مجموعه مقالات پانزدهمین کنفرانس بین‌المللی انجمن رمز ایران
دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ۶-۷ شهریور ۱۳۹۷
(مقاله مدعو)

طراحی چند سامانه رمزگذاری کارآ مبتنی بر مشبکه‌ها و کد-مشبکه‌ها

خدیجه باقری، محمدرضا (رفسنجانی) صادقی، دانشگاه صنعتی امیرکبیر، دانشکده ریاضی و علوم کامپیوتر، تهران، ایران
kbagheri, msadeghi@aut.ac.ir
ترانه اقلیدس، پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران
teghlidos@sharif.edu

چکیده - در این مقاله، با استفاده از کد-مشبکه‌ها و مشبکه‌هایی که به‌صورت کارآ قابل پیاده‌سازی هستند، به طراحی سامانه‌های رمز کلید متقارن و نامتقارن با کارآیی بیشتر نسبت به سامانه‌های مشبکه مبنای موجود می‌پردازیم. ابتدا خانواده‌ی جدیدی از مشبکه‌ها به‌نام مشبکه‌های QC-MDPC را معرفی می‌کنیم. سامانه‌ی رمز کلید نامتقارنی بر اساس این مشبکه‌ها پیشنهاد می‌کنیم که دارای پیچیدگی رمزگذاری و رمزگشایی خطی است. ماتریس‌های مولد و توازن‌آزمای این مشبکه‌ها دارای ساختار شبه دوری هستند. این ویژگی به همراه تنک بودن ماتریس توازن‌آزمای آن‌ها، اندازه‌ی کلید این سامانه را نسبت به رقیبان خود در سامانه‌های رمزگذاری مشبکه‌مبنا و رمزگذاری کدمبنا کوچک‌تر ساخته است. توسیع پیام این سامانه نیز کم‌تر از سامانه‌های رمز مشبکه‌مبنا و کدمبنای موجود است. حملات شناخته شده به سامانه‌های رمز مشبکه‌مبنا و کدمبنا، به سامانه پیشنهادی اعمال شده و نتایج به دست آمده حاکی از مقاومت سامانه پیشنهادی در برابر این حملات است. در بخش دیگر مقاله، با هدف ارائه یک طرح عملی که سه فرآیند رمزگذاری، کدگذاری و مدولاسیون را در یک گام واحد انجام دهد، از کدمشبکه‌های حاصل از مشبکه‌های QC-LDPC در طراحی یک سامانه‌ی رمز کلید متقارن شبه Rao-Nam استفاده می‌کنیم. سامانه پیشنهاد شده در برابر تمام حملات متن اصلی منتخب به سامانه‌های رمز شبه Rao-Nam مقاوم است. خطی بودن پیچیدگی محاسباتی الگوریتم‌های رمزگذاری و رمزگشایی، کوچک بودن اندازه کلید و نرخ زیاد انتقال اطلاعات در سامانه‌ی پیشنهادی، کارآیی مطلوبی را برای ایجاد یک ارتباط امن و قابل اطمینان روی کانال‌های دارای محدودیت پهنای باند فراهم می‌سازد.

کلید واژه‌ها
سامانه‌های رمز مشبکه‌مبنا، سامانه‌های رمز کدمبنا، کدمشبکه‌ها.

۱- مقدمه

امنیت سامانه‌های رمز کلید عمومی موجود که بر سختی مسئله‌ی تجزیه اعداد مرکب و لگاریتم گسسته تکیه کرده‌اند، در حضور رایانه‌های کوانتومی در مقیاس بزرگ، از دست می‌رود. درنتیجه طراحی سامانه‌های رمز کلید عمومی مقاوم در برابر رایانه‌های کوانتومی به یک ضرورت در سه دهه‌ی اخیر تبدیل شده است. مطالعه و طراحی این سامانه‌ها را رمزنگاری پسا کوانتومی[۱] می‌نامند [۱]. سامانه‌های رمز مشبکه‌مبنا[۲] و سامانه‌های رمز کدمبنا[۳]، دو خانواده‌ی نوید بخش از سامانه‌های رمز کلید عمومی هستند که با دانش امروزی بالقوه در برابر حملات کوانتومی امن هستند.

سامانه‌های رمز مشبکه‌مبنا بر اساس سختی مسائل مشبکه مانند مسئله‌ی کوتاه‌ترین بردار (SVP)، مسئله‌ی نزدیک‌ترین بردار (CVP)، مسئله جواب صحیح کوتاه (SIS) و مسئله یادگیری با خطا (LWE) طراحی شده‌اند که جزء مسائل کلاس NP-سخت هستند. این مسائل نه تنها در حوزه محاسبات کلاسیک، بلکه در حوزه محاسبات کوانتومی نیز دارای حل با پیچیدگی زمانی چندجمله‌ای نیستند. سامانه‌های رمز مشبکه‌مبنا، با توجه به امکان پیاده سازی کارآ و دارا بودن امنیت اثبات‌پذیر در برخی از نمونه‌هایش، کاندیدهای امیدوارکننده‌ای برای رمزنگاری پساکوانتومی به شمار می‌روند و توجه پژوهشگران بسیاری را به خود جلب کرده اند.

سامانه‌های AD[۴] و GGH[۵] دو سامانه‌ی بنیادین در سامانه‌های رمز مشبکه‌مبنا هستند که سامانه‌های دیگر در این حوزه بر پایه‌ی آن‌ها طراحی شده‌اند. سامانه‌ی AD در سال ۱۹۹۷ بر اساس سختی مسئله‌ی SVP معرفی

[۱] post quantum cryptography
[۲] Lattice based cryptosystems
[۳] Code based cryptosystems
[۴] Ajtai-Dwork
[۵] Goldreich-Goldwasser-Halevi

شد. این سامانه دارای امنیت اثبات‌پذیر است اما به علت داشتن اندازه‌ی کلید بسیار بزرگ و عملیات رمزگذاری بیت به بیت از نظر عملی غیر کاربردی است [۲]. عملیات رمزگذاری و رمزگشایی در سامانه‌ی GGH کارآتر از سامانه AD است اما چون این سامانه فاقد امنیت اثبات‌پذیر است، برای تامین امنیت آن به مشبکه‌هایی با بُعدهای بزرگ نیازمندیم و این موضوع کارآیی آن را به شدت تحت الشعاع قرار می‌دهد [۳].

سامانه رمز کلید عمومی NTRU در سال ۱۹۹۸ و بر اساس حلقه‌ی چندجمله‌ای‌ها معرفی شد [۴]. ماهیت بسیار ساده‌ی عملیات و امکان موازی سازی آن‌ها، سامانه‌ی رمز NTRU را به کارآترین سامانه‌ی مشبکه‌مبنای موجود تبدیل کرده است که از سامانه‌های رمز کلاسیک نیز سریع‌تر می‌باشد [۵]. NTRU دارای امنیت اثبات‌پذیر نیست. حمله‌ی مشبکه‌مبنایی[۶] به آن اعمال شده است که با حل یک مسئله‌ی SVP در مشبکه‌ی NTRU، منجر به بازیابی کلید خصوصی می‌شود. طرح‌های شبه NTRU بسیاری ارائه شده‌اند که اکثر آن‌ها شکسته شده‌اند و برخی دیگر نیز عملیاتی نبوده‌اند. به طور کلی، بهبودهای پیشنهاد شده برای NTRU معمولا با کاهش امنیت یا کارآیی آن همراه بوده است. سامانه رمز کلید عمومی مبتنی بر مسئله‌ی LWE در سال ۲۰۰۵ معرفی شد و از جمله سامانه‌ی مهم در رمزنگاری مشبکه‌مبنا است [۶]. NTRU بر اساس حلقه‌ی چندجمله‌ای‌ها و سامانه رمز مبتنی بر مسئله‌ی LWE بر اساس نظریه یادگیری معرفی شده‌اند. این سامانه دارای امنیت اثبات‌پذیر بوده اما از کارآیی مطلوبی برخوردار نیست. معرفی یک سامانه‌ی شبه LWE با کارآیی قابل مقایسه با کارآیی NTRU که دارای امنیت اثبات‌پذیر باشد، از مهم‌ترین پژوهش‌های عصر حاضر در این حوزه است.

اولین سامانه رمز کدمبنا در سال ۱۹۷۸ توسط مک الیس[۷]، بر اساس کدهای گوپا معرفی شد [۷]. امنیت این دسته از سامانه‌های رمز بر مبنای پیچیدگی عمل کدگشایی یک کد خطی تصادفی با ابعاد بزرگ است که جزء مسائل کلاس NP–تمام است [۸].چارچوب جبری کدهای گوپای به‌کار رفته در سامانه‌ی مک الیس، کارآیی و امنیت آن را به شدت تحت الشعاع قرار می‌دهد. طی چند دهه‌ی گذشته، کدهای متفاوتی مانند کدهای LDPC، QC-LDPC و QC-MDPC جایگزین کدهای گوپا شده و سامانه‌های شبه مک الیس بسیاری برای کاهش اندازه‌ی کلید، افزایش نرخ اطلاعات و افزایش امنیت آن پیشنهاد شده است [۹]، [۱۰]، [۱۱]، [۱۲]، [۱۳]. اکثر سامانه‌های اخیر در رمزگذاری کدمبنا دارای پیچیدگی محاسباتی از مرتبه خطی برحسب طول کد هستند، لیکن امن‌ترین نمونه‌های موجود در این سامانه‌ها به خاطر اندازه‌ی بزرگ کلید و نرخ پایین انتقال اطلاعات[۸] هنوز عملیاتی نشده‌اند.

از سوی دیگر به کارگیری الگوریتم‌های رمزنگاری مناسب به منظور تامین امنیت و اطمینان پذیری[۹] در ارتباطات به عنوان یک نیاز پایه‌ای الزامی‌است. سامانه‌های سنتی از الگوریتم‌های رمزگذاری و کدگذاری کانال در لایه‌های مختلف شبکه برای انتقال اطلاعات و برای برآورده ساختن نیازهای مذکور استفاده می‌نمایند. در کدگذاری کانال با اضافه کردن بیت‌های افزونگی[۱۰] به پیام اصلی، امکان تشخیص و تصحیح خطا برای گیرنده فراهم می‌شود. در رمزگذاری با هدف تامین امنیت، سعی بر این است که تا حد امکان از گسترش طول پیام در روند رمزگذاری جلوگیری شود. لذا این دو الگوریتم از دیدگاه گسترش طول پیام در تقابل با یکدیگر عمل می‌کنند. با توجه به بار محاسباتی و زمان مورد نیاز در هر بار اجرای عملیات رمزگذاری و رمزگشایی، بحث تامین امنیت و اطمینان پذیری در ارسال پیام یک چالش جدی به نظر می‌رسد.

رائو[۱۱] با روشی مشابه با مک الیس به طراحی سامانه‌های توأم رمزگذاری–کدگذاری کانال پرداخت که فرآیند رمزگذاری و تصحیح خطا را در یک گام واحد ادغام می‌کند [۱۴]. هدف اصلی این طرح فراهم کردن توأم انتقال امن و مطمئن داده ها با استفاده از یک سامانه‌ی رمز کلید متقارن کدمبنا بوده است. در یک سامانه‌ی توأم، امنیت در بخش کدگذاری کانال نشانده شده تا امنیت کل سامانه به‌گونه‌ای افزایش یابد که مهاجم بدون اطلاع از کلید مخفی قادر به تصحیح خطای ناشی از کانال نبوده و نتواند داده‌ی منتقل شده را کدگشایی نماید. سامانه‌ی رائو در برابر حملات با متن اصلی منتخب امن نیست. برای غلبه بر این ضعف، رائو و نام[۱۲] نسخه اصلاح شده‌ی آن را ارائه کردند که به سامانه‌ی Rao-Nam معروف است [۱۵]، [۱۶]. طرح‌های توأم زیادی به منظور کاهش اندازه‌ی کلید، افزایش نرخ انتقال اطلاعات و بهبود امنیت سامانه‌ی Rao-Nam در برابر حملات شناخته شده ارائه شده است ولی اندازه‌ی کلید آن‌ها همچنان بزرگ است [۱۷]، [۱۸]، [۱۹]، [۲۰]. به تازگی یک طرح توأم رمزگذاری–کدگذاری بر اساس مشبکه‌های LDLC پیشنهاد شده است که اندازه‌ی کلید آن بسیار بزرگ است و از کارآیی مطلوبی برخوردار نیست [۳۴].

در این مقاله، به‌منظور بهبود کارآیی با حفظ امنیت محاسباتی سامانه‌های رمز مشبکه‌مبنا، از مشبکه‌ها با ساختار خاص استفاده می‌کنیم. این مشبکه‌ها رابطه‌ی تنگاتنگی بین ساختار مشبکه‌ها و کدهای تصحیح خطا ایجاد می‌کنند و الگوریتم کدگشایی آن‌ها برای حل مسئله CVP در ابعاد بزرگ، به‌صورت کارآ قابل پیاده سازی است. لذا می‌توانند به منظور طراحی سامانه‌های رمز کلید متقارن و کلید نامتقارن کارآ استفاده شوند.

در بخش ۲– مفاهیم مورد نیاز را بیان می‌کنیم. در بخش ۳– یک طرح رمزگذاری کلید نامتقارن کارآ مبتنی بر مشبکه‌های QC-MDPC معرفی می‌کنیم. در بخش ۴– با بهره گیری از مشبکه‌های QC-LDPC به معرفی یک سامانه‌ی رمز کلید متقارن می‌پردازیم که توأما سه عمل رمزگذاری، کدگذاری و مدولاسیون را در یک فرآیند واحد انجام می‌دهد. در بخش ۵– جمع‌بندی آورده شده است.

۲– مفاهیم مورد نیاز

در این بخش، به معرفی مفاهیم اساسی موجود در نظریه‌ی مشبکه‌ها، کدمشبکه‌ها[۱۳] و مشبکه‌های QC-LDPC و نحوه ساخت آن‌ها می‌پردازیم.

---

[۶] Lattice attack
[۷] McElliece
[۸] information rate
[۹] reliability
[۱۰] Redundancy
[۱۱] Rao
[۱۲] Nam
[۱۳] Lattice codes

مزیت عمده این مشبکه‌ها عملکرد مناسب و پیچیدگی پایین کدگذاری و کدگشایی آن‌ها نسبت به سایر مشبکه‌ها است.

تعریف ۲-۱. مجموعه گسسته نا متناهی $\Lambda \subset R^m$ را یک مشبکه گوییم هرگاه Λ یک گروه جمعی در اعداد حقیقی باشد. اعضای یک مشبکه را نقاط یا بردارهای مشبکه می‌گویند.

می‌توان نشان داد که هر مشبکه دارای مجموعه‌ای از بردارهای مستقل خطی به‌عنوان پایه است. تعداد اعضای پایه را بعد یا رتبه‌ی مشبکه می‌گویند. واضح است که اگر $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ یک پایه برای مشبکه باشند، آنگاه $n \leq m$. اگر $m = n$ آنگاه مشبکه را دارای رتبه‌ی کامل[۱۴] می‌گویند. تمام مشبکه‌های معرفی شده در این مقاله دارای رتبه کامل هستند.

تعریف ۲-۲. فرض کنیم $\mathbf{b_i} = (b_{i,1}, b_{i,2}, \ldots b_{i,m})$ با ازای $i = 1, 2, \ldots n$ اعضای پایه مشبکه باشند. ماتریس مولد مشبکه به صورت زیر تعریف می‌شود

$$\mathbf{B} = \begin{bmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_n} \end{bmatrix} = \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,m} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,m} \end{bmatrix}. \qquad (1)$$

با توجه به تعریف فوق می‌توان نوشت

$$\Lambda = \{\mathbf{xB} \mid \mathbf{x} \in Z^n\}. \qquad (2)$$

نگاشت بردار صحیح $\mathbf{x}$ به نقطه مشبکه $\mathbf{xB}$ را کدگذاری مشبکه می‌نامند. همچنین، منظور از کدگشایی در مشبکه ها، حل مسئله نزدیکترین بردار (CVP) در مشبکه است.

تعریف ۲-۳. دترمینان یا حجم یک مشبکه با استفاده از فرمول $\det(\Lambda) = \det(\mathbf{B}\mathbf{B}^T)^{\frac{1}{2}}$ به‌دست می‌آید.

پایه‌ی یک مشبکه یکتا نیست و پایه‌های بسیاری برای هر مشبکه وجود دارد. به این معنی که دو ماتریس مولد متفاوت $\mathbf{B}$ و $\mathbf{B'}$ می‌توانند مشبکه‌ی یکسانی را تولید کنند:

$$\{\mathbf{xB} \mid \mathbf{x} \in Z^n\} = \{\mathbf{xB'} \mid \mathbf{x} \in Z^n\}.$$

تعریف ۲-۴. ماتریس $\mathbf{U} \in Z^{n \times m}$ را یک ماتریس تک هنگ[۱۵] می‌نامیم، اگر $\det(\mathbf{U}) = \pm 1$.

پایه‌های مختلف یک مشبکه توسط یک ماتریس تک هنگ به یکدیگر مربوط می‌شوند. درواقع اگر $\mathbf{B}, \mathbf{B'} \in R^{n \times m}$ ماتریس‌های مولد یک مشبکه باشند، آنگاه ماتریس تک هنگ $\mathbf{U}$ وجود دارد که $\mathbf{B'} = \mathbf{UB}$.

در بسیاری از کاربردهای رمزنگاری از صورت نرمال هرمیتی[۱۶] پایه استفاده می‌شود که به آن پایه‌ی HNF می‌گویند. صورت نرمال هرمیتی یک پایه‌ی مربعی $\mathbf{B}$ با داریه‌های صحیح دارای صورت نرمال هرمیتی $\mathbf{H}$ است اگر یک ماتریس تک هنگ $\mathbf{U}$ وجود داشته باشد که $\mathbf{H} = \mathbf{UB}$ و $\mathbf{H}$ دارای شرایط زیر باشد: ۱) بالا مثلثی باشد، یعنی برای $i > j$ داریم $h_{ij} = 0$، ۲) برای تمام iها داریم $h_{ii} > 0$ و ۳) برای $i < j$ داریم $h_{ij} < h_{ii}$.

تعریف ۲-۵. برای بررسی میزان متعامد بودن یک پایه‌ی $\mathbf{B}$، پارامتر کاستی تعامد[۱۷] آن را محاسبه می‌نماییم.

$$\textit{orth-defect}(\mathbf{B}) = \frac{\prod_{i=1}^{n} \|\mathbf{b}_i\|}{\det(\mathbf{B})}. \qquad (3)$$

همواره $\text{orth-defect}(\mathbf{B}) \geq 1$ و این پارامتر با میزان عمود بودن بردارها نسبت مستقیم دارد، هر چه بردارهای پایه عمودتر باشند پارامتر کاستی تعامد به یک نزدیکتر خواهد شد [۱].

تعریف ۲-۶. مشبکه Λ را یک مشبکه *QC-LDPC* نامیم در صورتی که با استفاده از ساختار A به دست آمده و کد $\mathcal{C}$ زیرین آن یک کد دودویی *QC-LDPC* باشد. به عبارت دیگر، $\mathbf{x} \in Z^n$ متعلق به Λ است اگر و تنها اگر $\mathbf{H}_{qc}\mathbf{x}^t = 0 \pmod 2$، که در آن $\mathbf{H}_{qc}$ ماتریس توازن‌آزمای شبه دوری کد $\mathcal{C}$ است.

در ادامه‌ی مقاله، $\mathbf{H}_{qc}$ نشان دهنده‌ی ماتریس توازن‌آزمای یک مشبکه QC-LDPC است که برابر ماتریس توازن‌آزمای کد زیرین آن است. ماتریس مولد این مشبکه به‌صورت زیر ارائه می‌شود

$$\mathbf{G}_\Lambda = \begin{bmatrix} \mathbf{I}_k & \mathbf{A}_{k\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & 2\mathbf{I}_{n-k} \end{bmatrix}, \qquad (4)$$

که در آن $\mathbf{G}_\mathcal{C} = \begin{bmatrix} \mathbf{I}_k & \mathbf{A}_{k\times(n-k)} \end{bmatrix}$ ماتریس مولد کد $\mathcal{C}$ به فرم سیستماتیک است [۲۱]. همچنین می‌توان نشان داد که

$$\mathbf{G^{-1}}_\Lambda = \begin{bmatrix} \mathbf{I_k} & -\frac{1}{2}\mathbf{A_{k\times(n-k)}} \\ \mathbf{0}_{\mathbf{(n-k)}\times\mathbf{k}} & \frac{1}{2}\mathbf{I_{(n-k)}} \end{bmatrix}. \qquad (5)$$

بالا مثلثی از مشبکه را ارائه می‌دهد که به طور کارآ از هر پایه‌ی مشبکه با استفاده از عملیات سطری و ستونی به‌دست آمده و منحصربه فرد است. یک ماتریس مربعی $\mathbf{B}$ با داریه‌های صحیح دارای صورت نرمال هرمیتی $\mathbf{H}$ است اگر یک ماتریس تک هنگ $\mathbf{U}$ وجود داشته باشد که $\mathbf{H} = \mathbf{UB}$ و $\mathbf{H}$ دارای شرایط زیر باشد: ۱) بالا مثلثی باشد، یعنی برای $i > j$ داریم $h_{ij} = 0$، ۲) برای تمام iها داریم $h_{ii} > 0$ و ۳) برای $i < j$ داریم $h_{ij} < h_{ii}$.

تعریف ۲-۵. برای بررسی میزان متعامد بودن یک پایه‌ی $\mathbf{B}$، پارامتر کاستی تعامد[۱۷] آن را محاسبه می‌نماییم.

$$\textit{orth-defect}(\mathbf{B}) = \frac{\prod_{i=1}^{n} \|\mathbf{b}_i\|}{\det(\mathbf{B})}. \qquad (3)$$

همواره $\text{orth-defect}(\mathbf{B}) \geq 1$ و این پارامتر با میزان عمود بودن بردارها نسبت مستقیم دارد، هر چه بردارهای پایه عمودتر باشند پارامتر کاستی تعامد به یک نزدیکتر خواهد شد [۱].

۲-۱- ساخت مشبکه با استفاده از کدها

در این بخش به معرفی یکی از روش‌های موجود برای ساخت مشبکه با استفاده از کدهای تصحیح خطا می‌پردازیم. جزئیات این روش‌ها را می‌توان در [۲۱] و [۲۲] یافت. سپس به معرفی کدمشبکه‌ها و مشبکه‌های QC-LDPC و نحوه ساخت آن‌ها می‌پردازیم. مزیت عمده این مشبکه‌ها عملکرد مناسب و پیچیدگی پایین کدگذاری و کدگشایی آن‌ها نسبت به سایر مشبکه‌ها است. فرض کنیم $\mathcal{C} = [n, M, d_{min}]$ یک کد دودویی (نه لزوما خطی) از طول n و دارای M کدواژه باشد. مجموعه‌ی Λ شامل نقاط $\mathbf{x} \in R^n$ که به ازای یک کدواژه‌ی $\mathbf{c} \in \mathcal{C}$ در رابطه‌ی زیر صدق کنند را مشبکه‌ی "ساختار A[۱۸]" می‌گوییم:

$\mathbf{x} \in \Lambda$ اگر و تنها اگر $\mathbf{c} \in \mathcal{C}$ موجود باشد که $\mathbf{x} \equiv \mathbf{c} \pmod 2$.

[۱۴] Full-rank

[۱۵] Unimodular matrix

[۱۶] Hermite Normal Form (HNF)

[۱۷] orthogonality defect

[۱۸] construction A

کدگذاری یک بردار سطری صحیح $\mathbf{u} \in Z^n$ در مشبکه QC-LDPC عبارت است از

$$\mathcal{E}(\mathbf{u}) = ۲\mathbf{u}\mathbf{G}_\Lambda - (۱, \ldots, ۱). \qquad (۶)$$

الگوریتم کدگشایی این مشبکه‌ها یک الگوریتم کاراَ و تکراری به‌نام الگوریتم SPA است که جزییات آن در [۲۵] ارائه شده است.

۳- سامانه‌ی رمز کلید نامتقارن مبتنی بر مشبکه‌های QC-MDPC

در این بخش، با معرفی خانواده‌ی جدیدی از مشبکه‌ها به‌نام مشبکه‌های QC-MDPC، یک سامانه‌ی رمز کلید عمومی شبه GGH بر اساس آن‌ها پیشنهاد می‌کنیم.

به طور کلی، کدهای MDPC دارای ساختار کمتری نسبت به کدهای استفاده شده در سامانه‌های رمز کدمبنا هستند و به کدهای تصادفی نزدیک هستند. درنتیجه انتخاب مناسبی برای استفاده در این سامانه‌های رمز هستند. همچنین سامانه‌ی طراحی شده بر اساس این کدها که به (QC-)MDPC McEliece مشهور است، در برابر حمله‌های مبتنی بر کدگشایی مجموعه اطلاعاتی[۱۹] [۲۳] که کدکلمات با وزن کم را در سامانه‌های مبتنی بر کدهای QC-LDPC مانند [۱۱] پیدا می‌کنند، امن است.

یک $[n,\ r,\ w]$–کد MDPC، یک کد خطی از طول n و افزونگی r است که توسط یک ماتریس توازن‌آزمای $r \times n$ و با وزن سطری $w = \mathcal{O}(\sqrt{n \log n})$ تعریف می‌شود. در واقع کدهای MDPC را می‌توان مانند کدهای LDPC فرض کرد که ماتریس توازن‌آزمای آن‌ها دارای چگالی بیشتری است [۲۴]. اگرچه هنوز ماتریس توازن‌آزمای آن‌ها تنک‌تر از کدهای کلاسیک است.

در ادامه به منظور افزایش کارآیی سامانه ی رمز، از مدل شبه دوری این کدها (QC-MDPC) استفاده می‌کنیم.

تعریف ۳-۱. مشبکه *QC-MDPC*، یک مشبکه بر اساس ساختار A است که از یک کد *QC-MDPC* دودویی $\mathcal{C}$ به‌عنوان کد زیرین خود استفاده می‌کند. به‌طور معادل $\mathbf{x} \in Z^n$ متعلق به Λ است اگر و تنها اگر $\mathbf{H}_{qc}\mathbf{x}^t = ۰ \pmod ۲$، که $\mathbf{H}_{qc}$ ماتریس توازن‌آزمای شبه دوری کد $\mathcal{C}$ است.

در [۲۶]، الگوریتم‌های کدگشایی تکراری BFA برای این مشبکه‌ها ارائه کرده‌ایم که به دلیل محدودیت صفحات از بیان آن در این مقاله اجتناب کرده‌ایم. پیچیدگی محاسباتی این الگوریتم نسبت به بعد مشبکه، خطی است.

در طرح رمزگذاری پیشنهادی در این بخش، باب یک (n, r, w)–کد QC-MDPC را به صورت تصادفی انتخاب می‌کند که در آن $\mathbf{H}_{qc}$ ماتریس توازن‌آزمای کد با وزن سطری ثابت w است. طول کد $n = n_۰ b$ و $r = b$ که $n_۰$ یک عدد صحیح نامنفی است. درنتیجه ماتریس‌های $b \times b$ چرخشی مانند $\mathbf{H}_۰, \ldots, \mathbf{H}_{n_۰-۱}$ وجود دارند به‌طوری که

$$\mathbf{H}_{qc} = \left[\ \mathbf{H}_۰ \ \middle|\ \mathbf{H}_۱ \ \middle|\ \cdots \ \middle|\ \mathbf{H}_{n_۰-۱}\ \right]. \qquad (۷)$$

فرض کنید تعداد عناصر ناصفر در سطرهای $\mathbf{H}_i$ برابر با w_i باشد، به طوری که $\sum_{i=۰}^{n_۰-۱} w_i = w$. همچنین فرض کنید ماتریس $\mathbf{H}_{n_۰-۱}$ نامنفرد باشند. آنگاه ماتریس مولد این مشبکه برابر است با

$$\mathbf{G}_\Lambda = \left[\begin{array}{c|c} & \mathbf{P}_۰^t \\ & \mathbf{P}_۱^t \\ \mathbf{I_k} & \vdots \\ & \mathbf{P}_{n_۰-۲}^t \\ \hline mycolor{۲۰}_{(\mathbf{n-k})\times\mathbf{k}} & ۲\mathbf{I_{n-k}} \end{array}\right], \qquad (۸)$$

که برای هر $i = ۰, \ldots, n_۰ - ۲$ داریم: $\mathbf{P}_i = \mathbf{H}_{n_۰-۱}^{-۱}\mathbf{H}_i$.

با توجه به تعریف مشبکه‌های (QC)-LDPC و (QC)-MDPC داریم: $\mathrm{HNF}(\mathbf{G}_\Lambda) = \mathbf{G}_\Lambda \pmod ۲$.

چون $\text{orth-defect}(\mathbf{G}_\Lambda) \gg (\sqrt{۲})^{(n_۰-۱)b} = (\sqrt{۲})^k$، درنتیجه $\text{orth-defect}(\mathbf{G}_\Lambda) \gg ۱$ که نشان دهنده دور بودن پایه عمومی $\mathbf{G}_\Lambda$ از پایه‌ی متعامد است. بنابراین $\mathbf{G}_\Lambda$ یک پایه‌ی بد برای پیدا کردن نزدیکترین بردار (CVP) در مشبکه‌ی Λ است و انتخاب مناسبی برای پایه‌ی عمومی باب است.

زیر ماتریس‌های $\mathbf{P}_i$ (برای $i = ۰, \ldots, n_۰ - ۲$) در $\mathbf{G}_\Lambda$ را به‌عنوان کلید عمومی منتشر می‌کنیم. ماتریس توازن‌آزمای $\mathbf{H}_{qc}$ را نیز کلید خصوصی طرح پیشنهادی درنظر می‌گیریم.

۳-۱- الگوریتم رمزگذاری

برای رمزکردن پیام $\mathbf{m} \in Z^n$، ابتدا با استفاده از الگوریتم کدگذاری مشبکه آن را به یک نقطه از مشبکه تبدیل می‌کنیم، سپس بردار خطای $\mathbf{e}$ از طول n را به طور تصادفی انتخاب کرده و به آن اضافه می‌کنیم.

$$\mathbf{y} = 2\mathbf{m}\mathbf{G}_\Lambda - \mathbf{1} + \mathbf{e},$$

که بردار خطای $\mathbf{e}$ که به‌طور عمدی اضافه کردیم، از یک توزیع گوسی با واریانس $\sigma^۲$ انتخاب شده است، یعنی $\mathbf{e} \sim \mathcal{N}(۰, \sigma^۲)$.

واریانس $\sigma^۲$ چنان انتخاب می‌شود که نرخ شکست کدگشایی در رمزگشایی ناچیز (مثلا $۱۰^{-۷}$) باشد. برای افزایش کارآیی سامانه‌ی پیشنهادی، نیاز به انتخاب یک زیرمجموعه‌ی متناهی از مشبکه داریم تا درایه‌های متن رمز شده را کوچک نگه دارد. این کار را با انتخاب یک ناحیه محدود حول مبدا در R^n و در نظر گرفتن نقاط مشبکه که در این ناحیه قرار دارند، انجام می‌دهیم. به این ناحیه، ناحیه شکل‌دهی[۲۰] گفته می‌شود و نقاط داخل این ناحیه را به‌عنوان کدمشبکه درنظرمی‌گیرند. در واقع به جای نگاشت پیام $\mathbf{m}$ به نقطه‌ی $\boldsymbol{\lambda} = \mathbf{m}\mathbf{G}_\Lambda$ در مشبکه نامتناهی Λ، آن را به نقطه $\boldsymbol{\lambda}' = \mathbf{m}'\mathbf{G}_\Lambda$ داخل ناحیه‌ی شکل‌دهی می‌نگاریم. به الگوریتمی که عملیات انتخاب نقاط جدید $\boldsymbol{\lambda}'$ در بین کدمشبکه‌ها را انجام می‌دهد الگوریتم شکل‌دهی[۲۱] گفته می‌شود.

[۱۹] Information set decoding (ISD) attacks

[۲۰] Shaping region

[۲۱] shaping method

برای انجام الگوریتم شکل‌دهی، بردار صحیح $\mathbf{m}$ را به مجموعه‌ی متناهی زیر محدود می‌کنیم

$$m_i \in \left\{ x \in Z \;\middle|\; \frac{-L_i}{۲} \le x \le \frac{L_i}{۲} - ۱ \right\},\ i = ۱, \ldots, n, \qquad (۹)$$

که L_iها اعداد صحیح زوج هستند. حال نقطه‌ی جدید

$$\boldsymbol{\lambda}' = \mathbf{m}'\mathbf{G}_\Lambda = (\mathbf{m} - \mathbf{tL})\mathbf{G}_\Lambda$$

در مشبکه Λ را به جای $\boldsymbol{\lambda} = \mathbf{m}\mathbf{G}_\Lambda$ درنظر می‌گیریم که $\mathbf{L} = \mathrm{diag}(L_۱, \ldots, L_n)$ یک ماتریس قطری $n \times n$ است و بردار پیام جدید برابر با $\mathbf{m}' = \mathbf{m} - \mathbf{tL}$ است. بردار $\mathbf{t}$ یک بردار صحیح از طول n است که به گونه‌ای انتخاب می‌شود که بردار مشبکه‌ی حاصل درون ابرمکعب واقع شده حول مبدا قرار بگیرند، یعنی به ازای هر $i = ۱, \ldots, n$ داشته باشیم $|\lambda'_i| \le L_i$.

پس از یافتن بردار مشبکه‌ی شکل داده شده $\mathbf{m}'\mathbf{G}_\Lambda$ باید با ضریب ۲ مقیاس شده و با بردار $(-۱, \ldots, -۱)$ انتقال یابد. درنهایت متن رمزشده‌ی زیر ارسال می‌شود:

$$\mathbf{y} = ۲\mathbf{m}'\mathbf{G}_\Lambda - \mathbf{1} + \mathbf{e}. \qquad (۱۰)$$

چون بردار خطای عمدی $\mathbf{e}$ یک بردار با مولفه‌های حقیقی است، به‌منظور افزایش توان محاسباتی و بهینه سازی توان ذخیره‌سازی، از یک نگاشت تقریب کننده[۲۲] استفاده می‌کنیم تا مولفه‌های بردار خطای عمدی را تقریب بزند. به این ترتیب می‌توان تعداد بیت مورد نیاز برای ذخیره‌سازی متن رمز را مشخص نمود. در این مقاله از تقریب کننده‌ی ۱۶ سطحی[۲۳] استفاده شده است. فرض می‌کنیم که $\mathbf{y}$ روی کانال امن و بدون نویز مخابره می‌شود.

۳-۲- الگوریتم رمزگشایی

با توجه به اینکه $\mathbf{y} = ۲\mathbf{m}'\mathbf{G}_\Lambda - ۱ + \mathbf{e}$ یک بردار شکل‌دهی شده مشبکه است که توسط $\mathbf{e}$ منحرف شده است، رمزگشایی با حل مسئله‌ی نزدیکترین بردار با ورودی بردار $\mathbf{y}$ انجام می‌شود. در واقع برای رمزگشایی متن رمز شده‌ی $\mathbf{y}$ و بازیابی پیام $\mathbf{m}$، ابتدا با استفاده از یکی از الگوریتم‌های کدگشایی تکراری SPA یا BFA ([۲۵] و [۲۶]) برای مشبکه‌های QC-MDPC و کلید خصوصی $\mathbf{H}_{qc}$، بردار خطا را حذف می‌کنیم. آنگاه بردار پیام اصلی $\mathbf{m}$ از بردار مشبکه شکل‌دهی شده $\boldsymbol{\lambda}' = ۲\mathbf{m}'\mathbf{G}_\Lambda - ۱$ با اعمال الگوریتم ۱ بدست می‌آید.

۳-۳- تحلیل

تمام حملات شناخته شده به سامانه‌های رمز مشبکه‌مبنا و کدمبنای موجود را به سامانه‌ی پیشنهادی اعمال، و مقاومت آن را بررسی کرده‌ایم. بخش تحلیل رمز این سامانه به دلیل کمبود فضا آورده نشده است. جزییات بیشتر در [۲۶] قابل دسترسی است.

پیچیدگی زمانی و فضایی الگوریتم رمزگذاری و رمزگشایی سامانه پیشنهادی نسبت به بعد مشبکه، خطی است [۲۶]. در جدول ۱، حداکثر تعداد بیت‌های مورد نیاز برای نشان دادن متن اصلی و متن رمز، اندازه‌ی کلید خصوصی و عمومی، و

[۲۲] Quantization

[۲۳] ۱۶-level quantization

الگوریتم ۱ بازیابی بردار اولیه از بردار مشبکه شکل‌دهی شده.

procedure MOD $\left(\boldsymbol{\lambda}', (L_۱, \ldots, L_n), \mathbf{G}_\Lambda^{-۱}\right)$
  $\mathbf{b}' \leftarrow \left\lfloor \left(\frac{\boldsymbol{\lambda}'+۱}{۲}\right)\mathbf{G}_\Lambda^{-۱} \right\rfloor$
  for $i = ۱ : n$ **do**
    if $b'_i \pmod{L_i} < \frac{L_i}{۲}$ **then**
      $r_i \leftarrow b'_i \pmod{L_i}$.
    else
      $r_i \leftarrow b'_i \pmod{L_i} - L_i$
    end if
  end for
  return $\mathbf{m} = (r_۱, \ldots, r_n)$.
end procedure

پیچیدگی زمانی و فضایی الگوریتم رمزگذاری و رمزگشایی را بر حسب پارامترهای آن به‌طور خلاصه ارائه کرده‌ایم.

جدول ۱: مشخصات عملیاتی طرح پیشنهادی بر حسب پارامترهای آن.

بیت‌های مورد نیاز متن اصلی	$n\lceil \log_۲(L-۱) \rceil$ بیت
بیت‌های مورد نیاز متن رمز	$(n-k)\lceil \log_۲(۴L) \rceil + k\lceil \log_۲(۲L-۲) \rceil + n\log_۲ q$ بیت
اندازه‌ی کلید خصوصی	n بیت
اندازه‌ی کلید عمومی	k بیت
پیچیدگی رمزگشایی	$O(n)$
پیچیدگی رمزگذاری	$O(n)$

در واقع به منظور ساده سازی، برای هر $i = ۱, \ldots, n$ در معادله (۹)، قرار می‌دهیم $L_i = L$ و بردار صحیح پیام $\mathbf{m}$ را به مجموعه متناهی $m_i \in \{-L/۲, \ldots, L/۲ - ۱\}$ محدود می‌کنیم.

توسیع پیام[۲۴] برای سامانه‌ی پیشنهادی برابر است با:

$$\frac{(n-k)\lceil \log_۲(۴L) \rceil + k\lceil \log_۲(۲L-۲) \rceil + n\log_۲ q}{n\lceil \log_۲(L-۱) \rceil}. \qquad (۱۱)$$

پیچیدگی‌های رمزگذاری و رمزگشایی از مهمترین موضوعات مطرح در سامانه‌های رمز مشبکه‌مبنا است. یکی از مزایای طرح پیشنهادی این مقاله، دارا بودن الگوریتم های رمزگذاری و رمزگشایی با پیچیدگی کم است که هر دو نسبت به بعد مشبکه خطی هستند. با توجه به نتایج ارائه شده در جدول ۲، طرح مشبکه‌مبنای پیشنهادی، صرفه جویی قابل توجهی در پیچیدگی رمزگذاری و رمزگشایی دارد و کارآترین سامانه‌ی کلید عمومی مشبکه‌مبنا خواهد بود. توجه داشته باشید که اندازه کلید سامانه‌ی پیشنهادی از NTRU که یکی از کارآترین سامانه‌های مشبکه‌مبنا است، بزرگ‌تر است. اما خاص بودن ساختار مشبکه‌ی استفاده شده در این مقاله، باعث بهبود قابل توجه در پیچیدگی‌های رمزگذاری، رمزگشایی و توسیع پیام سامانه‌ی پیشنهادی شده است. از سوی دیگر، در مقایسه با کارآترین سامانه‌های کدمبنای معرفی شده یعنی سامانه QC-MDPC-McEliece، که هم اکنون تحت حمله‌ی ارائه شده در [۲۷] ناامن است، سامانه پیشنهادی دارای توسیع پیام کمتری است. به‌عنوان نتیجه کلی از

[۲۴] Message expansion

جدول ۲: مقایسه‌ی سامانه‌ی کلید نامتقارن پیشنهادی با سامانه‌های کدمبنا و مشبکه‌مبنای موجود

	[۳] GGH	[۳۳] NTRU	[۷] McEliece	[۱۲] QC-MDPC-McEliece	[۳۵] سامانه مبتنی بر LDLC	سامانه پیشنهادی
اندازه‌ی کلید عمومی	$\mathcal{O}(n^{۳}\log n)$	$n\log q$ بیت	$k(n-k)$ بیت	$n-r$ بیت	$\mathcal{O}(n^{۲})$	$n-r$ بیت
اندازه‌ی کلید خصوصی	$\mathcal{O}(n^{۳}\log n)$	$۲n\log p$	$\mathcal{O}(n^{۲}(\log n)^{۲})$	$\mathcal{O}(n)$	$\mathcal{O}(n^{۲})$	$\mathcal{O}(n)$
سرعت رمزگشایی	$\mathcal{O}(n^{۲})$	$\mathcal{O}(n\log n)$	$\mathcal{O}(n^{۲})$	$\mathcal{O}(n)$	$\mathcal{O}(n^{۲})$	$\mathcal{O}(n)$
سرعت رمزگذاری	$\mathcal{O}(n^{۲})$	$\mathcal{O}(n\log n)$	$\mathcal{O}(n^{۲})$	$\mathcal{O}(n)$	$\mathcal{O}(n^{۲})$	$\mathcal{O}(n)$
توسیع پیام	ارائه نشده است	$\log_p q \approx ۵/۰۵$	۲	۲	ارائه نشده است	۱/۷
اندازه‌ی کلید عمومی	۳۳۰ کیلو بایت	۲۶۹۶ بیت	۲۶۲ کیلو بیت	۴۸۰۱ بیت	۱ مگابیت	۴۸۰۱ بیت
پارامترهای پیشنهادی	$n = ۴۰۰$	$(n,q,p) = (۳۳۷, ۲۵۶, ۳)$	$(n,k) = (۱۰۲۴, ۵۲۴)$	$(n,r) = (۹۶۰۲, ۴۸۰۱)$	$n = ۱۰۰۰$	$(n,r) = (۹۶۰۲, ۴۸۰۱)$, $q = ۱۶, L = ۲۵۶$

این جدول، سامانه پیشنهادی بهبود مطلوبی در پیچیدگی رمزگذاری، رمزگشایی و توسیع پیام نسبت به سامانه‌های رمز مشبکه‌مبنا و کدمبنای موجود داشته است و همچنین در برابر تمام حملات شناخته شده به سامانه‌های رمز مشبکه‌مبنا و کدمبنا مقاوم است.

٤- سامانه‌ی توأم رمزگذاری، کدگذاری و مدولاسیون مبتنی بر مشبکه QC-LDPC

کدمشبکه‌های حاصل از مشبکه‌های QC-LDPC، یک طرح توأم کدگذاری-مدولاسیون کارآ در کانال‌های AWGN دارای محدودیت پهنای باند معرفی می‌کنند [۲۵]. در این بخش، با بهره گیری از کارآیی این کدمشبکه‌ها و سامانه‌ی رمز کلید متقارن شبه Rao-Nam معرفی شده در [۲۸]، سامانه‌ی رمزی پیشنهاد می‌دهیم که توأما سه عمل رمزگذاری، کدگذاری و مدولاسیون را در یک فرآیند واحد انجام می‌دهد.

٤-۱- کلیدهای مخفی

الگوریتم رمزگذاری با استفاده از کلیدهای مخفی زیر انجام می‌شود که توسط فرستنده و گیرنده مجاز انتخاب می‌شوند:

۱. یک کد EDF-QC-LDPC[۲۵] با ماتریس توازن‌آزمای $\mathbf{H}_{qc}$ به فرم (۷)، با پارامترهای $(n = n_۰ b,\ k = (n_۰ - ۱)b,\ d_r)$ و وزن سطری d_r، برای ساخت یک مشبکه‌ی QC-LDPC،

۲. T به‌عنوان مقدار اولیه $(n-k)$ بیتی از یک LFSR، برای تولید یک دنباله از ۲^{n-k} سندرم شبه تصادفی $\mathbf{s} \in F_۲^{n-k}$،

۳. یک ماتریس جایگشت $\mathbf{P}$ از بعد $n \times n$ که توسط زیر ماتریس جایگشت $\boldsymbol{\pi}$ از بعد $q \times q$ ساخته شده است:

$$\mathbf{P} = \begin{bmatrix} \boldsymbol{\pi} & ۰ & \cdots & ۰ \\ ۰ & \boldsymbol{\pi} & \cdots & ۰ \\ \vdots & & \ddots & \vdots \\ ۰ & ۰ & \cdots & \boldsymbol{\pi} \end{bmatrix}_{n\times n}. \qquad (۱۲)$$

مشابه با بخش قبل، ماتریس مولد مشبکه‌ی QC-LDPC متناظر با $\mathbf{H}_{qc}$ به فرم (۸) است.

٤-۲- الگوریتم رمزگذاری

برای رمزگذاری یک پیام $\mathbf{m} \in Z^n$، یک سندرم شبه تصادفی $\mathbf{s} \in F_۲^{n-k}$ با استفاده از LFSR با مقدار اولیه T تولید می‌شود. آنگاه، یک بردار خطای عمدی به صورت زیر تعریف می‌شود:

$$\mathbf{e}(\mathbf{s}) = \mathbf{s}(\mathbf{H}_{qc}^{-۱})^t \pmod 2, \qquad (۱۳)$$

که در آن $\mathbf{H}_{qc}^{-۱}$[۱] وارون راست ماتریس توازن‌آزمای $\mathbf{H}_{qc}$ در $F_۲$ است.

وابستگی خطی ستون‌های $\mathbf{H}_{qc}$ منجر به صفر شدن بعضی از سطرهای $\mathbf{H}_{qc}^{-۱}$ می‌شود. برای جلوگیری از این نشت، صفرهای ثابت ایجاد شده را می توان با اضافه کردن یک جمله‌ی تصادفی حذف کرد [۱۷]. درنتیجه بردار اغتشاش[۲۶] $\mathbf{e}_p$ را به‌صورت مجموع بردار $\mathbf{e}(\mathbf{s})$ و یک بردار تصادفی $\mathbf{b}(\mathbf{s})$ از طول n تعریف می‌کنیم که مقدار $\mathbf{b}(\mathbf{s})$ در مولفه‌های متناظر با مولفه‌های صفر در $\mathbf{e}(\mathbf{s})$، برابر با یک است:

$$\mathbf{e}_p = \mathbf{e}(\mathbf{s}) + \mathbf{b}(\mathbf{s}) \pmod 2. \qquad (۱۴)$$

مولفه‌های ناصفر در $\mathbf{b}(\mathbf{s})$ را می توان با بردار $\bar{\mathbf{s}}$ (مکمل بردار سندرم $\mathbf{s}$ در $F_۲$) یا دنباله ای از این بیت ها، در حالتی که $n-k < k$ است، پر کرد. به این ترتیب، بردار $\mathbf{e}_p$ یک بردار دودویی با وزن زیاد خواهد بود.

در این بخش به منظور کنترل توان متن رمز شده‌ی ارسالی، روش شکل دهی مکعبی را در الگوریتم رمزگذاری همراه می‌کنیم. در واقع ابتدا تمام نقاط مشبکه Λ را درون ابر مکعب n بعدی حول مبدا منتقل می‌کنیم و عملیات رمزگذاری را مطابق با [۲۸] اجرا می‌کنیم. متن رمزشده‌ی ارسالی روی کانال نویزی به صورت زیر خواهد بود:

$$\mathbf{y} = (۲\mathbf{m}'\mathbf{G}_\Lambda - \mathbf{۱} + ۲\mathbf{e}_p)\mathbf{P}. \qquad (۱۵)$$

چون نقاط کدمشبکه $۲\,(\Lambda \cap \mathcal{L}) - (۱,\ldots,۱)$ در تناظر یک به یک با بردارهای پیام $\mathbf{m}$ هستند، نرخ انتقال سامانه‌ی توأم پیشنهادی برابر است با

$$R = \frac{\log_۲(|\Gamma|)}{n} = \frac{\sum_{i=۱}^{n}\log_۲(L_i)}{n}. \qquad (۱۶)$$

٤-۳- الگوریتم رمزگشایی

گیرنده مجاز سعی در رمزگشایی بردار دریافتی خطا دار شده‌ی $\mathbf{r} = (۲\mathbf{m}'\mathbf{G}_\Lambda - ۱ + ۲\mathbf{e}_p)\mathbf{P} + \mathbf{e}_{ch}$ را دارد که در آن $\mathbf{e}_{ch}$ بردار نویز کانال AWGN با توزیع گوسی و واریانس $\sigma^۲$ است.

با انجام مراحل زیر پیام مورد نظر بازیابی می‌شود:

[۲۵] extended difference family-quasi cyclic-low density parity check

[۲۶] perturbation vector

جدول ۳: مقایسه اندازه‌ی کلید و نرخ انتقال سامانه‌ی کلید متقارن پیشنهادی با دو سامانه‌ی توأم رمزگذاری-کدگذاری اخیر.

سامانه	کد استفاده شده	نرخ انتقال	اندازه‌ی کلید
سامانه‌ی توأم ارائه شده در [۳۱]	کد EDF-QC-LDPC با $(n,k)=(۲۰۴۸, ۱۵۳۶)$ و ۳۲ تغییر	۰/۷۵	۲/۲۲ کیلو بیت
سامانه‌ی مبتنی بر LDLC [۳۴]	مشبکه‌ی LDLC مبتنی بر مربع لاتین با $n = ۱۰^۴$ سمبل	—	۳ مگا بیت
سامانه‌ی توأم پیشنهاد شده در این مقاله	کدمشبکه‌های EDF-QC-LDPC با $(n,k)=(۱۶۰۸, ۱۴۰۷)$ و $l = ۱۶$	۴	۸۸۱ بیت

۱. ضرب $\mathbf{r}$ با $\mathbf{P}^{-۱} = \mathbf{P}^t$ و محاسبه‌ی
$$\mathbf{r}' = \mathbf{r}\mathbf{P}^t = ۲\mathbf{m}'\mathbf{G}_\Lambda - \mathbf{1} + ۲\mathbf{e}_p + \mathbf{e}_{ch}\mathbf{P}^t.$$

۲. محاسبه‌ی بردار اغتشاش $\mathbf{e}_p$ به ازای سندرم متناظر $\mathbf{s}$ و بدست آوردن $\mathbf{r}'' = \mathbf{r}' - ۲\mathbf{e}_p$.

۳. کدگشایی بردار $\mathbf{r}'' = ۲\mathbf{m}'\mathbf{G}_\Lambda - ۱ + \mathbf{e}_{ch}\mathbf{P}^t$. با به‌کارگیری الگوریتم کدگشایی SPA برای مشبکه‌های QC-LDPC ([۲۵])، می‌توان بردار $\overline{\lambda}' = ۲\mathbf{m}'\mathbf{G}_\Lambda - ۱$ را استخراج کرد.

۴. بازیابی پیام $\mathbf{m}$ از بردار مشبکه‌ی شکل دهی شده‌ی $\overline{\lambda}'$ با استفاده از الگوریتم ۱، یعنی $\mathbf{m} = \mathrm{MOD}(\overline{\lambda}')$.

٤-٤- تحلیل

سناریوی حمله با متن اصلی منتخب، یکی از مهمترین حملات است که در تحلیل رمز سامانه‌های شبه Rao-Nam مورد بررسی قرار می‌گیرد [۱۵، ۲۹]. در این سناریو مهاجم توانایی انتخاب مجموعه‌ایی از متن‌های اصلی و متن رمز متناظر با آن‌ها را برای کسب اطلاع از کلید مخفی، دارد. مقاومت سامانه‌های شبه Rao-Nam پیشنهادی در برابر حملات متن اصلی منتخب و راه حل های مناسب برای بهبود امنیت آن در [۲۸] ارائه شده است.

اگر از روش کدگذاری دو مرحله ایی برای مشبکه‌های QC-LDPC استفاده کنیم، پیچیدگی زمانی و فضایی در کدگذاری بردار $\mathbf{m}$ از مرتبه‌ی $O(n-k)$ است. پیچیدگی محاسباتی روش شکل دهی مکعبی برابر با $O(nw_c)$ است که در آن w_c برابر با میانگین وزنی سطرهای $\mathbf{G}_\Lambda$ است. بنابراین پیچیدگی زمانی و فضایی فرآیند رمزگذاری در سامانه‌ی پیشنهادی نسبت به بعد مشبکه، n، خطی است.

به طور مشابه، پیچیدگی محاسباتی الگوریتم کدگشایی مشبکه‌های QC-LDPC از مرتبه $O(nd_vI)$ است که در آن I حداکثر تعداد تکرارهای مورد نیاز الگوریتم برای اصلاح خطاها است و d_v میانگین وزن ستونی ماتریس توازن‌آزمای $\mathbf{H}_{qc}$ است. همچنین داریم $C_{MOD}(\boldsymbol{\lambda}') = O(n-k)$. در نتیجه، پیچیدگی زمانی و فضایی فرآیند رمزگشایی سامانه‌ی پیشنهادی نیز نسبت به بعد مشبکه، n، خطی است.

تعداد بیت مورد نیاز برای ذخیره کردن مقدار اولیه T برابر با $(n-k)$ است. از طرف دیگر، چون وزن هر سطر از $\mathbf{H}_{qc}$ برابر با d_r است، برای ذخیره سازی فشرده شده‌ی سطر اول آن حداکثر $d_r\lceil\log n\rceil$ بیت نیاز است. ماتریس جایگشت $\boldsymbol{\pi}$ را می توان با روش ارائه شده در الگوریتم III از مقاله [۳۰]، به‌وسیله یک بردار اولیه $(q-۱)$ بیتی ساخت و ذخیره کرد. درنتیجه، اندازه‌ی کلید مخفی سامانه‌ی پیشنهادی برابر با $d_r\lceil\log_۲(n)\rceil + (n-k) + (n-k-۱)$ است.

ویژگی‌های عملیاتی طرح پیشنهادی را بر حسب پارامترهای آن در جدول ۴ به طورخلاصه بیان نموده‌ایم، که مشابه بخش قبل، عدد l کران درایه‌های بردار پیام $\mathbf{m}$ و d_r وزن سطری $\mathbf{H_{qc}}$ است.

جدول ۴: ویژگی‌های عملیاتی طرح پیشنهادی برحسب پارامترها.

اندازه متن اصلی	$n\lceil\log_۲(۲l-۱)\rceil$ بیت
اندازه متن رمز	$k\lceil\log_۲(۲l)\rceil + (n-k)\lceil\log_۲(۴l+۲)\rceil$ بیت
اندازه کلید	$d_r\lceil\log_۲(n)\rceil + ۲(n-k) - ۱$ بیت
پیچیدگی رمزگشایی	$O(n)$
پیچیدگی رمزگذاری	$O(n-k)$

با توجه به معادله (۱۶)، نرخ انتقال در سامانه‌ی پیشنهای وقتی $L_i = l$، برای $i = ۱,\ldots,n$، برابر با $R = \log_۲(l)$ است. بنابراین، نرخ انتقال سامانه‌ی توأم رمزگذاری، کدگذاری و مدولاسیون پیشنهادی برای $l = ۱۶$، برابر با $R = ۴$ است که یک مزیت در طراحی برای هر کانال با محدودیت پهنای باند است. برخلاف سامانه‌های توأم رمزگذاری-کدگذاری قبلی که بر اساس کدهای تصحیح خطا طراحی شده‌اند و برای سامانه‌های با محدودیت توان، مناسب هستند، سامانه‌ی پیشنهادی این فصل که بر اساس کدمشبکه‌های QC-LDPC است، برای هر کانال با محدودیت پهنای باند مناسب است و عمل مدولاسیون را نیز به طور همزمان انجام می‌دهد.

در جدول ۳، سامانه‌ی پیشنهادی را با دو سامانه‌ی توأم رمزگذاری-کدگذاری اخیر مقایسه کرده‌ایم. در سامانه‌ی مطرح شده در [۳۱]، بیت‌های کد واژه‌ی متناظر با متن اصلی در یک کد QC-LDPC به صورت تصادفی حذف و اضافه می‌شوند. این سامانه مناسب سامانه‌های با محدودیت توان است، اما اندازه بزرگ کلید آن را غیر عملی ساخته است. الگوریتم‌های رمزگذاری و رمزگشایی سامانه‌ی [۳۴] برابر با $O(n^۲)$ است که نسبت به طرح پیشنهادی در این بخش (پیچیدگی خطی نسبت به بعد مشبکه) از کارآیی مطلوبی برخوردار نیست.

سامانه پیشنهاد شده در این بخش، در برابر تمام حملات موجود به سامانه‌های رمز شبه Rao-Nam مقاوم است. خطی بودن پیچیدگی محاسباتی الگوریتم‌های رمزگذاری و رمزگشایی، کوچک بودن اندازه کلید و نرخ زیاد انتقال پیام در سامانه‌ی پیشنهادی، کارآیی مطلوبی را برای ایجاد یک ارتباط امن و مطمئن روی کانال‌های دارای محدودیت پهنای باند فراهم می‌سازد.

۵- جمع‌بندی

در این مقاله، با استفاده از مشبکه‌ها و کد-مشبکه‌هایی که الگوریتم‌های کدگذاری و کدگشایی آن‌ها به‌صورت کارآ قابل پیاده سازی هستند، به طراحی سامانه‌های رمز کلید متقارن و کلید نامتقارن کارآ پرداخته‌ایم. در بخش اول، یک سامانه‌ی رمز کلید عمومی شبه GGH با استفاده از مشبکه‌های QC-MDPC ارائه کرده‌ایم. سامانه‌ی رمز پیشنهادی دارای کارآیی بهتری نسبت به سامانه‌های رمز مشبکه‌مبنای موجود است. درواقع کارآیی الگوریتم‌های کدگذاری و کدگشایی این مشبکه ها منجر به سرعت زیاد الگوریتم‌های رمزگذاری و رمزگشایی این سامانه در مقایسه با سایر سامانه‌های رمز مشبکه‌مبنا می‌شود. تنک بودن ماتریس توازن‌آزمای این مشبکه‌ها و ساختار شبه دوری ماتریس‌های مولد و توازن‌آزمای آن‌ها، اندازه‌ی کلید کوچکی را برای این سامانه فراهم کرده است. به‌علاوه، تمام حملات شناخته شده به سامانه‌های رمز مشبکه‌مبنا و کدمبنای موجود را به سامانه‌ی پیشنهادی اعمال، و مقاومت آن را بررسی کرده‌ایم. همچنین، نشان داده شد که توسیع پیام سامانه‌ی کلید نامتقارن پیشنهادی کم‌تر از سامانه‌های رمز مشبکه‌مبنا و کدمبنای موجود است. در ادامه مقاله، با توجه به کاربرد مشبکه‌های QC-LDPC در کانال‌های AWGN، از مدولاسیون حاصل از این مشبکه‌ها استفاده کرده و یک سامانه‌ی رمزگذاری کلید متقارن پیشنهاد می‌کنیم. این سامانه سه عمل رمزگذاری، کدگذاری و مدولاسیون را در یک گام واحد انجام می‌دهد. تنک بودن ماتریس توازن‌آزمای این مشبکه‌ها منجر به کوچک بودن اندازه کلید سامانه می‌شود. کارآیی و عملکرد خطای مطلوب این مشبکه‌ها منجر به خطی بودن پیچیدگی زمانی و فضایی الگوریتم‌های رمزگذاری و رمزگشایی و نرخ زیاد انتقال اطلاعات در سامانه شده است. درنتیجه، سامانه‌ی رمزگذاری، کدگذاری و مدولاسیون پیشنهادی، کارآیی مطلوبی را برای ایجاد یک ارتباط امن و قابل اطمینان روی کانال‌های AWGN با پهنای باند محدود فراهم می‌سازد.

مراجع

[1] D. J. Bernstein, J. Buchmann, and E. Dahmen (eds.), "Post-quantum cryptography," Mathematics and Statistics Springer-11649; ZDB-2-SMA, Springer Berlin Heidelberg, 2009.

[2] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/averagecase equivalence". STOC'97 , ACM, NewYork, 1999, pp. 284–293.

[3] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, Aug. 17-21, Lecture Notes in Computer Science, **1294**, Springer, 1997, pp. 112–131.

[4] J. Hoffstein, J. Pipher, J. H. Silverman "NTRU, a ring-based public-key cryptosystem," In: Algorithmic number theory. Lecture Notes in Computer Science, **1423**, pp. 267–288. Springer Berlin Heidelberg, 1998.

[5] J. Hermans, F. Vercauteren, B. Preneel "Speed records for NTRU," Topics in Cryptology - CT-RSA 2010: The Cryptographers' Track at the RSA Conference 2010, Lecture Notes in Computer Science, **5985**, 2010, pp. 73–88. Springer.

[6] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography", Journal of the ACM, **56**, no. 6, 2009, extended abstract in STOC 2005.

[7] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Deep Space Network Progress Report, **42**, no. 44, pp. 114–116, 1978.

[8] E.R. Berlekamp, J.R. McEliece and H. van Tilborg, "On the Inherent Intractibility of Certain Coding Problems," IEEE Trans. Inf. Theory, vol. IT-24, pp. 384–386, May 1978.

[9] M. Baldi, F. Chiaraluce, R. Garello and F. Mininni, "Quasi-cyclic low-density parity-check codes in the McEliece cryptosystem," Proc. IEEE International Conference on Comm. (ICC 2007), Glasgow, Scotland, Jun. 2007, pp. 951–956.

[10] C. Monico, J. Rosenthal and A. Shokrollahi, "Using low density parity check codes in the McEliece cryptosystem," Proc.. IEEE International Symp. on Inf. Theory (ISIT 2000), Sorrento, Italy, Jun. 2000, pp. 215.

[11] M. Baldi and F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes," IEEE International Symposium on Information Theory, ISIT'07, Jun. 2007, pp. 2591–2595.

[12] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes," IEEE International Symposium on Information Theory, ISIT'13, Istanbul, Turkey, Jul. 7-12, 2013, pp. 2069–2073.

[13] M. Baldi, QC-LDPC Code-Based Cryptography,' Springer, Berlin, 2014.

[14] T. N. R. Rao, "Joint encryption and error correction schemes," Proc. 11th annual International Symposium on Computer Architecture, ISCA'84, 1984, pp. 240–241.

[15] T. N. R. Rao and K. H. Nam, "A private-key algebraic-coded cryptosystem," In: Advances in Cryptology, Crypto'86, LNCS, **263**, 1986, pp. 35–48, Springer Berlin Heidelberg.

[16] T. N. R. Rao and K. H. Nam, "Private-key algebraic-code encryptions," IEEE Trans. Inf. Theory, **35**, pp. 829–33, 1989.

[17] A. A. Sobhi Afshar, T. Eghlidos and M. R. Aref, "Efficient secure channel coding based on quasi-cyclic low-density parity-check codes," IET Communications, **3**, pp. 279–292, 2009.

[18] R. Hooshmand, T. Eghlidos and M. Aref, "Improving the Rao-Nam secret key cryptosystem using regular EDF-QC-LDPC codes," ISeCure, **4**, no. 1, pp. 3–14, 2012.

[19] R. Hooshmand, M. K. Shooshtari, and M. R. Aref, "Secret key cryptosystem based on polar codes over binary erasure channel," In Information Security and Cryptology (ISCISC), 10th International ISC Conference on. IEEE, 2013, pp. 1–6.

[20] M. Esmaeili, M. Dakhilalian and T.A. Gulliver, "New secure channel coding scheme based on randomly punctured quasi-cyclic low-density parity check codes," IET Communication, **8**, no. 14, pp. 2556–2562, 2014.

[21] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+SNR)$ on the AWGN channel with lattice encoding and decoding," IEEE Trans. on Inform. Theory, **50**, no. 10, pp. 2293–2314, 2004.

[22] M.-R. Sadeghi, A. H. Banihashemi, and D. Panario, "Low-density parity-check lattices: Construction and decoding

analysis," IEEE Trans. on Inform. Theory, **52**, no. 10, 4481–4495, 2006.
[23] J. Stern, "A method for finding codewords of small weight," Coding Theory and Applications, 3rd International Colloquium, Toulon, France, Nov. 2-4, 1988, pp. 106–113.
[24] S. Ouzan and Y. Be'ery, "Moderate-density parity-check codes," 2009.
[25] H. Khodaiemehr, M.-R. Sadeghi, and A. Sakzad, "Practical encoder and decoder for power constrained QC LDPC-lattice codes," IEEE Transactions on Communications, **65**, no. 2, pp. 486–500, 2017.
[26] K. Bagheri, M. Sadeghi and T. Eghlidos, "An Efficient Public Key Encryption Scheme Based on QC-MDPC Lattices," in IEEE Access, **5**, pp. 25527–25541, 2017.
[27] Q. Guo, T. Johansson, and P. Stankovski, "A key recovery attack on MDPC with CCA security using decoding errors," Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, Dec. 4-8, 2016, pp. 789–815.
[28] K. Bagheri, M.-R. Sadeghi, T. Eghlidos and D. Panario, A secret key encryption scheme based on 1-level QC-LDPC lattices", In Proc. of 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Tehran, Iran, 2016, pp. 20–25.
[29] R. Struik and J. van Tilburg, "The Rao-Nam scheme is insecure against a chosen-plaintext attack," In: Advances in Cryptology, Crypto'87, LNCS, **293**, 1988, pp. 445–457, Springer Berlin Heidelberg.
[30] H. M. Sun and T. Hwang, "Key generation of algebraic-code cryptosystems," Computers & Mathematics with Applications, **27**, pp. 99–106, 1994.
[31] M. Esmaeili and T. A. Gulliver, "Joint channel coding-cryptography based on random insertions and deletions in QC-LDPC codes," IET Communication, **9**, no. 12, pp. 1555–1560, 2015.
[32] T. Fabšič," V. Hromada, P. Stankovski, P. Zajac, Q. Guo, and T. Johansson, "A reaction attack on the QC-LDPC McEliece cryptosystem," Post-Quantum Cryptography : 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, Jun. 26-28, Springer International Publishing, 2017, pp. 51–68.
[33] J. Hoffstein, N. H. Graham, J. Pipher, J. H. Silverman, and W. Whyte, "Hybrid lattice reduction and meet in the middle resistant parameter selection for NTRUEncrypt," Ntru cryptosystems, inc., technical report, 2007.
[34] R. Hooshmand and M. R. Aref, "Efficient secure channel coding scheme based on low-density Lattice codes," IET Communications, **10**, no. 11, pp. 1365–1373, 2016.
[35] R. Hooshmand and M. R. Aref, "Public key cryptosystem based on low density lattice codes," Wireless Personal Communications, **92**, no. 3, pp. 1107–1123, 2017.