدی خودش ID_Y ، uوv را محاسبه می کند.

$$u = h_1(ID_X||ID_Y||B_X) \pmod p \in R_p$$
$$v = h_2(ID_X||ID_Y||B_X||D_Y) \pmod p \in R_p,$$

که $(h_1,h_2$)توابع چکیده ساز هستند.

در این مرحله(v , ID_Y , D_Y , C_Y) تحت کانال امن SSL یا TLSتوسط شنونده مورد اعتماد به کاربر ارسال می کند. البته توجه کنید که می تواند به جایv ، uرا ارسال کند. کاربر پس از دریافت (v , ID_Y , D_Y , C_Y) شروع به ساخت کلید نشست S_x می کند.

$$u = h_1(ID_X||ID_Y||B_X) \pmod p \in Rp$$
$$S_X = [(C_Y)^v + D_Y]^{(ax\cdot u+dx)} \pmod p$$

سپس کلید S_x را به شنونده مورد اعتماد تحت کانال امن ارسال می کند. در مرحله ی پایانی شنونده ی مورد اعتماد ابتدا کلید نشست S_yرا به صورت

$$S_Y = [(A_x)^u + B_x]^{(by\cdot v+dy)} \pmod p$$

محاسبه می کند و پس از دریافت S_x شروع به بررسی با کلید نشست خود به شرح زیر می کند.

$$S_X = [(C_Y)^v + D_Y]^{(ax\cdot u+dxX)} \pmod p،$$
$$S_X = [g^{by.v} + g^{dy}]^{(ax.u+dX)} \pmod p \text{ و}$$
$$S_X = [(A_X)^u + B_X]^{(by.v+dY)} \pmod p$$

در صورتی که $S_y = S_x$ باشد، اجازه ورود و ارسال یا دریافت پیام صادر می شود.

۶- بررسی امنیت طرح در حملات کوانتومی

یک رایانه کلاسیک از رشته های طولانی بیت استفاده می کند که صفر یا یک را کد می کند. رمزنگاری کوانتومی به الگوریتم‌های رمزنگاری یا الگوریتم های ابتدایی گفته می‌شود که برای پیاده‌سازی آن‌ها بر تکنیک مکانیک کوانتومی تکیه می‌کنند. از طرف دیگر یک کامپیوتر کوانتومی از بیت های کوانتومی یا کیوبیت استفاده می کند. کیوبیت یک سیستم کوانتومی است که صفر و یک را به دو حالت کوانتومی قابل تشخیص کد می کند. اما چون کیوبیت ها به صورت کوانتومی رفتار می کنند، می توانیم از پدیده های برهم نهی و درهم تنیدگی استفاده کنیم. برهم نهی اساساً توانایی یک سیستم کوانتومی برای قرار گرفتن همزمان در چندین حالت است یعنی چیزی می تواند همزمان این جا و آن جا یا بالا و پایین باشد. درهم تنیدگی نیز یک همبستگی فوق العاده قوی است که بین ذرات کوانتومی وجود دارد.

الگوریتم‌های کوانتومی با بهره‌گیری از غیر فیزیکی بودن جای کوانتوم‌ها، توانایی شکست دادن مدارهای کلاسیک را دارند. الگوریتم کوانتومی شور به کمک این توانایی به طور مؤثری برخی مسائل را برطرف می‌کند[4]. طرح های رمزنگاری مبتنی بر مشبکه، کاندیداهای اصلی برای رمزنگاری پس از کوانتومی کلید عمومی هستند[5]. بسیاری از آن ها بسیار کارآمد هستند و برخی حتی با بهترین گزینه های شناخته شده رقابت می کنند. پیاده سازی آن ها معمولاً بسیار ساده است. البته اعتقاد بر این است که همه آن ها چنین هستند. علاوه بر این ایمن در برابر حملات کوانتومی هستند. در حال حاضر هیچ الگوریتم کوانتومی شناخته شده ای برای حل مسائل مشبکه وجود ندارد که به طور قابل توجهی بهتر از شناخته شده ترین الگوریتم های کلاسیک عمل کند. این در حالی است که مسائل مشبکه به عنوان یک نامزد برای تلاش در حل الگوریتم های کوانتومی مطرح می شود زیرا اعتقاد بر این است که آن ها برای عوامل تقریبی معمولی به دلیل ساختار متناوب و تبدیل سریع فوریه مورد استفاده سخت نیستند.

تلاش ها برای حل مسائل مشبکه با الگوریتم های کوانتومی از زمان کشف الگوریتم تجزیه کوانتومی توسط شور در اواسط دهه ۱۹۹۰ انجام شده اما تاکنون با موفقیت کمی همراه بوده است[4]. مسئله ی اصلی این است که به نظر می رسد تکنیک هایی که در الگوریتم تجزیه شور و الگوریتم های کوانتومی مربوط به آن استفاده می شود، برای مسائل مشبکه کاربردی ندارد.

۷- نتیجه گیری و پژوهش های آتی

با تکامل دستگاه های ارتباطی وتوسعه ی اینترنت اشیا ارسال اطلاعات همراه با رمزگذاری ایمن صورت می گیرد. علاوه بر این، طراحی یک راه حل رمزگذاری موثر برای چنین محیطی با توجه به محدودیت منابع دستگاه های هوشمند مورد استفاده در این محیط، کاری چالش برانگیز است. بنابراین، برای مقابله با این نوع مسائل یک رمزگذاری امن مبتنی بر مشبکه برای مراقبت های

بهداشتی هوشمند در محیط شهرهای هوشمند ارائه شده است. طرح پیشنهادی با توجه به محاسبات سبک تری که در کلید ها و رمزگذاری طرح هست هزینه محاسبه و ارتباط کمتری در مقایسه با طرح های موجود دارد. در آینده، باید در مورد امنیت کانال و اطلاعات اولیه رمزگذاری شده برای داده های یک حوزه مشخص دریک محیط توزیع شده، تحقیقاتی بیشتر صورت گیرد. علاوه براین تکنیک های کاهش ابعاد را می توان در طرح پیشنهادی برای کاهش اندازه متن رمز در طول های بالاتر و همچنین پیچیدگی رمزگشایی پیام استفاده کرد.

۷- منابع

[1] J. Zhou, Z. Cao, X. Dong,'' Security and Privacy for Cloud-Based IoT'' - IEEE Communications, 2017.

[2] O. Regev, On Lattices Learning with Errors Random Linear Codes and Cryptography, JACM, 56(6), 2009.

[3] S. Paeng, B. Jung, K. Chan Ha, A Lattice Based Public Key Cryptosystem:Using Polynomial Representations, Springer-Verlag Berlin, 292–308, 2003.

[4] Shor, P., Algorithms for quantum computation: discrete logarithms and factoring, IEEE Comput Soc, 124-134, 1994.

[5] Micciancio, D., Regev, O., Lattice-based Cryptography, springer, 2008.

[6] Blum A., Furst M. L, Kearns M. J, and Lipton R. J, Cryptographic primitives based on hard learning problems, Heidelberg, Aug 1994 , pages 278-291.

[7] Katz, J., Lindell, Y., Modern Cryptography, Crc press, 2015.

[8] Ling, S., Xing, Ch., Coding Theory:A First Course, Cambridge, 2004.

[9] Stinsonn, D., Paterson, M., Cryptography Theory and Practice, Crc press, 2019.

[10]http://www.gartner.com/newsroom/id/3598917, 2017.

[11] Chaudhary, V., et al., Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment, IEEE Communications Magazine, 2018.

[12] Micciancio, D., Regev, O., Lattice-based Cryptography, springer, 2008.

فرشته حیدری مدرک کارشناسی خود را در رشته ریاضیات و کاربردها در سال ۱۳۹۸ و کارشناسی ارشد خود را در رشته ی ریاضی کاربردی گرایش رمزکد در سال ۱۴۰۰ از دانشگاه شاهد تهران اخذ کرده است. زمینه ی پژوهشی مورد علاقه ایشان رمزنگاری، ارتباطات امن در برابر حملات کوانتومی و نظریه حلقه ها می باشد.

نشانه رایانامه ی ایشان عبارتند از:

fereshteh.heydari216@gmail.com

روش ارجاع به مقاله :

ف.حیدری، رمز گذاری و احرازهو یت ایمن مبتنی بر مشـــبکه، دوفصلنامه محاسبات و سامانه های توزیع شده، سال پنجم، شماره ۲، شماره پیاپی ۱۰، صفحه ۴۳ تا ۴۸، سال ۱۴۰۱

How to cite: F.Heydari, Secure Lattice-based Encryption And Authentication, Journal of Distributed Computing and Systems(JDCS), Vol 5, Issue 2, Page 43-48, 2023.