دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۱ (۱-۱۴)
https://monadi.isc.org.ir

مروری بر طرح‌های رمزنگاری کدمبنا و روند استانداردسازی رمزنگاری پساکوانتومی: شروع دوره‌ی جدید

آرش خالوان*[۱،۲]، امیرحسین زالی[۱] و محمود احمدیان عطاری[۲]

[۱] آزمایشگاه رمز و شناسه، دانشکده مهندسی برق، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران
[۲] دانشکده مهندسی برق، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۵ بهمن ۱۴۰۲
تاریخ پذیرش: ۱۲ تیر ۱۴۰۳
انتشار آنلاین: ۲۰ تیر ۱۴۰۳

کلمات کلیدی:
رمزنگاری کدمبنا
پردازش کوانتومی
سیستم Niederreiter
رمزنگاری پساکوانتوم
رمزنگاری کلید عمومی

نوع مقاله: مروری

چکیده

با ظهور کامپیوترها و الگوریتم‌های کوانتومی، امنیت سیستم‌های رمزنگاری کلید عمومی کنونی می‌تواند با چالش روبرو شود. شکسته‌شدن ساختارهای رمزنگاری کنونی نیازمند کامپیوترهای کوانتومی چند میلیون کیوبیتی است که تاکنون ساخته نشده‌اند؛ اما با پیشرفت چشمگیر در فناوری ساخت تجهیزات کوانتومی در شرکت‌های پیشرو در این حوزه و احساس خطر جامعه‌ی رمزنگاری، احساس نیاز شد تا سریعاً راهکارهایی برای مقابله ارائه شود. در سال ۲۰۱۶ موسسه ملی استاندارد و فناوری (NIST) برای حل این مسئله خواستار پیشنهادهایی از سراسر دنیا برای استانداردسازی طرح‌های رمزنگاری پساکوانتومی شد. در آن زمان سیستم رمز کدمبنای McEliece (و سیستم Niederreiter معادل آن) با وجود اثبات مقاومت در برابر الگوریتم‌های کلاسیک و کوانتومی، به علت کلیدهای عمومی بزرگ مورد پذیرش قرار نگرفت. در آخر، سیستم‌های رمز Classic McEliece، HQC و BIKE سیستم‌های رمز در دسته‌ی رمزنگاری کدمبنا هستند که به مرحله نهایی این مسابقات راه یافته‌اند و منتخبین این دسته‌ی رمزنگاری نهایتا تا پایان سال ۲۰۲۴ معرفی خواهند شد. در این مقاله تلاش شده‌است تا علاوه بر مرور تحولات صورت گرفته برای بهینه‌سازی ساختارهای کدمبنا، طرح‌های رمزنگاری کدمبنای منتخب و آخرین وضعیت استانداردسازی Classic McEliece نیز بررسی شود.

۱ مقدمه

امنیت اطلاعات یک موضوع اساسی و فوری در عصر تحول دیجیتال است. در حال حاضر در سراسر جهان برای حفاظت از اطلاعات در بستر اینترنت و تمامی شبکه‌های ارتباط کامپیوتری از الگوریتم‌های رمز نظریه‌ی اعدادی مانند RSA (یا الگوریتم‌های با ساختار مشابه) استفاده می‌شود که این الگوریتم‌ها بر سختی حل مسائل لگاریتم گسسته و فاکتورگیری اعداد صحیح تکیه دارند. الگوریتم رمز RSA برای اولین‌بار در سال ۱۹۷۸ توسط ریوست، شامیر و آدلمن [۱] عنوان یک الگوریتم رمز کلید عمومی با قابلیت پیاده‌سازی به دنیا معرفی شد.

تا سال ۱۹۹۷ میلادی باور جامعه رمزنگاری و به تبع آن متخصصان علم ریاضیات بر این بود که مسئله تجزیه اعداد صحیح بزرگ، از نظر محاسباتی جزء مسائل سخت رمزنگاری محسوب می‌شود. سختی این مسئله برای کامپیوترهای کلاسیک کاملاً درست است.

پس از مقاله‌ی معروف پروفسور آمریکایی پیتر شور[1] [۲] ارائه الگوریتم کوانتومی با توانایی شکستن سیستم‌های رمز مبتنی بر مسائل

[1] Shor

*نویسنده مسئول
آدرس‌های رایانامه: a.khalvan@email.kntu.ac.ir (آرش خالوان)، a.zali1@email.kntu.ac.ir (امیرحسین زالی)، mahmoud@eetd.kntu.ac.ir (محمود احمدیان عطاری)

سخت نظریه اعداد همانند تجزیه اعداد صحیح بزرگ و لگاریتم گسسته توسط پردازنده‌های کوانتومی، تمامی معادلات امنیت برهم ریخت. از سوی دیگر باتوجه به رشد سریع پردازنده‌های دیجیتال و مقدور نبودن دستیابی به ابعاد کوچک‌تر از نانومتر، به منظور افزایش توان محاسباتی و غلبه بر محدودیت‌های موجود در سیستم‌های دیجیتال، مشخص شد که پردازنده‌های مبتنی بر معماری کوانتوم به طور حتم جایگزین پردازنده‌های دیجیتال خواهند شد.

کامپیوتر کوانتومی نوعی پردازشگر است که از اصول مکانیک کوانتومی برای انجام محاسبات استفاده می‌کند. برای مثال، کامپیوترهای کوانتومی می‌توانند مسائل ریاضی خاصی مانند فاکتورگیری اعداد صحیح بزرگ را حل کنند که انجام آن از نظر محاسباتی برای کامپیوترهای کلاسیک در زمان چندجمله‌ای غیرممکن است.

مشکلات امنیتی اصلی که پردازنده‌های کوانتومی می‌توانند ایجاد کنند در حوزه‌ی مربوط به رمزنگاری کلید عمومی است، اما این مشکلات در رمزنگاری کلید خصوصی به این شکل وجود ندارند. در الگوریتم کوانتومی که گرور[1] در سال ۱۹۹۶ معرفی کرد [۳]، نشان داد برای جستجو در یک پایگاه‌داده بدون ساختار شامل N عضو می‌توان پیچیدگی جستجو در کامپیوترهای کلاسیک را از $\mathcal{O}(N)$ به $\mathcal{O}(\sqrt{N})$ کاهش داد. ثابت شده است که الگوریتم گرور بهینه است و هیچ الگوریتم کوانتومی نمی‌تواند بیش از این الگوریتم، جستجو در یک پایگاه داده نامرتب را بهبود ببخشد [۴]. با ظهور کامپیوترهای کوانتومی و بکارگیری الگوریتم گرور، طول کلید موثر الگوریتم‌های رمزنگاری کلید خصوصی نصف می‌شود اما در رمزنگاری کلید خصوصی، با توجه به وجود یک کانال امن پیش از شروع ارتباط که کلیدهای مربوطه بین طرفین ارتباط از طریق آن جابجا می‌شود، محدودیت قابل توجهی برای افزایش طول کلیدها وجود ندارد. در نتیجه با هزینه‌ی بسیار اندک مثل افزایش دو برابری طول کلیدها، اکثر سیستم‌های رمزنگاری کلید خصوصی استاندارد، همانند AES و DES در مقابل حملات کوانتومی شناخته شده امن باقی می‌مانند و شکستن آن‌ها در زمان چندجمله ای میسر نخواهد بود.

در رمزنگاری کلید عمومی با توجه به الگوریتم‌های اثبات شده و پیاده‌سازی شده‌ی شور و گرور [۳] و با توجه به نبود یک کانال امن برای مبادله‌ی کلیدهای رمزنگاری، در صورتی که سال‌های حیاتی پیش از کوانتوم را از دست بدهیم و در مقابل پردازنده‌های کوانتومی بتوانند به رشد مورد انتظارشان برسند عملاً با یک مشکل جهانی روبرو خواهیم شد و به همین دلیل است که NIST بر لزوم انجام کار در حوزه رمزنگاری کلید عمومی اهتمام ورزیده است.

برای غلبه بر تهدید پردازشگرهای کوانتومی، باید روش‌ها و تکنیک‌هایی جایگزین شوند که علاوه بر داشتن امنیت مناسب، سیستم‌های ارتباطی موجود را با چالش مواجه نکنند. یکی از راهکارهای مقابله با مهاجمان مجهز به پردازنده‌ی کوانتومی، استفاده از رمزنگاری پساکوانتومی[2] است و سیستم‌های رمزنگاری کدمبنا یک نمونه از ساختارهای پساکوانتومی هستند. سیستم‌های رمزنگاری پساکوانتومی بر روی ۵ ساختار زیر متمرکز هستند:

(۱) Lattice-based Cryptography
(۲) Code-based Cryptography
(۳) Hash-based Cryptography
(۴) Multivariate-based Cryptography
(۵) Isogeny-based Cryptography

پساکوانتومی بودن یک سیستم به این معناست که جنس محاسبات به دنیای کلاسیک کنونی تعلق دارد؛ اما هیچ الگوریتم کلاسیک و کوانتومی برای شکستن آن وجود ندارد. به عبارت دیگر رمزنگاری پساکوانتومی با سامانه‌های رمزی سروکار دارد که در کامپیوترهای مرسوم اجرا می‌شوند؛ ولی در برابر کامپیوترهای کوانتومی امن هستند.

با توجه به اثبات سخت بودن مسئله‌ی کدبرداری از یک پیام کدشده، بدون در اختیار داشتن چندجمله‌ای مولد [۵] و همچنین سرعت بالای انجام عملیات‌های باینری در سیستم‌های کدگذاری، مزایای سیستم‌های رمزگذاری و رمزگشایی در سیستم‌های باینری کدمبنا نمایان شدند و نهایتاً این ساختار به پیشنهاد ناسا توسط McEliece در سال ۱۹۷۸ طراحی و اجرا شد [۶]. با اثبات مقاوم بودن ساختارهای رمزنگاری کدمبنا در مقابل پردازش کوانتومی، بر اهمیت و مزایای این ساختارها افزوده شده و مورد توجه جامعه رمزنگاری قرار گرفت.

سیستم رمز McEliece اولین نمونه‌ی معرفی‌کننده‌ی رمزنگاری پساکوانتومی است [۶]. نقطه ضعف کلید عمومی بزرگ در نمونه اصلی McEliece (که در محدوده بین ۵۰ تا ۱۰۰ کیلوبایت است) و نرخ انتقال پایین اطلاعات در مقایسه با سایر ساختارهای رمزنگاری کلید عمومی، تاکنون از کاربردهای آن در دنیای واقعی جلوگیری کرده است اما مقاومت آن در برابر پردازش کوانتومی امروزه بر اهمیت آن افزوده است.

در حالی که کامپیوتر کوانتومی در مقیاس بزرگ در زمان نگارش این مقاله با واقعیت فاصله دارد، توجه به PQC از اهمیت ویژه‌ای برخوردار است و چند دلیل را می‌توان در اینجا فهرست کرد [۷]:

آماده سازی: توسعه الگوریتم‌های PQC اجازه می‌دهد تا جامعه‌ی رمزنگاری برای تهدیدات آینده رایانه‌های کوانتومی آماده شود. سیستم های رمزنگاری اغلب برای محافظت از داده‌ها برای دوره‌های طولانی استفاده می‌شوند، بنابراین ضروری است که از هم اکنون برنامه‌ریزی برای احتمال حملات کوانتومی آغاز شود.

طول عمر: الگوریتم های PQC برای ایمن‌سازی در برابر حملات کلاسیک و مبتنی بر پردازش کوانتومی طراحی شده‌اند. این بدان معناست که حتی اگر قدرت محاسباتی ساختارهای کلاسیک نیز به افزایش خود ادامه دهد، آن‌ها امن خواهند ماند.

[1] Grover [2] Post Quantum Cryptography

جدول ۱. مقایسه سیستم‌های رمز RSA، McEliece و Niederreiter

پارامترها	Niederreiter	McEliece	RSA
طول قالب اطلاعات (بیت)	۲۸۴	۵۲۴	۱۰۲۴
طول کلید (بایت)	۳۲۷۵۰	۶۷۰۷۲	۲۵۶
نرخ	۰/۵۷	۰/۵۱	۱
تعداد عملیات در رمزگذاری به ازای هر بیت	۵۰	۵۱۴	۲۴۰۲
تعداد عملیات در رمزگذاری به ازای هر بیت	۷۸۶۳	۵۱۴۰	۷۳۸۱۱۲

پذیرش: توسعه، آزمایش و پذیرش سیستم های رمزنگاری به زمان نیاز دارد. با شروع کار بر روی الگوریتم‌های PQC، می‌توان اطمینان حاصل کرد که در صورت نیاز، جایگزین‌های مناسبی برای سیستم‌های رمزنگاری فعلی وجود خواهد داشت.

با خطر احساس شده از جانب کامپیوترهای کوانتومی به جامعه‌ی رمزنگاری جهانی، NIST در سال ۲۰۱۶ فراخوانی را برای ارسال طرح‌های پساکوانتومی در حوزه‌های رمزنگاری کلید عمومی، امضای دیجیتال و تبادل کلید اعلام کرد که نتایج نهایی آن قرار است در سال ۲۰۲۴ منتشر شده و استانداردهایی را برای این حوزه معرفی کنند. گزارش‌های NIST با محوریت فضای پساکوانتومی، محققان تمامی حوزه‌های مرتبط را برای ورود به فضای PQC تشویق می‌کند و تأکید بسیار زیادی بر آن دارد تا جایی که این ورود و مهاجرت را بسیار ارزشمندتر از رسیدن به سطوح بالاتر امنیت می‌داند.

در مطالعه اخیر گیدنی و همکاران [۸]، نشان داده شد که کیوبیت منطقی مورد نیاز برای تجزیه‌ی یک عدد n بیتی از رابطه‌ی $3n+0.002n\log n$ محاسبه می‌گردد که بر اساس فرضیات معقول در مورد خطای گیت معماری پردازنده‌ی کوانتومی، زمان چرخه و سایر پارامترها، می‌توان تخمین زد که اگر ۲۰ میلیون کیوبیت فیزیکی در دسترس باشد، یک الگوریتم رمز کلید عمومی RSA 2048 بیتی را می‌شود در عرض ۸ ساعت تجزیه کرد. با توجه به روند روبه‌رشد شرکت‌های فناور در حوزه‌ی ساخت تجهیزات کوانتومی پیش‌بینی می‌شود حصول این تعداد کیوبیت فیزیکی به کمتر از ۲۰ سال زمان نیاز دارد.

در جدول ۱ یک مقایسه بین سیستم‌های رمز McEliece، RSA و Niederreiter انجام شده است.

۲ مسائل سخت نظریه کدگذاری

تقریباً تمامی ساختارهای رمزنگاری کدمبنا بر سه مسئله‌ی سخت یا تعمیم‌هایی از آن‌ها استوار هستند که همگی در زیر آورده شده‌اند.

مسئله‌ی کدگشایی عام: به ازای یک کد C با $[n,k]$ روی میدان $\mathbb{F}_q$، عدد صحیح t و بردار دریافتی $c\in\mathbb{F}_q^n$، کلمه کد $x\in C$ را به نحوی بیابید که $d(x,c)\le t$ باشد.

مسئله‌ی کدگشایی سندروم: به‌ازای ماتریس بررسی توازن H و بردار s که هردو در $\mathbb{F}_q$ هستند و عدد صحیح غیرمنفی t، بردار $xc\in\mathbb{F}_q^n$ با وزن همینگ $wt(x)=t$ را به نحوی بیابید که $Hx^T=s^T$.

مسئله‌ی تمایز کد Goppa: به ازای ماتریس بررسی توازن $H_{r\times n}$ نشان دهید که این ماتریس متعلق به یک کد Goppa می‌باشد.

با این حال در سال ۲۰۱۳ تیلیچ و همکارانش [۹] نشان دادند که کدهای دودویی Goppa با نرخ بالا را می‌توان از کدهای خطی تصادفی متمایز کرد اما این نتایج برای حمله به ساختار McEliece کافی نبود. با روش حمله‌ی مطرح شده در [۹] در مقابل سیستم رمز McEliece با طول ۱۰۲۴، نهایتا وجود ۸ خطا قابل تشخیص بود، اما در این ساختار تعداد خطاها برابر ۵۰ است. در [۱۰] نیز نویسندگان روشی را معرفی کردند که در آن چندجمله‌ای اولیه ساختارهای با نرخ بالای کدهای Goppa که در [۹] ثابت شده بود قابل تشخیص هستند را استخراج کردند اما این روش نیز به کدهای بسیار محدودی قابل تعمیم بود.

۳ ساختار McEliece

به طور کلی برای هر چندجمله‌ای درجه‌ی t روی $GF(2^m)$، یک کد گوپای باینری ساده نشدنی با طول $n=2^m$ و بعد $k\ge n-tm$، با قابلیت تصحیح حداقل t خطا وجود دارد. با توجه به این نکته طراح سیستم با انتخاب هر m و t دلخواه می‌تواند یک چندجمله‌ای از درجه‌ی t را به صورت کاملاً اتفاقی روی میدان $GF(2^m)$ انتخاب کند و با توجه به اینکه یک الگوریتم سریع برای بررسی تجزیه‌پذیری یک چندجمله‌ای از درجه‌ی t روی یک میدان متناهی وجود دارد (این احتمال در حدود $\frac{1}{t}$ است) می‌تواند به سرعت یک چندجمله‌ای مناسب برای ساخت یک کد گوپای باینری را بدست آورد. پس از انتخاب چندجمله‌ای مطلوب، طراح می‌تواند ماتریس مولد $G_{(k\times n)}$ یک کد گوپای باینری را به فرم سیستماتیک بدست آورد که از همان کد در ساختار رمزگذاری استفاده می‌شود. McEliece پارامترهای سیستم خود را $[n,k,t]=[1024,524,50]$ در نظر گرفت.

۴ رمزگذاری و رمزگشایی در ساختار McEliece

رمزگذاری در سیستم McEliece بدین نحو انجام می‌شود که ابتدا اطلاعات به بلوک‌های k بیتی تقسیم می‌شوند و در نهایت بردار $c=mG'+e$ به عنوان متن رمز ارسال می‌شود. G' ماتریس مولد کلید عمومی و به فرم $G'=SGP$ و e از یک بردار تصادفی با طول n و وزن t ساخته شده است. در رابطه‌ی مربوطه به ماتریس مولد کلید عمومی، S یک ماتریس ناویژه تصادفی، P یک ماتریس جایگشت تصادفی و G ماتریس مولد یک کد گوپای باینری است.

در رمزگشایی سیستم رمزگذاری McEliece، با دریافت بردار c در گیرنده، ابتدا با ضرب معکوس ماتریس جایگشت P از راست، عبارت $c'=cP^{-1}=mSG+eP^{-1}$ محاسبه می‌شود. چون P^{-1} یک

ماتریس جایگشت است، وزن e در عبارت eP^{-1} را دستخوش تغییر نمی‌کند و مشکلی برای کدگشایی ایجاد نمی‌کند. با استفاده از الگوریتم کدبرداری پترسون[1] می‌توان $c^{2} = \mathrm{Decode}(c^{1}) = mS$ را محاسبه کرد [۶]. در پایان با ضرب معکوس ماتریس S در رابطه c^{2}، پیام به شکل $c^{3} = c^{2}S^{-1} = mSS^{-1} = m$ محاسبه می‌شود.

۵ رمزگذاری و رمزگشایی در ساختار Niederreiter

در ساختار رمز Niederreiter نیز مانند سیستم رمز McEliece از کدهای قالبی خطی استفاده شده است و تنها تفاوت، استفاده از ماتریس بررسی توازن به‌جای ماتریس مولد بکار رفته در ساختار McEliece است که مطابق جدول ۱، طراح از همین نکته جهت کوتاه کردن کلید عمومی بهره برده است [۱۱].

الگوریتم رمزگذاری در این ساختار به شکل زیر است: $P_{n\times n}$ را یک ماتریس جایگشت تصادفی و $M_{r\times r}$ را ماتریس ناویژه تصادفی در نظر بگیرید. طراح سیستم با انتخاب یک ماتریس بررسی توازن مناسب H، ماتریس مولد کلید عمومی را به شکل $H' = MHP$ می‌سازد. در عملیات رمزگذاری ابتدا متن اصلی به قالب‌هایی k بیتی تقسیم می‌شود که با استفاده از یک تابع یک به یک φ، به یک الگوی خطای n بیتی با وزن t نگاشت می‌شود و سپس به یک بردارمشخصه‌ی[2] متناظر به عنوان قالب متن رمزی تبدیل می‌شود. به طور خلاصه:

$$e = \varphi(m) \qquad (۱)$$

$$c = eH'^{T} \qquad (۲)$$

در رمزگشایی ابتدا متن رمزی به قالب‌هایی به طول $r = n - k$ تقسیم شوند و مرحله‌ی اول رمزگشایی مطابق رابطه‌ی (۳) انجام می‌شود:

$$c^{1} = c\left(M^{T}\right)^{-1} = e\left(P^{T}\right)H^{T} \qquad (۳)$$

در مرحله‌ی بعد باتوجه به وجود یک الگوریتم کدگشایی سریع برای کدهای قالبی خطی با ماتریس مولد H،

$c^{2} = \mathrm{Decode}(c^{1}) = e(P^{T})$ به دست می‌آید. در نهایت با محاسبه‌ی $c^{3} = c^{2}(P^{T})^{-1} = e(P^{T})(P^{T})^{-1} = e$ الگوی خطای مربوطه بدست می‌آید و با محاسبه‌ی معکوس تابع یک به یک به شکل $m = \varphi^{-1}(e)$، پیام بدست می‌آید.

۶ کاهش طول کلید عمومی در ساختار McEliece

استفاده از کدهای GRS[3] به جای کد گوپا برای نخستین‌بار توسط H. Niederreiter در سال ۱۹۸۶ مطرح شد [۱۱]. در این سیستم در مقایسه با ساختار اصلی McEliece چون قابلیت استفاده از حالت سیستماتیک کلید فراهم بود و با توجه به ابعاد k و n، طول کلید عمومی را نصف می‌کرد و نرخ ارسال را نیز اندکی افزایش می‌داد. این سیستم در ابتدا به قدری قدرتمند ظاهر شد که به عنوان پایه‌ی امضای دیجیتال معرفی شد؛ اما در [۱۲] مشخص شد که این ساختار امنیت لازم برای استفاده در رمزنگاری را ندارد. اگر در سیستم رمز معرفی شده توسط Niederreiter از کد گوپا استفاده شود آنگاه سیستم‌های رمز Niederreiter و McEliece معادل امنیتی خواهند بود که این موضوع در [۱۳] اثبات شده است.

از تلاش‌های دیگر برای کوتاه کردن طول کلید عمومی می‌توان به سیستم مبتنی بر کدهای Reed-Muller اشاره کرد که در سال ۲۰۰۷ توسط مایندر و شکراللهی با یک حمله ساختاری شکسته شد [۱۴] و سیستم مبتنی بر کدهای الحاقی[4] نیز در سال ۱۹۹۴ وقتی معلوم شد از روی جایگشت ماتریس تبدیل قابل بازیابی است، کنار گذاشته شد [۱۵].

از روش‌های بکار رفته به منظور فشرده‌سازی کلید عمومی سیستم رمزنگاری کدمبنا، می‌توان به ساختارهای شبه دوری در کدهای BCH [۱۶] و Alternant [۱۷] اشاره نمود که البته هر دو سیستم به ترتیب در [۱۸] و [۱۹] شکسته شده‌اند.

سیستم مبتنی بر کدهای BCH [۱۶] در سال ۲۰۰۵ توسط گابوری مطرح شد که در آن از کدهای شبه دوری روی میدان‌های کوچک برای کاهش طول کلید استفاده می‌شد. در این ساختار برای حفظ ساختار شبه دوری نوع خاصی از ماتریس جایگشت بکار گرفته شده بود که سیستم را آسیب‌پذیر می‌ساخت و نهایتا در [۱۹] شکسته شد.

بالدی در سال ۲۰۰۷ روی کدهای شبه دوری QC-LDPC[5] متمرکز شد و با استفاده از ویژگی شبه دوری و قدرت تصحیح خطای کد توانست طول کلید را کاهش و نرخ ارسال را افزایش دهد [۲۰]. در [۲۱] حمله‌ای مؤثر به این ساختار با این فرض که طول کد به‌صورت توانی از ۲ باشد انجام شد؛ اما طولی نکشید که سیستم بالدی با یک حمله ساختاری به‌کلی شکسته شد [۱۸]. این ساختار مجدداً در [۲۲، ۲۳] توسط کوچک شوشتری و همکارانش به طور مؤثر شکسته شد.

یک‌روند بسیار محبوب در رمزنگاری مبتنی بر کد، کاهش اندازه کلید عمومی با تمرکز بر زیر کلاس‌های کدهای جایگزین گوپا است که ماتریس عمومی بسیار فشرده، معمولاً شبه چرخه‌ای (QC)، شبه دیادیک (QD)، یا ماتریس‌های شبه مونوئیدی (QM) است. پیشنهاد استفاده از این کدها برای کاهش اندازه کلید عمومی از چند صدهزار بیت (۵۰۰ کیلوبیت برای پیشنهاد اصلی) به تنها ۲۰ کیلوبیت است [۲۴، ۲۵]. برای مثال در [۲۵] ساختاری بر اساس کدهای Srivastava تعمیم‌یافته معرفی شد که یک کلاس بزرگ‌تر از کدهای Goppa به عنوان یک مورد خاص است و کلیدهای عمومی نسبتاً کوتاه‌تری را تولید می‌کند.

ایده این ساختارها تولید کل ماتریس از طریق جایگشت‌های سطر اول است. علاوه بر این، این ساختارها امکان رمزگذاری پیام را بدون محاسبه کل ماتریس و فقط با استفاده از سطر اول فراهم می‌کنند. در

[1] Patterson [2] Syndrome [3] Generalized Reed-solomon

[4] Cancatenated code [5] Quasi Cyclic Low Density Parity Check

این ساختارها همان دلیلی که اجازه ساخت یک کلید عمومی فشرده را می‌دهد، مشکل بازیابی کلید را ذاتاً آسان‌تر می‌کند و اینگونه ساختارها با توجه به حمله‌ی مطرح شده در [۲۶] به علت وجود ساختارهای تکراری و امکان شکستن قسمت‌های کوچک‌تری از ساختار اصلی و تعمیم آن به کل، احتمال شکستن ساختار آن‌ها را افزایش می‌دهد. به عبارت دیگر نکته اساسی در حمله‌ی مطرح شده در [۲۶] در این است که از ماتریس مولد عمومی $k \times n$ یک McEliece فشرده، می‌توان یک ماتریس مولد $\frac{k}{p} \times \frac{n}{p}$ ساخت که از نقطه‌نظر مهاجم به خوبی کلید عمومی اولیه است و با شکستن آن کلید کوچک‌تر، کل ساختار را می‌شکند.

در سال ۲۰۱۰ برنشتین و همکارانش یک بار دیگر استفاده از کدهای Goppa غیرباینری را بنام Wild McEliece دنبال نمودند [۲۷] و در حالی که به نظر می‌رسید طرحشان بسیار موفق است در سال ۲۰۱۴ در [۲۸] شکسته شد.

در سال ۲۰۱۲، میزوسکی و همکارانش سیستم رمز دیگری مبتنی بر کدهای MDPC [1] و نوع شبه دوری آن (QC-MDPC [2]) ارائه دادند و نشان دادند که می‌توان از این کدها در سیستم رمزنگاری McEliece استفاده کرد و کلید عمومی را به تنها ۰٫۶ کیلوبایت کاهش داد تا به سطح امنیتی ۸۰ بیتی دست یابد [۲۹]. با وجود موفقیت‌هایی که این ساختار به نظر می‌رسید به دست آورده است در [۳۰] با شناسایی یک وابستگی بین کلید مخفی و شکست‌های رمزگشایی [3] با یک حمله‌ی بازیابی این ساختار نیز شکسته شد. این حمله جدید از همبستگی قوی بین ساختارهای خاص در کلید مخفی و احتمال خطای رمزگشایی هنگام استفاده از خطاهای با الگوهای مرتب استفاده می‌کند. سپس با اجرای یک رویه بازسازی، چندجمله‌ای مولد مخفی را به طور مؤثر بازسازی می‌کند، بنابراین طرح QC-MDPC را می‌شکند.

مدتی بعد در سال ۲۰۱۲ یک سیستم مبتنی بر کدهای کانولوشنی معرفی شده است [۳۱] اما در [۳۲] با مشخص شدن ضعف آن، با یک حمله‌ی ساختاری درهم شکست.

در سال ۲۰۱۴ سیستم رمز کلید عمومی مبتنی بر کدهای قطبی [4] در [۳۳] مطرح شد که در [۳۴] نیز با استفاده از ویژگی‌های کدهای قطبی و معرفی یک رویکرد کارآمد، اندازه کلیدهای عمومی و مخفی و پیچیدگی محاسباتی را در مقایسه با سیستم رمزنگاری McEliece کاهش دادند. این ساختار نیز در سال ۲۰۱۶ در [۳۵] شکسته شده است.

در [۳۶] نیز یک روش جدید، بر اساس کدهای با متریک رتبه پیشنهاد شد که آن طرح نیز در [۳۷] با دو روش مختلف شکسته شد. نهایتاً در سال ۲۰۱۶ NIST با توجه به طولانی‌شدن روند یافتن یک ساختار رمز پساکوانتومی مقاوم در برابر پردازش کوانتومی و حساسیت از دست دادن سال‌های حیاتی پیش از ورود تجهیزات کوانتومی، تصمیم گرفت تا با ساماندهی این فرایند به این روند سرعت ببخشد و محققان را تشویق کند تا بادقت و تلاش بیشتری برای ارتقای این حوزه عمل کنند.

۷ استانداردسازی PQC

به عنوان اولین گام مهم به سمت پذیرش PQC در مقیاس وسیع، NIST خواستار پیشنهادهایی برای استانداردسازی طرح‌های رمزنگاری پساکوانتومی و به ویژه سه نمونه اصلی یعنی رمزگذاری کلید عمومی (Public Key Encryption)، امضای دیجیتال (Digital Signature) و مکانیسم‌های کپسوله‌سازی کلید (Key Encapsulation Mechanism) شد [۳۶] که به عنوان ابزارهای رمزنگاری کلید عمومی در نظر گرفته می‌شوند و سه معیار زیر را برای ارزیابی طرح‌های PQC مد نظر گرفته است:

- امنیت
- هزینه و عملکرد
- الگوریتم و ویژگی‌های پیاده‌سازی

الگوریتم‌های بسیاری از سراسر دنیا که ادعای پساکوانتومی بودن داشتند به NIST ارسال شدند؛ اما تنها تعداد کمی از آنها به دور پایانی راه یافتند که ما منتظر استانداردسازی نهایی این سیستم رمزنگاری هستیم و NIST قصد دارد مجموعه‌ای از الگوریتم‌های رمزنگاری را بر اساس خانواده‌های مختلف سیستم‌های رمزنگاری به جای یک برنده منفرد انتخاب کند تا ریسک تحلیل رمز بالقوه آن نامزد منتخب را کاهش دهد و در عوض گزینه‌های بازگشتی به راحتی در دسترس باشد [۳۸].

تعداد ۶۹ مقاله برای این فراخوان از سوی NIST مجاز خوانده شدند که در [۳۹] منتخبین مختلفی که از دور اول به دور دوم راه یافتند، مورد بررسی قرار گرفته است. الگوریتم‌های واجد شرایط مرحله دوم برای مکانیسم کپسوله‌سازی کلید عبارت بودند از:

CRYSTALS-KYBER, NTRU Prime, SIKE, FrodoKEM, LAC, BIKE, LEDAcrypt, NTRU Prime, NewHope, NTRU, NTS-KEM, ROLLO, NTRU Prime, RQC, Round5, SABER.

در بخش امضای دیجیتال، ۹ طرح به نام های

qTESLA, CRYSTALS-DILITHIUM, FALCON, GeMSS, Rainbow, MQDSS, SPHINCS+, Picnic, LUOV

به دور بعد رسیدند. در [۴۰] عملکرد الگوریتم‌های معرفی شده فوق را بررسی و آن‌ها را با هم مقایسه کرده است.

پس از مدتی به عنوان بخشی از برنامه رمزنگاری پساکوانتومی NIST، منتخبین مرحله سوم و نیمه‌نهایی انتخاب شدند. چهار سیستم رمزنگاری وجود داشت که از آن‌ها برای رمزگذاری کلید عمومی (PKE) و مدیریت استقرار کلید (PKE) می‌توان استفاده کرد که عبارت‌اند از:

- Classic McEliece
- SABER

[1] Moderate Density Parity Check [2] Quasi Cyclic Moderate Density Parity Check [3] Decoding Failure Rate [4] Polar Code

- CRYSTALS-KYBER
- NTRU

برای دسته امضای دیجیتال، سه ساختار موفق شدند به‌دور نهایی برسند که عبارت‌اند از:

- CRYSTALS-DILITHIUM
- FALCON
- Rainbow

در مجموع ۸ الگوریتم به عنوان الگوریتم‌های جایگزین (PKE/KEM و DSA) انتخاب شدند. پنج جایگزین برای رمزگذاری کلید عمومی و مدیریت ایجاد کلید (PKE/KEM) وجود دارد که عبارتند از:

- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

سه الگوریتم نیز کاندیدای الگوریتم امضای دیجیتال (DSA) هستند که عبارت‌اند از:

- GeMSS
- Picnic
- SPHINCS+

در [۴۱] تمامی نامزدهای نهایی NIST بررسی شده است.

از میان ۱۵ طرح نهایی و رزرو انتخابی در دور سوم، طرح Classic McEliece به‌عنوان تنها نماینده‌ی گروه اصلی از خانواده‌ی سیستم‌های رمز کدمبنا که از کد گوپا در سامانه رمز نیدریتر (سامانه رمز کدمبنای ارائه شده توسط نیدریتر در سال ۱۹۸۶ که از لحاظ امنیتی با سامانه رمز McEliece معادل است) استفاده می‌کند، باقی‌مانده است که این طرح امنیت IND-CCA2 [1] برای مقابله با انواع حملات فراهم می‌کند [۴۲].

طرح‌های Bit flipping Key Encapsulation که از نوع شبه دوری کدهای MDPC استفاده می‌کند [۴۳] و Hamming Quasi-Cyclic که بر اساس کدهای شبه دوری همینگ است [۴۴] به دسته رمزنگاری کدمبنا اختصاص دارند که در دسته‌ی رزرو قرار دارند. نامزدهای باقی مانده در دور چهارم که در سال ۲۰۲۲ برگزار شد با هم رقابت کردند و در نهایت نامزدهایی از هر دسته به عنوان نامزد نهایی نهایتا تا سال ۲۰۲۴ انتخاب خواهد شد[۴۵]. در جدول‌های ۲ و ۳ ما خلاصه ای از این نامزدها را آورده‌ایم.

پس از برگزاری دور چهارم این استانداردسازی، ۴ طرح برنده شدند که سه طرح در دسته‌ی Lattice-Based و یک طرح در دسته‌ی Hash-Based قرار دارند، ۴ طرح راهی آخرین مرحله شدند و سایر طرح‌ها شکست خوردند [۴۶] و جدول ۴ خلاصه‌ی آخرین نتایج در پایان مرحله‌ی چهارم

[1] Indistinguishability under Adaptive Chosen Ciphertext Attack

جدول ۲. لیست کامل الگوریتم‌های [۴۵] PQC Round-3 گروه اصلی

S/No	Algorithm PQC	Type	Mechanism
۱	McEliece Classic	Code-Based	KEM / PKE
۲	CRYSTALS-KYBER	Lattice-Based	KEM / PKE
۳	NTRU	Lattice-Based	KEM / PKE
۴	SABER	Lattice-Based	KEM / PKE
۵	CRYSTALS-DILITHIUM	Lattice-based	Signature Digital signature
۶	FALCON	lattice-based	Signature Digital signature
۷	Rainbow	Multivariate-based	Signature Digital

جدول ۳. لیست کامل الگوریتم‌های PQC Round-3 [۴۵]گروه جایگزین

S/No	Algorithm PQC	Type	Mechanism
۱	BIKE	Code-Based	KEM / PKE
۲	FrodoKEM	Lattice-Based	KEM / PKE
۳	(Hamming HQC Quasi-Cyclic)	Code-Based	KEM / PKE
۴	Prime NTRU	Lattice-Based	KEM / PKE
۵	SIKE	Isogeny-Based	KEM / PKE
۶	GeMSS	Multivariate-Based	Signature Digital
۷	Picnic	Hash-based	Signature Digital
۸	SPHINCS+	Hash-based	Signature Digital

شکل ۱. خلاصه‌ی فرایند استانداردسازی

و جدول ۵، مقایسه‌ای برای طول کلید عمومی و طول پیام رمزشده برای این مرحله را نشان می‌دهد.

در طول فرایند انتخاب مرحله‌ی چهارم، الگوریتم نامزد SIKE نیز توسط کاستریک و دکرو با استفاده از یک کامپیوتر کلاسیک شکسته شد [۴۷] و در حال حاضر، فرایند استانداردسازی NIST در مرحله چهارم خود قرار دارد و تنها سه طرح باقی‌مانده‌اند که هر سه طرح در دسته‌ی Code-Based قرار دارند. خلاصه این مراحل استانداردسازی در شکل ۱ نشان داده شده است.

Kyber در حال حاضر تنها نماینده برای مبادله‌ی کلید پساکوانتومی است و در سومین دور مسابقات به عنوان استاندارد انتخاب شده‌است. به طورکلی، Kyber بهترین و سریع‌ترین روش برای تولید کلید، کپسوله‌سازی و کپسوله‌زدایی است. برای مقابله با خطرات احتمالی، NIST به دنبال

جدول ۴. خلاصه‌ی نتایج دور چهارم استانداردسازی NIST [۴۵]

S/No	Problem	Status	Algorithm
group exchange key and encryption Public-key			
۱	Code-based	Candidate for round 4	McEliece Classic
۲	Lattice-based	Winner becomes standard	CRYSTALS-KYBER
۳	Lattice-based	Withdrawn	NTRU
۴	Lattice-based	Withdrawn	SABER
۵	Code-based	Candidate for round 4	BIKE
۶	Lattice-based	Withdrawn	FrodoKEM
۷	Code-based	Candidate for round 4	HQC
۸	Lattice-based	Withdrawn	Prime NTRU
۹	Isogeny-based	Candidate for round 4	SIKE
group signatures Digital			
۱	Lattice-based	Winner becomes standard	CRYSTALS DILITHIUM
۲	Lattice-based	Winner becomes standard	FALCON
۳	Multivariate	Withdrawn	Rainbow
۴	Multivariate	Withdrawn	GeMSS
۵	Zero-knowledge	Withdrawn	Picnic
۶	Hash-based	Winner becomes standard	SPHINCS+

جایگزینی است که مبتنی بر lattice نباشد. با علم به این موضوع که منتخبین دور چهارم همگی در دسته کدمبنا قرار دارند، قطعا جایگزین سیستم رمز Kyber کدمبنا خواهد بود. علاوه بر این موضوع، اخیرا گروه‌های زیادی در تلاش هستند تا توسط کامپیوترهای کوانتومی و کلاسیک در زمان چند جمله‌ای به مسئله سخت LWE [1] در سیستم‌های رمزنگاری Lattice-Based حمله کنند و پیشرفت هایی نیز حاصل شده است. این مسئله روش‌های پذیرفته شده‌ی Lattice-Based را با تهدید جدی روبه‌رو می‌کند و از سوی دیگر بر اهمیت رمزنگاری کدمبنا و نمایندگان دور آخر می‌افزاید.

افزایش مداوم علاقه به رمزنگاری پساکوانتومی، به ویژه انتخاب نامزدها توسط NIST، نشان‌دهنده تمایل به استفاده از روش‌های رمزگذاری امن در برابر حملات کوانتومی است. این روند به وضوح در نموداره‌ای ارائه شده در شکل ۲ نشان داده شده، که اهمیت و تمرکز تحقیقاتی رو به رشد PQC را نشان می‌دهد.

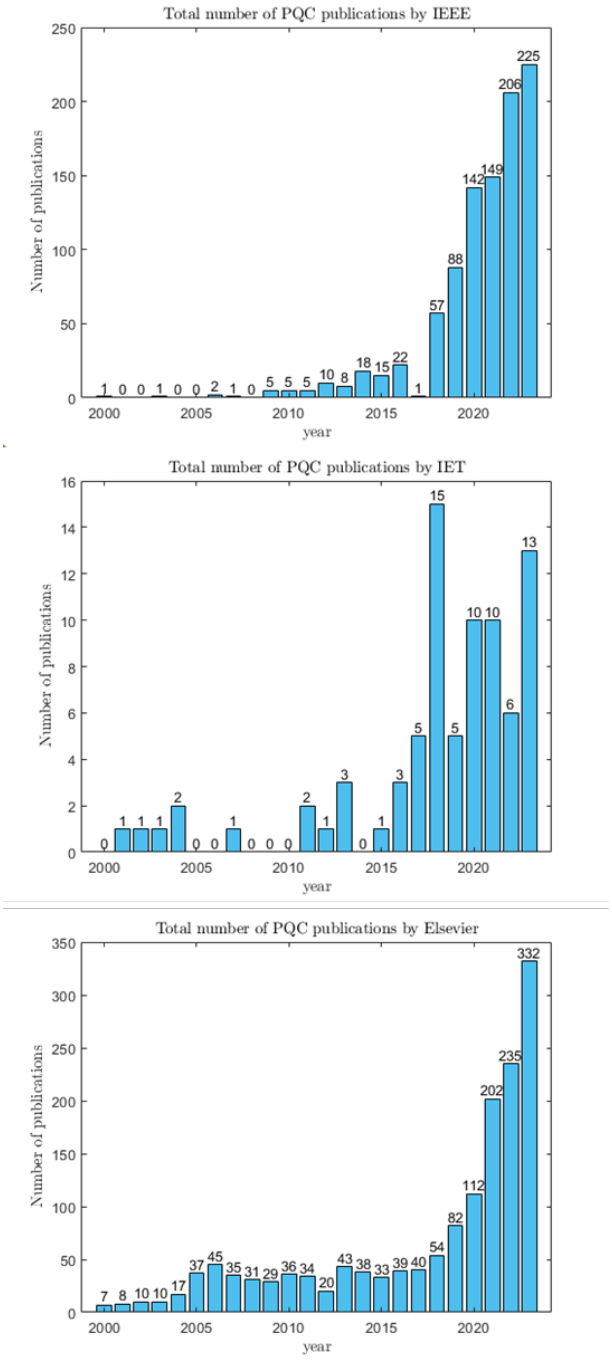
با تمامی این تلاش‌های مهم، هنوز خطر از بین نرفته است؛ زیرا میلیاردها دستگاه قدیمی و جدید وجود دارند که باید به مجموعه الگوریتم‌های PQC منتقل شوند که منجر به فرایند انتقال چند دهه‌ای می‌شود که باید آن را در نظر گرفت. در [۴۸]، استراتژی‌های پیشرو برای محافظت از سیستم‌ها در برابر حملات کوانتومی و رویکردهایی برای

[1] Learning with Errors

جدول ۵. مقایسه اندازه طول کلید عمومی و متن رمزی در ساختارهای دور نهایی NIST

نام طرح	وضعیت مسابقه	خانواده‌ی مسئله	پارامترهای تعیین شده	$\|p_k\|$	$\|c_t\|$
McEliece	finalist	code	Mceliece348864	K255	128
			Mceliece460896	K512	188
			Mceliece6688128	M1	240
			Mceliece6960119	M1	226
			Mceliece8192128	M3/1	240
KYBER	finalist	lattice	KYBER512	800	768
			KYBER768	1184	1088
			KYBER1024	1568	1568
NTRU	finalist	lattice	NTRUHPS2048509	699	699
			NTRUHPS20488677	930	930
			NTRUHPS701	1138	1138
			NTRUHPS4096821	1230	1230
SABER	finalist	lattice	LIGHTSABE	672	736
			SABER	992	1088
			FIRESABER	1312	1472
FrodoKEM	alternate	lattice	FrodoKEM640	9616	9720
			FrodoKEM976	15,632	15744
			FrodoKEM1344	21520	21632
NTRUPrime	alternate	lattice	ntrulpr6534	897	1025
			ntrulpr761	1039	1167
			ntrulpr857	1184	1312
			ntrulpr953	1349	1477
			ntrulpr1013	1455	1583
			ntrulpr1277	1847	1975
HQC	alternate	code	HQC128	2289	4481
			HQC192	4522	9026
			HQC256	7245	14469
BIKE	alternate	code	BIKE_L1	1541	1573
			BIKE_L3	3083	3115
SIKE	alternate	isogeny	SIKE_P434	346	330
			SIKE_P503	378	402
			SIKE_P610	462	486
			SIKE_P751	564	596

ترکیب رمزنگاری پیش کوانتومی با PQC برای به حداقل رساندن خطرات انتقال بحث شده است و یک دیدگاه سازمانی از انتقال PQC را ارائه می‌کند تا سازمان‌ها بتوانند به یک انتقال روان و به موقع PQC دست یابند. در ادامه به بررسی کاندیدهای کدمبنای مرحله ۴ پرداخته شده است.



شکل ۲. تعداد انتشارات علمی منتشر شده از سال ۲۰۰۰ تا ۲۰۲۳، فهرست شده به ترتیب از: (الف) IEEE Xplore، (ب) IET Digital Library، (ج) Elsevier Library.

۸ سیستم رمزنگاری HQC [۴۴]

HQC یک طرح رمزگذاری مؤثر بر اساس نظریه کدگذاری است که از کدهای چرخشی بهره برده و مخفف Hamming Quasi-Cyclic است. این طرح یکی از مکانیسم‌های کپسوله‌سازی کلید IND-CCA2 است که برای استانداردسازی در رقابت NIST در رده طرح رمزگذاری کلید عمومی پساکوانتومی اجرا می‌شود. ویژگی‌های اصلی HQC ارسالی عبارت‌اند از:

- مکانیسم‌های کپسوله‌سازی کلید IND-CCA2
- اندازه کلید عمومی کوچک
- تجزیه‌وتحلیل دقیق DFR
- پیاده‌سازی‌های عالی بر اساس الگوریتم‌های رمزگشایی کلاسیک

این سیستم در سال ۲۰۲۳ به شکل کاملا بهینه ای توسط نویسندگان در [۴۹] پیاده سازی شد

۱.۸ الگوریتم رمزگذاری و رمزگشایی در HQC

الگوریتم رمزگذاری و رمزگشایی در ساختار HQC در ۴ مرحله و به شرح زیر انجام می‌شود: (Setup، KeyGen، Encrypt، Decrypt)

- $\text{Setup}(1^\lambda)$: که در آن λ سطح امنیت کوانتومی مورد نظر است و در خروجی پارامترهای اولیه طرح را تولید می‌کند: $\text{param} = (n, k, \Delta, w, w_r, w_e)$
- $\text{KeyGen}(\text{param})$: در اینجا با استفاده از نمونه‌های $h \xrightarrow{\$} R$، ماتریس مولد $G \in \mathbb{F}_2^{k\times n}$ از C، $R_w \times R_w \xrightarrow{\$} (X, Y)$، مجموعه‌های $S_k = (X, Y)$ و $P_k = (h, s = X + h \cdot Y)$ محاسبه شده و (S_k, P_k) برگردانده می‌شود.
- $\text{Encrypt}(P_k, m)$: در اینجا $R_{w_e} \xrightarrow{\$} e$ و

$$R_{w_r} \times R_{w_r} \xrightarrow{\$} (r_1, r_2) = r$$

قرار داده شده و مجموعه‌های $u = r_1 + h \cdot r_2$ و $v = mG + s \cdot$ محاسبه شده و $C = (u, v)$ بازگردانده می‌شود.

- $\text{Decrypt}(S_k, C)$: کدگشایی $v - u \cdot Y$ و بازگرداندن پیام m.

۹ سیستم‌های رمزنگاری BIKE [۴۳]

این ساختار مجموعه‌ای از الگوریتم‌های KEM بر اساس کدهای QC-MDPC است که می‌توانند با استفاده از تکنیک‌های Bit Flipping Decoding رمزگشایی شوند. روش‌های متعددی برای کدگشایی کدهای MDPC وجود دارد؛ اما الگوریتم Bit Flipping به دلیل سادگی آن بسیار مورد توجه قرار گرفته است. نقطه قوت الگوریتم BIKE، وابستگی بر کلیدهای زودگذر و موقت است، به این معنی که در هر ارسال یک بلوک پیام، یک جفت کلید جدید ایجاد می‌شود.

الگوریتم BIKE بر اساس کد QC-MDPC است و از تبدیل CCA Fujisaki-Okamoto و رمزگشای BGF [1] برای دست‌یابی به امنیت IND-CCA استفاده می‌کند.

در مورد حمله SCA [2]، BIKE از یک راه‌حل زمان ثابت یا تعداد ثابتی از تکرارها برای بخش‌های مختلف کد استفاده می‌کند، به طوری که شخص ثالث نمی‌تواند فرایند رمزگشایی را هنگام حمله تعیین کند. سیستم رمز BIKE دارای مزایای متعددی به شرح زیر است:

[1] Black-Gray-Flip [2] Side Channel Attack

- به طور کلی کارکرد این سیستم رمز بر اساس کدهای QC-MDPC است که می‌توانند به طور مؤثر از طریق تکنیک‌های رمزگشایی با چرخش بیت رمزگشایی شوند. این نوع از رمزگشایی بسیار ساده است به این صورت که موقعیت‌هایی را که احتمال خطا دارند تخمین می‌زند، آن‌ها را برگردانده و مشاهده می‌کند که آیا نتیجه بهتر از قبل است (وزن سندرم کوچک‌تر) یا نه.
- ویژگی دیگر این ساختار رمزگذاری متکی بودن آن بر کلیدهای موقت است که همین مورد دلیلی بر قدرت آن و راه‌یابی به مرحله‌ی نهایی مسابقات NIST بوده‌است و از حملاتی که نیاز به مشاهده‌ی طول بسیار زیادی دارند جلوگیری می‌کند.
- پهنای باند اِشغالی در این ساختار در مقایسه با ساختارهای موجود بسیار کمتر است.
- BIKE امنیت خود را بر مسائل بسیار معروف نظریه کدگذاری مانند رمزگشایی سندرم شبه چرخه‌ای و مسئله‌ی یافتن کلمه کد شبه چرخه‌ای تکیه داده است. بهترین استراتژی‌ها برای حل این مسائل مبتنی بر تکنیک‌های رمزگشایی مجموعه اطلاعات (ISD) است که یک زمینه‌ای تحقیقاتی باسابقه بسیار طولانی دارد که اولین بار در [۵۰] مطرح شده است و در طول سال‌ها پیشرفت بسیار کمی حاصل شده‌است.
- یکی از نکاتی که در BIKE مورد توجه قرار می‌گیرد این واقعیت است که امروزه، تکنیک‌های رمزگشایی با چرخش بیت به نرخ شکست رمزگشایی ناچیز نمی‌رسد. این امر دستیابی به مفاهیم امنیتی بالاتر مانند IND-CCA را به چالش می‌کشد و ممکن است استفاده از BIKE را در برنامه‌های خاصی مانند رمزگذاری ترکیبی، محدود کند.

در سال ۲۰۲۳ نویسندگان [۵۱] توانستند با ترکیب حمله‌های ISD و کانال جانبی توانی به ساختار BIKE حمله کنند.

۱.۹ الگوریتم رمزگذاری و رمزگشایی در BIKE

الگوریتم رمزگذاری و رمزگشایی در ساختار BIKE در ۳ مرحله و به شرح زیر انجام می‌شود:

$$(\text{KeyGen}, \text{Encaps}, \text{Decaps})$$

KeyGen:

- ورودی: λ که سطح امنیت کوانتومی مورد نظر است.
- خروجی: کلیدهای خصوصی کم چگال (h_0, h_1) و کلیدهای عمومی چگال (f_0, f_1)
- با توجه به λ، پارامترهای r و w تنظیم می‌شوند.
- تولید $R \xrightarrow{\$} h_0, h_1$ هردو با وزن فرد $|h_0| = |h_1| = w/2$
- تولید $R \xrightarrow{\$} g$ در وزن فرد $(|g| \approx r/2)$
- محاسبه‌ی $(f_0, f_1) \rightarrow (gh_0, gh_1)$

Encaps:

- ورودی: کلیدهای عمومی چگال (f_0, f_1)
- خروجی: کلید کپسوله‌سازی شده‌ی و پیام رمزنگاری شده‌ی c
- نمونه‌برداری $(e_0, e_1) \in R^2$ به شرطی که $|e_0| + |e_1| = t$
- تولید $R \xrightarrow{\$} m$
- محاسبه‌ی $c = (c_0, c_1) \leftarrow (mf_0 + e_0, mf_1 + e_1)$
- محاسبه‌ی $K \leftarrow \mathbf{K}(e_0, e_1)$

Decpas:

- ورودی: کلیدهای خصوصی کم چگال (h_0, h_1)و پیام رمزنگاری شده‌ی c
- خروجی: کلید کپسوله‌زدایی شده‌ی یا سمبل اشتباهی $\perp$
- محاسبه‌ی سندروم $ch_0 + ch_1 \rightarrow s$
- تلاش برای کدگشایی بدون نویز s برای بازیابی بردارهای خطای $((e'_0, e'_1)$
- اگر $|(e'_0, e'_1)| \neq t$ یا کدگشایی با شکست روبرو شد خروجی $\perp$ و متوقف شود
- محاسبه‌ی $K \leftarrow \mathbf{K}(e'_0, e'_1)$

۱۰ سیستم‌های رمزنگاری[۵۲] Classic McEliece

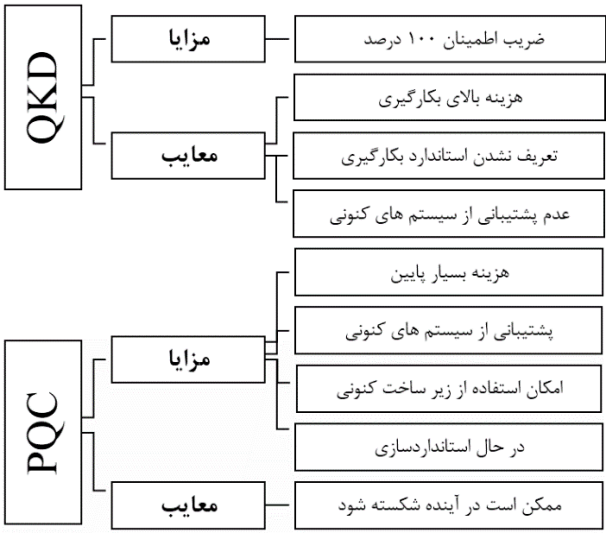
Classic McEliece یک KEM مبتنی بر کد با سطح امنیتی IND-CAA2 است. Classic McEliece برای کارایی بیشتر و امنیت بهتر با اعمال چندین پیشرفت ارتقا یافته است.

نویسندگان طرح Classic McEliece از ساختار رمز Niederreiter در طرح خود بهره برده‌اند که در بخش ۵ آن را تشریح کردیم و از کدهای Goppa در ساختار خود استفاده کردند که این ساختار برخلاف مدت زیادی که از زمان انتشارش می‌گذرد، تا به امروز توانسته است که امنیت مورد نیاز عصر کوانتوم را تضمین کند.

۱۱ امنیت در عصر کامپیوترهای کوانتومی

با روی کار آمدن پردازنده‌های کوانتومی، سیستم‌های کلیدعمومی مورد استفاده‌ی کنونی امنیت لازم را نخواهند داشت. برای مقابله با این مشکل دو راهکار ارائه می‌شود:

۱) بکارگیری سیستم‌های مبتنی بر ماهیت مکانیک کوانتوم و رمزنگاری کوانتومی که با توجه به مباحث پایه‌ای مکانیک کوانتوم، امنیت کامل را تضمین می‌کنند. تضمین امنیت در ارتباط کوانتومی به این معنی نیست که امکان شنود اطلاعات وجود ندارد بلکه به این معنا است که اگر مهاجمی به هر شکلی اطلاعات یک لینک کوانتومی را شنود کند، هر دو طرف ارتباط متوجه این موضوع خواهند شد. این سبک از ارتباط و رمزنگاری که از آن به عنوان رمزنگاری کوانتومی یاد می‌شود، با توجه به امن بودن در برابر تمامی حملات، احتمالاً در مراکز حساس نظامی، بخش‌های امنیتی و مراکز دولتی رده بالا مانند ارتباطات وزارتخانه یا ... استفاده خواهد شد. مزیت این سیستم‌ها امنیت تضمین شده‌ی آن



شکل ۳. مقایسه‌ی PQC و QKD

است که نگرانی از بابت امنیت را کاملاً از بین می‌برد ولی معایبی نیز دارد. این سبک از ارتباط برای بکارگیری به یک زیرساخت ارتباطی با سخت افزارهای جدید نیاز دارد که هزینه ساخت و راه‌اندازی بسیار بالایی خواهد داشت. عیب دیگر این ساختار، موجود نبودن تجهیزات عملیاتی در محیط واقعی و استانداردسازی مربوط به لایه‌های مختلف آن است که هنوز هیچ اقدامی در راستای آن انجام نشده است.

۲) بکارگیری تکنیک‌هایی از جنس محاسبات کلاسیک، که در برابر الگوریتم‌های کوانتومی و کلاسیکی که تا به حال شناخته شده‌اند آسیب‌پذیر نباشند. امنیت این ساختارها که از آن با عنوان رمزنگاری پساکوانتومی یاد می‌شود به مسائل کلاس NP وابسته است. پیاده سازی این ساختار بسیار ساده‌تر از حالت قبل است زیرا بر روی همین زیرساخت‌های موجود قابل پیاده‌سازی است و با توجه به این که تمامی عملیات فقط در لایه نرم افزار انجام می‌شود نیاز به هزینه‌های گزاف نخواهد بود. این سیستم‌ها به تبع در کاربردهای تجاری بکار گرفته می‌شوند و در مورد امنیت آنها نیز به طور قطع نمی‌توان صحبت کرد اما تاکنون هیچ مهاجمی نتوانسته است که آن‌ها را درهم بشکند. مقایسه‌ی بین هر دو روش گفته شده در شکل ۳ آورده شده است.

۱۰.۱۱ پژوهش‌های آینده

اساس کار در رمزنگاری کدمبنا بر ویژگی‌های کدِ مخفی شده در ساختار بکارگرفته شده‌است و بدیهی است که هرچه این کد بتواند خطای بیشتری به نسبت طول متن رمز شده تصحیح کند می‌توانیم از کدهای کوتاه‌تری که کمترین پیچیدگی را ایجاد می‌کنند استفاده کنیم. با توجه به پیشرفت‌های چشمگیری که در سال‌های اخیر در حوزه‌های یادگیری ماشین و یادگیری تقویتی شده‌است به نظر می‌رسد با به کارگیری این روش‌ها می‌توان با دستیابی به طرح‌های ارتقا یافته و استفاده از الگوریتم‌های کدبرداری کاراتر به ساختارهای با توان بیشتر و طول کوتاه‌تر رسید که توانایی به‌کارگیری در تمامی ساختارهای مختلف مانند IoT، RFID، شبکه‌های هوشمند و ... را داشته باشد.

بسیاری از حملاتی که به ساختارهای رمز کدمبنا می‌شود در دو دسته‌ی حملات ISD و حملات ساختاری قرار می‌گیرند. حملات ISD که در آن هدف دشمن کدبرداری مستقیم یک پیام از متن رمز شده‌ی متناظر با آن است، بر پایه‌ی یافتن ستون‌های بدون خطا از پیام رمز شده در ماتریس کلید عمومی مولد یا بررسی درستی استوار است (هر دو سیستم رمز کلید عمومی McEliece و Niederreiter بر به ترتیب بر مبنای ماتریس مولد و ماتریس بررسی درستی طراحی شده‌اند واثبات شده است که دارای امنیت معادل می‌باشند) و با حل دستگاه معادلات همان ستون‌ها، همواره رمزنگاری کدمبنا را تهدید کرده است. ممکن است ساختارهایی وجود داشته باشند که با این حملات تهدید نشوند و زمینه‌ی تحقیقات در آینده باشد. در حملات ساختاری نیز همواره تلاش بر این بوده است که از کلید عمومی به کلید خصوصی (ماتریس مولد کد مخفی) دست یابیم. در صورتی که بتوان از کلیدهای عمومی متغیر و زودگذر استفاده کرد، می‌توان ساختارها را به نحوی معرفی کرد که امکان حمله‌ی ساختاری میسر نباشد و این مسئله می‌تواند زمینه‌ی تحقیقاتی مناسبی باشد.

تولید خطاهای تصادفی e موجود در محاسبات ساختارهای شبه McEliece نیاز به حافظه‌ی بسیار بزرگ یا ساختاری مانند LFSR و ... دارد که داشتن این ساختارها دو مشکل اساسی دارد. ۱- ساخت و بکارگیری آن‌ها هزینه دارد. ۲- در صورت فراگیرشدن رایانه‌های کوانتومی برای بکارگیری بر روی سیستم‌هایی که اکنون در حال استفاده هستند و جایگزینی ساختارهای شبه McEliece با ساختارهای پیشین، نیاز به ایجاد یک سخت‌افزار جدید دارد که باید در کنار سخت‌افزار پیشین قرار بگیرد که انجام آن هزینه بر و بسیار وقت‌گیر است. ساختاری که استفاده می‌شود بهتر است فقط به صورت یک بروزرسانی نرم‌افزاری یا تغییری بر روی ساختار کدهای مربوطه در طراحی باشد. برای انجام این طراحی یک راه‌حل پیشنهادی وابسته کردن بردار خطای تصادفی به یک ساختار تصادفی غیرقابل دسترس برای مهاجم است. با این روش الزام در بکارگیری سخت‌افزارهای جانبی مانند LFSR از بین خواهد رفت.

۱۲ نتیجه‌گیری

با ورود پردازشگرهای کوانتومی، سیستم‌های رمز کنونی و به طور جدی سیستم‌هایی که با محدودیت منابع مواجه هستند با مشکل امنیت روبرو خواهند شد و لازم است که راهکاری برای مقابله اندیشیده شود. باتوجه به در دسترس نبودن کامپیوترهای کوانتومی با تعداد کیوبیت بالا در زمان حاضر، نباید فرصت حیاتی تحقیقات و استانداردسازی را از دست داد و در همین زمان باقی‌مانده بایستی تمامی ایرادات ساختارهای پیشنهادی را برطرف کرد و جایگزین‌هایی را نیز در نظر گرفت تا با ظهور پردازشگرهای کوانتومی غافلگیر نشویم. همچنین باید برای ارتقای سیستم‌هایی که در حال حاضر مورد استفاده قرار می‌گیرند نیز راهکارهایی در نظر گرفته شود، زیرا با روی کار آمدن کامپیوترهای کوانتومی نمی‌توان به یکباره همه

را کنار گذاشت و این تغییر وضعیت از پیش از کوانتوم به پساکوانتوم نیازمند یک فرایند چند دهه‌ای است. تنها در صورتی که تمامی این موارد در زمان مناسب و به درستی انجام شوند می‌توان مدعی شد که یک انتقال روان و مناسب صورت گرفته است و در آن صورت جامعه‌ی رمزنگاری از این چالش بزرگ سربلند بیرون خواهد آمد.

مراجع

[1] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[2] Peter Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE, 1994.

[3] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[4] Christof Zalka. Grover's quantum searching algorithm is optimal. *Physical Review A*, 60(4):2746, 1999.

[5] Elwyn Berlekamp, Robert McEliece, and Herbert Van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24:384–386, 1978.

[6] Robert McEliece. A public-key cryptosystem based on algebraic coding theory. *Jet Propulsion Laboratory Deep Space Network Progress Report*, 44:114–116, 1978.

[7] Lily Chen et al. Report on post-quantum cryptography. Technical report, US Department of Commerce, National Institute of Standards and Technology, 2016.

[8] Craig Gidney and Martin Ekera. How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, 2021.

[9] Jean-Charles Faugere, Valeria Gauthier-Umana, Anwar Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high-rate mceliece cryptosystems. *IEEE Transactions on Information Theory*, 59(10):6830–6844, 2013.

[10] Alain Couvreur, R Mora, and Jean-Pierre Tillich. A new approach based on quadratic forms to attack the mceliece cryptosystem. Technical report, Cryptology ePrint Archive, 2023.

[11] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15:159–166, 1986.

[12] Vladimir M Sidelnikov and Sergei O Shestakov. On insecurity of cryptosystems based on generalized reed-solomon codes. *Discrete Mathematics and Applications*, 2:439–444, 1992.

[13] Y X Li, R H Deng, and X M Wang. On the equivalence of mceliece's and niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, Jan 1994.

[14] Lorenz Minder and Amin Shokrollahi. Cryptanalysis of the sidelnikov cryptosystem. In *Advances in Cryptology - EUROCRYPT, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques*.

[15] Nicolas Sendrier. On the structure of a randomly permuted concatenated code. In Pierre Charpin, editor, *EUROCODE 94—Livre des résumés*, pages 169–173, 1994.

[16] Philippe Gaborit. Shorter keys for code based cryptography. In *WCC 2005, International Workshop on Coding and Cryptography*, pages 81–90, 2005.

[17] Thierry P Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Anwar Otmani. Reducing key length of the mceliece cryptosystem. In *International Conference on Cryptology in Africa*, pages 77–97. Springer, 2009.

[18] Anwar Otmani, Jean-Pierre Tillich, and Laurent Dallot. Cryptanalysis of two mceliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*, 3:129–140, 2010.

[19] Victor G Umana and Gregor Leander. Practical key recovery attacks on two mceliece variants. Technical report, Cryptology ePrint Archive, 2009.

[20] Marco Baldi, Franco Chiaraluce, Roberto Garello, and Fabrizio Mininni. Quasi-cyclic low-density parity-check codes in the mceliece cryptosystem. In *2007 IEEE International Conference on Communications*, pages 951–956. IEEE, 2007.

[21] Marco Baldi and Franco Chiaraluce. Cryptanalysis of a new instance of mceliece cryptosystem based on qc-ldpc codes. In *Proceedings IEEE ISIT 2007*, pages 2591–2595, 2007.

attack of a mceliece cryptosystem variant based on convolutional codes. Technical report, Cryptology ePrint Archive, 2013.

[33] Sudeep R Shrestha and Young-Sik Kim. New mceliece cryptosystem based on polar codes as a candidate for post-quantum cryptography. In *ISCIT 2014*, pages 368–372, 2014.

[34] R Hooshmand and M Khoshfekr. Key encapsulation mechanism based on polar codes. *IET Communications*, 16(20):2438–2447, 2022.

[35] Magali Bardet, Jerome Chaulet, Vincent Dragoi, Anwar Otmani, and Jean-Pierre Tillich. Cryptanalysis of the mceliece public key cryptosystem based on polar codes. In *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings 7*, pages 118–143. Springer, 2016.

[36] Philippe Gaborit, Anthony Hauteville, David H Phan, and Jean-Pierre Tillich. Identity-based encryption from codes with rank metric. In *Annual International Cryptology Conference*, pages 194–224. Springer, 2017.

[37] Thomas Debris-Alazard and Jean-Pierre Tillich. Two attacks on rank metric code-based schemes ranksign and an ibe scheme. In *Proc. International Conference on the Theory and Application of Cryptology and Information Security*, pages 62–92, 2018.

[38] NIST. Post-quantum crypto project. http://csrc.nist.gov/groups/ST/post-quantum-crypto/, 2016.

[39] Dustin Moody, Gorjan Alagic, Daniel C Apon, David A Cooper, Quynh H Dang, John M Kelsey, et al. Status report on the second round of the nist post-quantum cryptography standardization process, 2020.

[40] Anthony Onuora, Chisom Madubuike, Aniekan Otiko, and Joe Nworie. Post-quantum cryptographic algorithm: A systematic review of round-2 candidates. *Academia in Information Technology Profession AITP*, 2020.

[41] Felipe Borges, Pedro R Reis, and Daniel Pereira. A comparison of security and its performance for key agreements in post-quantum cryptography. In *2023 IEEE 36th International System-on-Chip Conference (SOCC)*, pages 17–28, 2023.

[42] Dan Swinhoe. The 15 biggest data breaches of the 21st century. https://www.csoonline.com/

[22] Mahdi Koochak Shooshtari, Mahdi Ahmadian-Attari, Thomas Johansson, and Mohammad Reza Aref. Cryptanalysis of mceliece cryptosystem variants based on quasi-cyclic low-density parity check codes. *IET Information Security*, 10(4):194–202, 2016.

[23] Carl Löndahl, Thomas Johansson, Mahdi Koochak Shooshtari, Mahdi Ahmadian-Attari, and Mohammad Reza Aref. Squaring attacks on mceliece public-key cryptosystems using quasi-cyclic codes of even dimension. *Designs, Codes and Cryptography*, 80:359–377, 2016.

[24] Rafael Misoczki and Paulo SLM Barreto. Compact mceliece keys from goppa codes. In *Selected Areas in Cryptography*, pages 376–392, 2009.

[25] Edoardo Persichetti. Compact mceliece keys based on quasi-dyadic srivastava codes. *Journal of Mathematical Cryptology*, 6(2):149–169, 2012.

[26] Jean-Charles Faugere, Anwar Otmani, Ludovic Perret, Fabien De Portzamparc, and Jean-Pierre Tillich. Structural cryptanalysis of mceliece schemes with compact keys. *Designs, Codes and Cryptography*, 79(1):87–112, 2016.

[27] Daniel J Bernstein, Tanja Lange, and Christiane Peters. Wild mceliece. In *International Workshop on Selected Areas in Cryptography*, pages 143–158. Springer, 2010.

[28] Alain Couvreur, Anwar Otmani, and Jean-Pierre Tillich. Polynomial time attack on wild mceliece over quadratic extensions. *IEEE Transactions on Information Theory*, 63(1):404–427, 2016.

[29] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S Barreto. Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In *2013 IEEE international symposium on information theory*, pages 2069–2073. IEEE, 2013.

[30] Qian Guo, Thomas Johansson, and Petz S Wagner. A key recovery reaction attack on qc-mdpc. *IEEE Transactions on Information Theory*, 65(3):1845–1861, 2018.

[31] Carl Löndahl and Thomas Johansson. A new version of mceliece pkc based on convolutional codes. In *Information and Communications Security: 14th International Conference, ICICS 2012, Hong Kong, China, October 29-31, 2012. Proceedings 14*, pages 461–470. Springer, 2012.

[32] Guillaume Landais and Jean-Pierre Tillich. An efficient

article/2130877/the-15-biggest-data-breaches-of-the-21st-century.html, 2021.

[43] Nicolas Aragon, Paulo Barreto, Saber Bettaieb, Luc Bidoux, Olivier Blazy, Jean-Charles Deneuville, et al. Bit flipping key encapsulation. https://bikesuite.org/files/v4.2, 2021.

[44] Carlos Aguilar A. Melchor, Nicolas Aragon, Saber Bettaieb, Luc Bidoux, Olivier Blazy, Joppe Bos, et al. Hqc. https://pqc-hqc.org.

[45] Dustin Moody. Status update on the 3rd round. https://csrc.nist.gov/Presentations/2021/status-update-on-the-3rd-round, 2021.

[46] Ben Redkins, Ivan Kuzminykh, and Bogdan Ghita. Security of public-key schemes in the quantum computing era, a literature review, 2023.

[47] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh (preliminary version). Technical report, Cryptology ePrint Archive, 2022.

[48] Douglas Joseph, Rafael Misoczki, Mauricio Manzano, Julien Tricot, Francisco De Pinuaga, Olivier Lacombe, et al. Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909):237–243, 2022.

[49] Chen Li, Shengyu Song, Jiadong Tian, Zhaofei Wang, and Çetin Kaya Koç. An efficient hardware design for fast implementation of hqc. In *2023 IEEE 36th International System-on-Chip Conference (SOCC)*, pages 1–6. IEEE, 2023.

[50] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.

[51] Anthony Cheriere, Nicolas Aragon, Timothy Richmond, and Benjamin Gérard. Bike key-recovery: Combining power consumption analysis and information-set decoding. pages 725–748, 2023.

[52] Martin R Albrecht, Daniel J Bernstein, Ting Chou, Carlos Cid, Julian Gilcher, Tanja Lange, et al. Classic mceliece: conservative code-based cryptography. 2022.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 1 (pp. 1–14)
https://monadi.isc.org.ir

A Survey Of Code-Based Cryptography Schemes and the Standardization Process of Post-Quantum Cryptography: The Beginning of a New Era

Arash Khalvan [1,*], Amirhossein Zali [1] and Mahmoud Ahmadian Attari [2]

[1] *Coding And Cryptography Laboratory, K. N. Toosi University of Technology, Tehran, Iran*
[2] *Faculty of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: January 25, 2024
Accepted: July 2, 2024
Published Online: July 10, 2024

Keywords:
code-based cryptosystem
Quantum processing
Niederreiter
Post-quantum cryptography
Public key cryptography

Type: Review paper

ABSTRACT

With the advent of computers and quantum algorithms, the security of current public key cryptography systems can face challenges. Breaking the current cryptographic structures would require multi-million qubit quantum computers, which have not yet been built; however, with significant advancements in quantum technology by leading companies in this field and the concern within the cryptography community, there has been a felt need to quickly provide countermeasures. In 2016, the National Institute of Standards and Technology (NIST) sought proposals from around the world to standardize post-quantum cryptographic schemes to address this issue. At that time, the McEliece code-based encryption system (and its equivalent Niederreiter system), despite being proven resistant to both classical and quantum algorithms, was not accepted due to its large public keys. Ultimately, the Classic McEliece, HQC, and BIKE encryption systems, which fall under code-based cryptography, advanced to the final stage of these competitions, and the winners of this cryptographic category will be announced by the end of 2024. This paper aims to review the developments made to optimize code-based structures and to examine the selected code-based cryptographic schemes and the latest status of Classic McEliece standardization.

* Corresponding author
Email addresses: a.khalvan@email.kntu.ac.ir (Arash Khalvan), a.zali1@email.kntu.ac.ir (Amirhossein Zali), mahmoud@eetd.kntu.ac.ir (Mahmoud Ahmadian Attari)