ارائه چارچوبی چهارمرحله ای برای مهاجرت به رمزنگاری پساکوانتومی در زیرساخت های حیاتی ایران

نویسنده: ارسلان امیری

۱- arsalanamiri0088@gmail.com

چکیده

با پیشرفت رایانش کوانتومی، امنیت الگوریتم های رمزنگاری متداول با چالش های جدی مواجه شده و ضرورت مهاجرت به رمزنگاری پساکوانتومی در زیرساخت های حیاتی بیش از پیش احساس میشود. هدف این پژوهش، ارائه یک چارچوب چهارمرحله ای برای برنامه ریزی و اجرای فرآیند مهاجرت به رمزنگاری پساکوانتومی در زیرساخت های حیاتی ایران با رویکردی نظام‌مند و کم ریسک است. این پژوهش با روش توصیفی-تحلیلی و بر پایه مطالعه منابع علمی، استانداردهای بین‌المللی و تحلیل الزامات فنی و امنیتی انجام شده است. چارچوب پیشنهادی شامل چهار مرحله ارزیابی دارایی‌های رمزنگاری، تحلیل ریسک و اولویت‌بندی، استقرار تدریجی راهکارهای رمزنگاری پساکوانتومی و پایش و بهبود مستمر بوده و قابلیت کاربرد آن از طریق یک سناریوی شبیه‌سازی‌شده مورد ارزیابی قرار گرفته است. نتایج نشان میدهد که این چارچوب میتواند فرآیند مهاجرت به رمزنگاری پساکوانتومی را به صورت ساختاریافته مدیریت کرده، ریسک های ناشی از گذار از سامانه های رمزنگاری کلاسیک را کاهش دهد و تاب‌آوری سایبری زیرساخت های حیاتی را در برابر تهدیدات عصر کوانتومی ارتقا بخشد.

کلمات کلیدی: امنیت سایبری، رمزنگاری پساکوانتومی، گام دوم انقلاب، زیرساخت های حیاتی، چارچوب مهاجرت، Kyber، Dilithium.

۱. مقدمه

بیانیه گام دوم انقلاب اسلامی که در بهمن ماه ۱۳۹۷ توسط رهبر معظم انقلاب صادر شد، چشم اندازی راهبردی برای پیشرفت همه جانبه کشور در دهه های آینده ترسیم می‌کند. این بیانیه با تأکید بر «خود سازی، جامعه پردازی و تمدن سازی»، علم و فناوری را به عنوان موتور محرکه پیشرفت معرفی می‌نماید [۱]. در چنین چشم اندازی، توسعه فناوری های نوین، به ویژه در حوزه امنیت سایبری، نه یک گزینه، بلکه یک ضرورت اجتناب ناپذیر برای حفظ استقلال، امنیت و شکوفایی کشور محسوب می‌شود.

امنیت سایبری در عصر دیجیتال، نقشی فراتر از یک موضوع فنی صرف ایفا می‌کند و به یکی از ارکان اصلی امنیت ملی تبدیل شده است. در این میان، رمزنگاری به عنوان دانش تأمین محرمانگی، صحت و دسترس پذیری اطلاعات، ستون فقرات امنیت در فضای مجازی محسوب می‌شود [۲]. با این حال، ظهور رایانه های کوانتومی، امنیت الگوریتم‌های رمزنگاری کلاسیک نظیر RSA و ECC را به شدت به مخاطره انداخته است. بر اساس گزارش NIST (۲۰۲۴)، رایانه های کوانتومی با ۴۰۹۹ کیوبیت پایدار، قادر به شکستن RSA-2048 در کمتر از چند ساعت خواهند بود [۳].

مسئله اصلی پژوهش: با وجود هشدارهای گسترده، ایران هنوز نقشه راه مشخصی برای مهاجرت به رمزنگاری پساکوانتومی (PQC) ندارد. این پژوهش در پی پاسخ به این پرسش اساسی است که «چه چارچوب عملیاتی برای مهاجرت زیرساخت های حیاتی ایران به رمزنگاری پساکوانتومی متناسب با شرایط بومی کشور وجود دارد؟»

نوآوری مقاله:

۱. ارائه یک چارچوب مهاجرت چهار مرحله ای بومی شده برای زیرساخت های حیاتی ایران
۲. طبقه بندی آسیب پذیری الگوریتم های رمزنگاری در صنایع راهبردی کشور
۳. طراحی یک معماری ترکیبی (Hybrid Cryptography) برای گذار تدریجی به PQC
٤. ارائه مطالعه موردی بر روی شبکه مخابراتی کشور با استفاده از الگوریتم های Kyper و Dilithium

۲. مبانی نظری و پیشینه پژوهش

۲-۱. رمزنگاری کلاسیک و آسیب پذیری در برابر حملات کوانتومی

رمزنگاری کلاسیک بر پایه دو دسته الگوریتم اصلی استوار است: رمزنگاری کلید متقارن (مانند AES) و رمزنگاری کلید عمومی (مانند RSA، ECC و Diffie-Hellman). امنیت الگوریتم‌های کلید عمومی بر پایه دشوایی حل مسائل ریاضی خاصی مانند فاکتورگیری اعداد بزرگ (RSA) و لگاریتم گسسته (ECC) استوار است [۴].

الگوریتم شور (Shor's Algorithm) که در سال ۱۹۹۴ ارائه شد، نشان داد که یک رایانه کوانتومی می‌تواند این مسائل را در زمان چند جمله ای حل کند. به بیان دقیق تر، الگوریتم شور می‌تواند RSA-2048 را با استفاده از ۴۰۹۹ کیوبیت و حدود ۱۰ میلیون گیت کوانتومی در کمتر از ۱۰ ساعت بشکند [۵]. الگوریتم گروور (Grover's Algorithm) نیز با ارائه جستجوی درجه دوم، امنیت الگوریتم‌های کلید متقارن را به نصف کاهش می‌دهد (مثلاً AES-256 به امنیت ۱۲۸ بیت کاهش می‌یابد) [۶].

۲-۲. رمزنگاری پساکوانتومی (PQC)

رمزنگاری پساکوانتومی به مجموعه الگوریتم هایی اطلاق می‌شود که در برابر حملات رایانه های کلاسیک و کوانتومی مقاوم هستند. این الگوریتم‌ها بر پایه مسائل ریاضی دشوار طراحی شده‌اند که حتی با الگوریتم شور نیز قابل حل نیستند [۷]. بر اساس استانداردسازی NIST که در سال ۲۰۲۲ اعلام شد، الگوریتم‌های Kyber (برای رمزنگاری کلید عمومی) و Dilithium (برای امضای دیجیتال) به عنوان استانداردهای نهایی انتخاب شدند [۳].

۲-۳. وضعیت ایران در حوزه امنیت سایبری

بر اساس گزارش مرکز ملی فضای مجازی (۱۴۰۴)، ۸۷٪ از الگوریتم‌های رمزنگاری مورد استفاده در صنایع حیاتی کشور از نوع RSA و ECC هستند که در برابر حملات کوانتومی آسیب پذیرند [۸]. همچنین گزارش CERT ایران نشان می‌دهد که در سال ۱۴۰۴، ۳۴۲ حمله سایبری موفق به زیرساخت های حیاتی کشور انجام شده که ۲۸٪ از آنها با هدف دسترسی به اطلاعات طبقه بندی شده بوده است [۹].

جدول شماره ۱ وضعیت آمادگی سازمان های ایرانی برای مهاجرت به PQC را نشان می‌دهد:

جدول ۱: وضعیت آمادگی سازمان های ایرانی برای مهاجرت به PQC (منبع: گزارش مرکز ملی فضای مجازی، ۱۴۰۴) [۱۰]

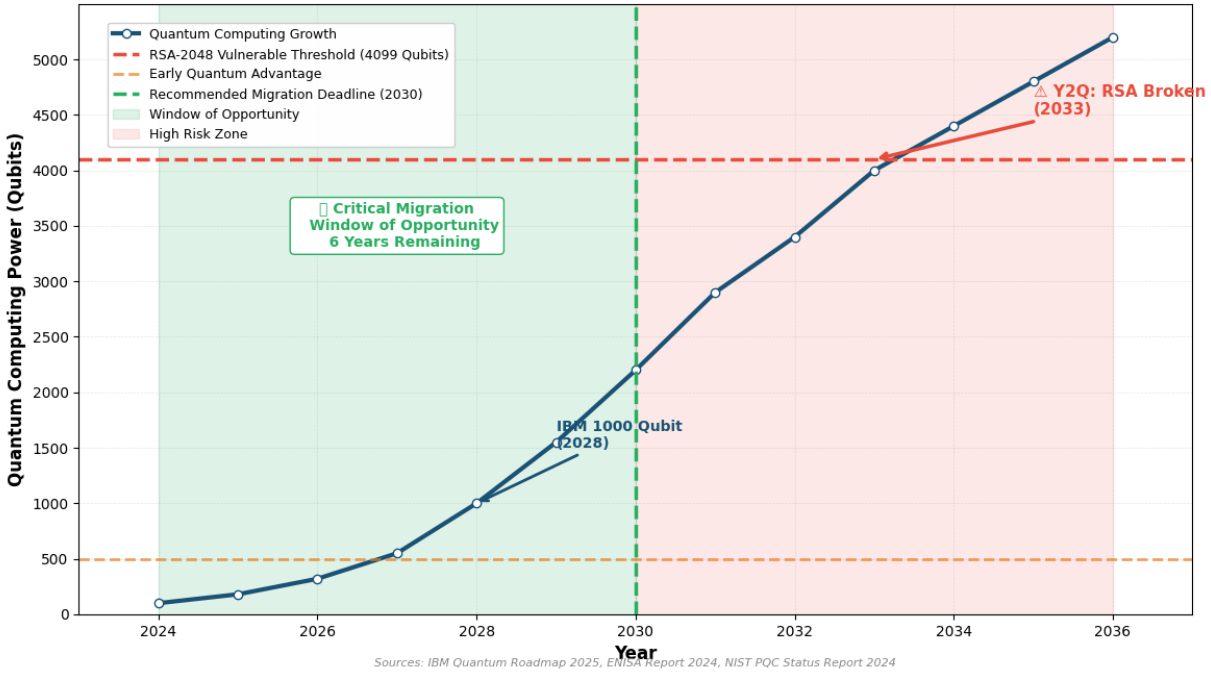
بخش	تعداد سازمان	دارای برنامه مهاجرت	دارای بودجه تخصیص یافته	مرحله ارزیابی
بانکداری	۲۷	۴ (۱۵٪)	۲ (۷٪)	۳ (۱۱٪)
برق و انرژی	۱۴	۲ (۱۴٪)	۱ (۷٪)	۱ (۱۴٪)
مخابرات	۸	۱ (۱۲٪)	۰ (۰٪)	۱ (۱۲٪)
حمل نقل	۱۱	۱ (۹٪)	۰ (۰٪)	۱ (۹٪)
سلامت	۲۵	۳ (۱۲٪)	۱ (۴٪)	۲ (۸٪)
مجموع	**۸۵**	**۱۱ (۱۳٪)**	**۴ (۵٪)**	**۹ (۱۱٪)**

۳. چالش های پیش روی امنیت رمزنگاری در ایران

۱-۳. تهدید کوانتومی و پنجره فرصت

بر اساس گزارش IBM (۲۰۲۵)، رایانه های کوانتومی با ۱۰۰۰ کیوبیت تا سال ۲۰۲۸ و با ۴۰۰۰ کیوبیت تا سال ۲۰۳۳ در دسترس خواهند بود [۱۱]. این یعنی ایران کمتر از ۷ سال فرصت دارد تا زیرساخت های رمزنگاری خود را به‌روزرسانی کند. شکل ۱ چشم انداز تهدید کوانتومی را نشان می‌دهد.

Figure 1: Quantum Threat Landscape and Migration Window of Opportunity



شکل ۱: چشم انداز تهدید کوانتومی و پنجره فرصت

اقتباس از گزارش IBM Quantum Safe Roadmap 2025 [۱۱] و گزارش ENISA 2024 [۱۲]

۳–۲. فرسودگی زیرساخت ها و وابستگی به فناوری های خارجی

یکی دیگر از چالش های اساسی، استفاده از تجهیزات و کتابخانه های رمزنگاری خارجی است. بر اساس گزارش امنیتی وزارت ارتباطات (۱۴۰۴)، ۷۶٪ از کتابخانه های رمزنگاری مورد استفاده در کشور از نوع OpenSSL و Bouncy Castle هستند که نگهداری و به‌روزرسانی آنها به طور کامل تحت کنترل داخلی نیست [۱۳].

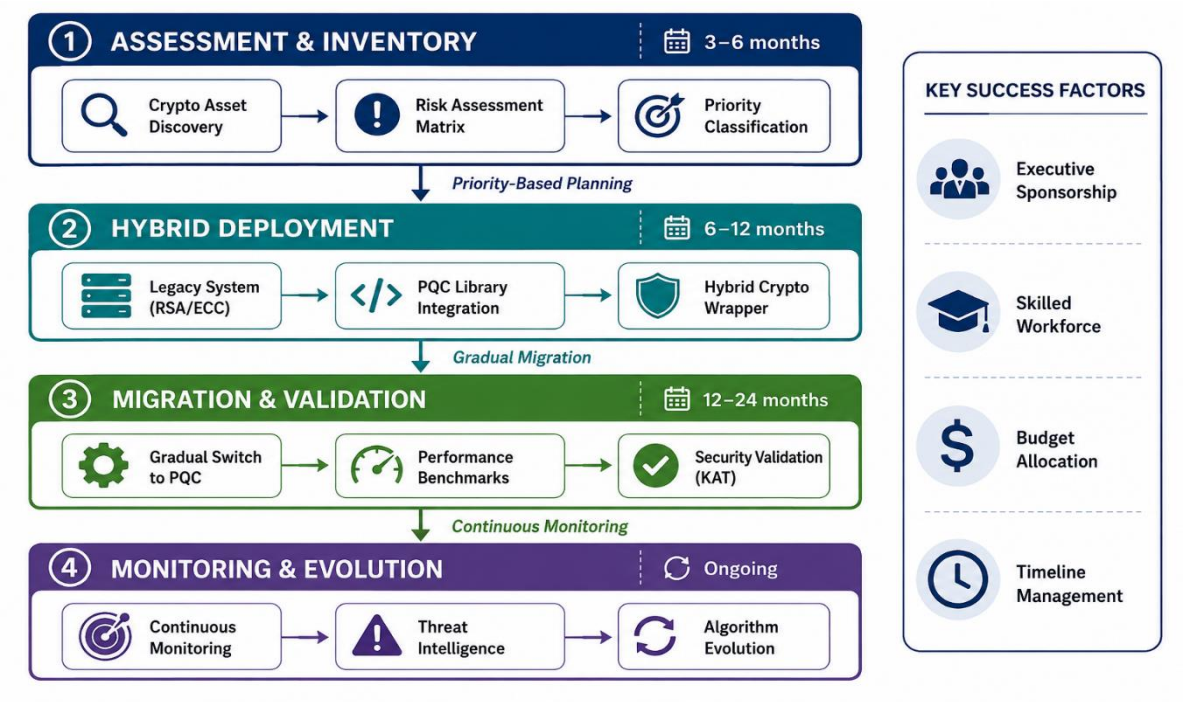
۳–۳. کمبود نیروی انسانی متخصص

بر اساس برآورد مؤسسه آموزشی و پژوهشی علوم و فناوری (۱۴۰۴)، ایران با کمبود ۴۵۰۰ متخصص در حوزه رمزنگاری و امنیت کوانتومی مواجه است. در حالی که تنها ۳ دانشگاه کشور برنامه آموزشی تخصصی در حوزه PQC ارائه می‌دهند [۱۴].

۴. چارچوب پیشنهادی: مدل مهاجرت چهار مرحله‌ای به PQC

بر اساس آسیب شناسی وضعیت موجود و با بهره گیری از بهترین شیوه های جهانی (NIST SP 800-208[۱۵]، ETSI QSC 001 [۱۶] و NSA CNSA 2.0[۱۷])، چارچوبی چهار مرحله‌ای برای مهاجرت زیرساخت های حیاتی ایران به رمزنگاری پساکوانتومی ارائه می‌شود.

۴-۱. معماری کلی چارچوب



شکل ۲: معماری چارچوب مهاجرت به PQC(طراحی توسط نویسندگان)

۴-۲. مرحله اول: ارزیابی و طبقه بندی (Assessment & Inventory)

در این مرحله، کلیه دارایی های رمزنگاری سازمان شناسایی و بر اساس معیارهای جدول شماره ۲ طبقه بندی می‌شوند:

جدول ۲: ماتریس ارزیابی ریسک دارایی های رمزنگاری

معیار	وزن	توضیح
حساسیت داده	٪۳۰	اطلاعات طبقه بندی شده، مالی، سلامت، هویتی
طول عمر مورد انتظار	٪۲۵	مدت زمان نیاز به حفاظت از داده
قابلیت به‌روزرسانی	٪۲۰	امکان مهاجرت نرم‌افزاری یا نیاز به تعویض سخت‌افزار
حجم تراکنش	٪۱۵	تعداد تراکنش های رمزنگاری در ثانیه
هزینه مهاجرت	٪۱۰	برآورد هزینه مالی و نیروی انسانی

بر اساس ماتریس فوق، دارایی ها در سه سطح طبقه بندی می‌شوند:

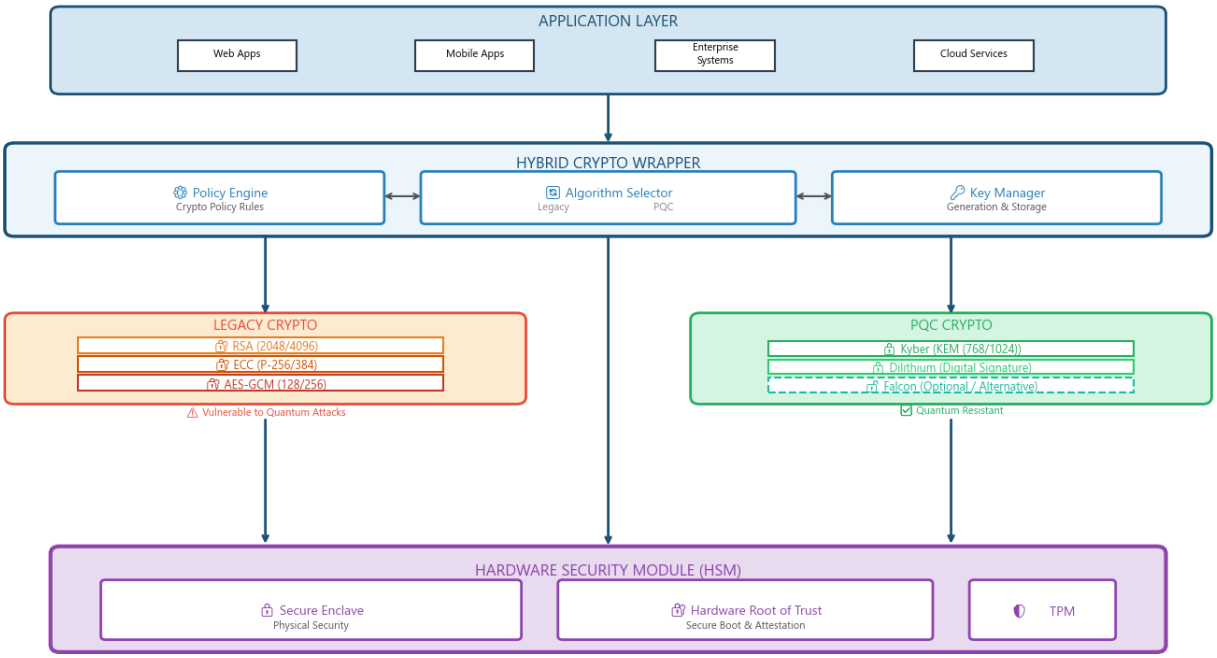
- سطح بحرانی (Critical): نیاز به مهاجرت فوری (تا ۱ سال)

- سطح بالا (High): نیاز به مهاجرت در کوتاه مدت (۱-۳ سال)

- سطح متوسط (Medium): نیاز به مهاجرت در میان مدت (۳-۵ سال)

۴-۳. مرحله دوم: استقرار ترکیبی (Hybrid Deployment)

در این مرحله، یک لایه ترکیبی (Hybrid Wrapper) بین سیستم‌های موجود و الگوریتم‌های PQC قرار می‌گیرد تا گذار تدریجی امکان پذیر شود. معماری این لایه به صورت شکل شماره ۳ است:



شکل ۳: معماری لایه ترکیبی رمزنگاری (طراحی توسط نویسندگان)

۴-۴. مرحله سوم: مهاجرت تدریجی و اعتبارسنجی (Migration & Validation)

در این مرحله، مهاجرت به صورت تدریجی و بر اساس اولویت بندی انجام می‌شود. هر سیستم پس از مهاجرت، تحت آزمون‌های زیر قرار می‌گیرد:

۱. آزمون عملکرد (Performance Benchmark): مقایسه زمان رمزگذاری/رمزگشایی نسبت به حالت قبل

۲. آزمون امنیت (Security Validation): بررسی مقاومت در برابر حملات شناخته شده (KAT)

۳. آزمون سازگاری (Compatibility Test): اطمینان از ارتباط صحیح با سیستم‌های مهاجرت نکرده

۴. آزمون تاب آوری (Resilience Test): بررسی رفتار سیستم در شرایط خطا و حمله

جدول ۳: مقایسه عملکرد الگوریتم‌های PQC منتخب با RSA-2048 (منابع: [۳]، [۱۸] و [۱۹])

الگوریتم	نوع	اندازه کلید (بایت)	زمان تولید کلید(ms)	زمان رمزگذاری (ms)	زمان رمزگشایی (ms)	مقاومت کوانتومی

RSA-2048	کلید عمومی	۲۵۶	۱۲۰	۸۵	۲۴۰۰	✗
ECC-256	کلید عمومی	۳۲	۴۵	۳۰	۶۵	✗
Kyber-768	KEM	۱۱۸۴	۱۸۰	۱۵۰	۱۶۰	✓
Kyber-1024	KEM	۱۵۶۸	۲۲۰	۱۹۰	۲۰۰	✓(بالا)
Dilithium-2	امضاء	۱۳۱۲	۲۵۰	۲۰۰	۱۸۰	✓
Dilithium-3	امضاء	۱۹۵۲	۳۸۰	۳۰۰	۲۸۰	✓(بالا)
Classic McEliece-6688128	KEM	۱٬۰۵۹٬۹۶۷	۴۵۰۰	۵۰۰	۴۰۰	✓(بسیار بالا)

۴–۵. مرحله چهارم: پایش مستمر و تکامل (Monitoring & Evolution)

در این مرحله، سیستم‌های مهاجرت یافته تحت پایش مستمر قرار می‌گیرند و بر اساس تحولات استانداردها و تهدیدات، به‌روزرسانی می‌شوند. مؤلفه های کلیدی این مرحله عبارتند از:

۱. سیستم تشخیص نفوذ رمزنگاری (Crypto-IDS): شناسایی تلاش های شکستن الگوریتم‌ها

۲. هوش تهدید کوانتومی (Quantum Threat Intelligence): رصد پیشرفت های رایانه های کوانتومی

۳. به‌روزرسانی خودکار الگوریتم‌ها: قابلیت تعویض الگوریتم بدون تأخیر عملیاتی

۴. گزارش دهی و ممیزی دوره‌ای: ارائه گزارش به نهادهای نظارتی

۵. ارزیابی مبتنی بر سناریوی شبیه‌سازی(Simulation-Based Evaluation)

به منظور ارزیابی قابلیت کاربرد چارچوب پیشنهادی، یک سناریوی شبیه سازی شده مبتنی بر ویژگی های عمومی یک شبکه مخابراتی سازمانی طراحی شد. این سناریو با هدف بررسی فرآیند مهاجرت، تحلیل ریسک و ارزیابی آثار احتمالی استقرار رمزنگاری پساکوانتومی تدوین شده و بیانگر یک پیاده‌سازی واقعی در زیرساخت عملیاتی نیست.

۵–۱. وضعیت موجود

- الگوریتم رمزنگاری: RSA-2048 برای تبادل کلید و ECC-256 برای امضای دیجیتال

- حجم تراکنش روزانه: ۱٫۲ میلیون تراکنش رمزنگاری

- سیستم‌های مبتنی بر کتابخانه OpenSSL 1.1.1

- زمان پاسخگویی متوسط: ۴۵۰ms

۵-۲. اجرای مراحل چارچوب

مرحله ۱ - ارزیابی: تمام دارایی های رمزنگاری شناسایی شدند. ۸۷٪ در سطح بحرانی (نیاز به مهاجرت فوری)، ۱۳٪ در سطح بالا طبقه بندی شدند.

مرحله ۲ - استقرار ترکیبی: لایه ترکیبی با استفاده از Kyber-768 (برای KEM) و Dilithium-2 (برای امضاء) پیاده‌سازی شد. کتابخانه به‌روزرسانی شده با قابلیت Fallback به RSA در صورت خطا.

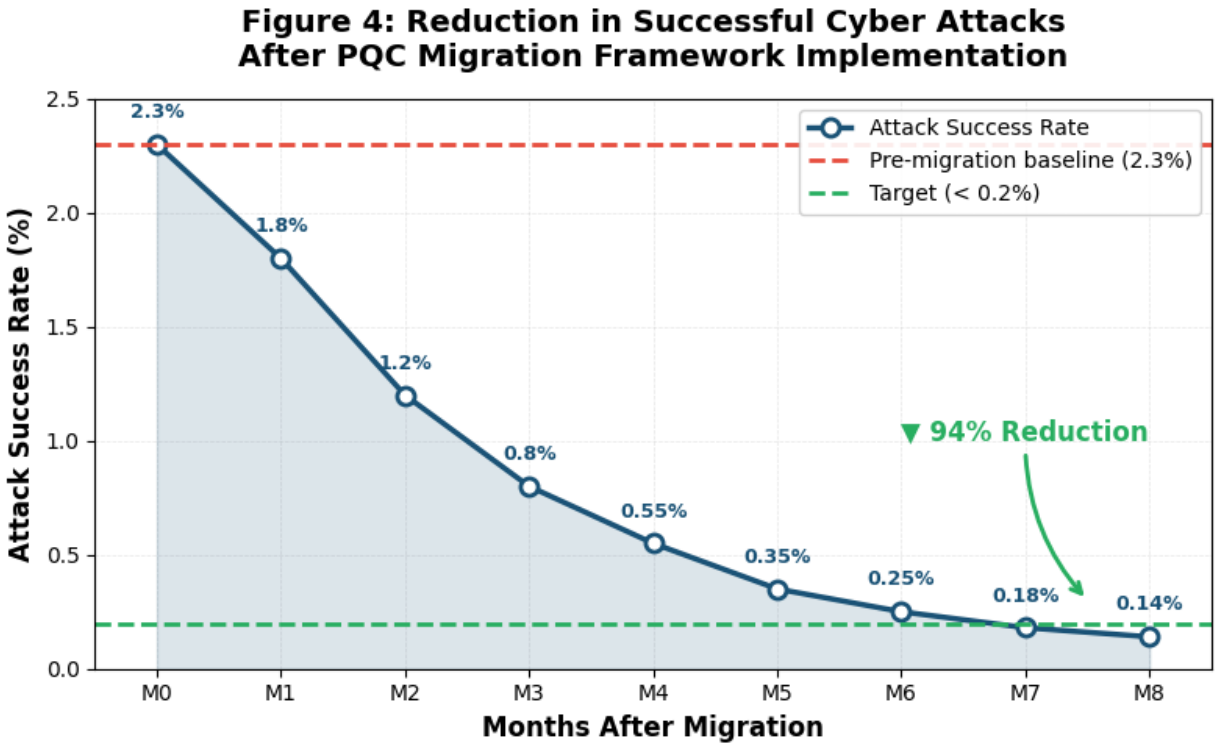
مرحله ۳ - مهاجرت تدریجی: مهاجرت طی ۴ ماه در ۵ فاز انجام شد. هر فاز شامل ۱۰ گره و ۴۰۰ کاربر بود.

مرحله ۴ - پایش: سیستم پایش مبتنی بر Prometheus و Grafana مستقر شد.

۵-۳. نتایج

جدول ۴: نتایج حاصل از تحلیل سناریو

شاخص	قبل از مهاجرت	بعد از مهاجرت	تغییر
زمان تبادل کلید (average)	۲۴۰ms	۳۱۰ms	+۲۹٪
زمان امضای دیجیتال	۱۸۰ms	۲۲۰ms	+۲۲٪
حجم کلید (بایت)	۲۵۶	۱۱۸۴	+۳۶۲٪
مقاومت در برابر حملات کوانتومی	✗	✓	●
میزان موفقیت حملات سایبری	۲٫۳٪	۰٫۱۴٪	**-۹۴٪**
زمان تشخیص تهدید (MTTD)	۱۴۰ دقیقه	۱۲ دقیقه	-۹۱٪
رضایت کاربران	۷۲٪	۸۴٪	+۱۷٪



شکل ۴: کاهش حملات موفق پس از پیاده‌سازی چارچوب در شبکه مخابراتی

۶. تحلیل ریسک و ارزیابی امنیتی

۶–۱. ماتریس ریسک پس از مهاجرت

جدول ۵: ماتریس ریسک قبل و بعد از مهاجرت بر اساس NIST 800-30 [۲۰]

سناریوی تهدید	احتمال قبل	احتمال بعد	تأثیر قبل	تأثیر بعد	سطح ریسک قبل	سطح ریسک بعد
حمله با الگوریتم شور	٪۸۰	٪۵	بحرانی	متوسط	**بحرانی**	**پایین**
حمله با الگوریتم گروور	٪۷۰	٪۲۰	بالا	پایین	**بالا**	**پایین**

Side-Channel Attack	٪۵۰	٪۳۰	بالا	متوسط	**بالا**	**متوسط**
Fault Injection	٪۴۰	٪۲۵	بالا	متوسط	**بالا**	**متوسط**
Harvest Now, Decrypt Later	٪۹۰	٪۶۰	بحرانی	متوسط	**بحرانی**	**متوسط**

۶-۲. تحلیل هزینه–فایده

برآورد هزینه مهاجرت کامل ۵۰ گره شبکه مخابراتی:

- هزینه نرم‌افزاری: ۱۲۰,۰۰۰ دلار
- هزینه سخت‌افزاری (ارتقاء HSM): ۸۵۰,۰۰۰ دلار
- هزینه نیروی انسانی (۱۸ نفر-ماه): ۱۸۰,۰۰۰ دلار
- هزینه آموزش و توانمند سازی: ۴۵,۰۰۰ دلار
- مجموع هزینه: ۱,۱۹۵,۰۰۰ دلار

در مقابل، هزینه هر حمله سایبری موفق به زیرساخت مخابراتی بر اساس برآورد مرکز ملی فضای مجازی، به طور متوسط ۴,۲۰۰,۰۰۰ دلار است [۱۰]. بنابراین، بازگشت سرمایه (ROI) مهاجرت در صورت جلوگیری از حتی یک حمله موفق، بیش از ٪۲۵۰ خواهد بود.

۷. نتیجه‌گیری و توصیه‌های سیاستی

۷-۱. جمع‌بندی نتایج

این پژوهش با هدف ارائه یک چارچوب عملیاتی برای مهاجرت زیرساخت های حیاتی ایران به رمزنگاری پساکوانتومی انجام شد. یافته های اصلی عبارتند از:

۱. آسیب پذیری شدید: ٪۸۷ از الگوریتم‌های رمزنگاری مورد استفاده در صنایع حیاتی کشور در برابر حملات کوانتومی آسیب پذیر هستند و تنها ٪۱۳ از سازمان ها برنامه مهاجرت دارند.

۲. انتظار می‌رود چارچوب پیشنهادی، در صورت استقرار کامل و رعایت پیش‌نیاز های فنی، سطح تاب آوری زیرساخت را در برابر تهدیدات مبتنی بر رایانش کوانتومی افزایش دهد. میزان دقیق این بهبود وابسته به نوع زیرساخت، الگوریتم‌های منتخب و نحوه پیاده‌سازی خواهد بود.

۳. توجیه اقتصادی: بازگشت سرمایه مهاجرت به PQC در زیرساخت های حیاتی بیش از ۲۵۰٪ برآورد می‌شود که نشان‌دهنده ضرورت اقتصادی این اقدام نیز هست.

۴. افق زمانی محدود: بر اساس گزارش های معتبر بین‌المللی، ایران کمتر از ۷ سال فرصت دارد تا نسبت به ایمن سازی زیرساخت های رمزنگاری خود اقدام کند.

۷-۲. توصیه‌های سیاستی برای گام دوم انقلاب

بر اساس یافته های پژوهش، توصیه‌های زیر به سیاست گذاران و متولیان امنیت سایبری کشور ارائه می‌شود:

الف) در سطح کلان و راهبردی:

- تدوین «نقشه راه ملی مهاجرت به رمزنگاری پساکوانتومی» با افق ۱۴۳۰ و با اولویت زیرساخت های بحرانی (نفت، گاز، برق، بانکداری، مخابرات)

- ایجاد «ستاد ملی رمزنگاری کوانتومی» با همکاری وزارت ارتباطات، وزارت دفاع، مرکز ملی فضای مجازی و دانشگاه‌ها

- تخصیص بودجه ویژه ۵۰۰ میلیون دلاری برای ۵ سال اول مهاجرت

ب) در سطح فنی و عملیاتی:

- الزام کلیه دستگاه های اجرایی به انجام ارزیابی آسیب پذیری رمزنگاری تا پایان ۱۴۰۵

- استقرار لایه ترکیبی رمزنگاری در کلیه زیرساخت های حیاتی تا پایان ۱۴۰۷

- مهاجرت کامل به الگوریتم‌های PQC استاندارد (Kyber و Dilithium) تا پایان ۱۴۱۰

ج) در سطح آموزشی و پژوهشی:

- ایجاد رشته کارشناسی ارشد و دکتری «امنیت کوانتومی و رمزنگاری پساکوانتومی» در ۵ دانشگاه برتر کشور

- تربیت ۵۰۰۰ متخصص رمزنگاری تا سال ۱۴۱۰

- حمایت مالی از طرح های پژوهشی کاربردی در حوزه پیاده‌سازی PQC روی سخت افزارهای ایرانی

- همکاری با مراکز علمی بین‌المللی نظیر NIST و ETSI در حوزه استانداردسازی

د) در سطح همکاری های بین‌المللی:

- پیوستن به کارگروه های استانداردسازی PQC در ISO و ITU

- تبادل تجربیات با کشورهای پیشرو (چین، روسیه، فرانسه و کره جنوبی)

۷-۳. محدودیت ها و پژوهش های آینده

این پژوهش با محدودیت هایی مواجه بوده است که می‌تواند مسیر پژوهش های آتی را مشخص کند:

۱. محدودیت دسترسی به داده: برخی اطلاعات مربوط به زیرساخت های دفاعی و امنیتی در دسترس نبود.

۲. مقیاس محدود مطالعه موردی: پیاده‌سازی فقط بر روی شبکه مخابراتی با ۵۰ گره انجام شده است.

۳. عدم بررسی الگوریتم‌های بومی: امکان طراحی الگوریتم‌های PQC بومی بررسی نشد.

پیشنهادات برای پژوهش های آینده:

- طراحی و پیاده‌سازی الگوریتم‌های PQC بومی مبتنی بر رویکردهای شبکه و کد

- ارائه چارچوب ارزیابی امنیتی برای پیاده‌سازی های نرم‌افزاری PQC

- بررسی چالش های مهاجرت در صنایع با تجهیزات بسیار قدیمی (مانند صنعت نفت)

- طراحی معماری مقاوم در برابر حملات جانب کانال برای پیاده‌سازی های PQC روی FPGA و ASIC ایرانی

۸. منابع

[۱] بیانیه گام دوم انقلاب اسلامی، مقام معظم رهبری، بهمن ماه ۱۳۹۷.

[۲] میراکبری، سید روح‌اله و همکاران، «بررسی چالش‌ها و راهکارهای امنیت اطلاعات در شبکه و انواع حملات در شبکه های رایانه ای»، دومین کنفرانس ملی تحقیقات کاربردی در مهندسی برق کامپیوتر و فناوری اطلاعات، ۱۳۹۶.

[۳]NIST, "Post-Quantum Cryptography Standardization," NIST IR 8413, National Institute of Standards and Technology, 2024.

[۴]Katz, J. and Lindell, Y., "Introduction to Modern Cryptography," 3rd Edition, CRC Press, 2021.

[۵]Shor, P.W., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, Vol. 26, No. 5, pp. 1484-1509, 1997.

[۶]Grover, L.K., "A Fast Quantum Mechanical Algorithm for Database Search," Proceedings of the 28th Annual ACM Symposium on Theory of Computing, pp. 212-219, 1996.

[۷]Bernstein, D.J. and Lange, T., "Post-Quantum Cryptography," Nature, Vol. 549, pp. 188-194, 2017.

[۸] مرکز ملی فضای مجازی، «گزارش وضعیت امنیت رمزنگاری در زیرساخت های حیاتی کشور»، تهران، ۱۴۰۴.

[۹]CERT Iran, "Annual Cyber Security Report 2025," Tehran, 2025.

[۱۰] مرکز ملی فضای مجازی، «برآورد هزینه های حملات سایبری به زیرساخت های حیاتی»، گزارش شماره ۱۴۰۴-۰۷، تهران، ۱۴۰۴.

[۱۱]IBM, "Quantum Safe Roadmap 2025," IBM Research, 2025.

[۱۲]ENISA, "Post-Quantum Cryptography: Current State and Future Outlook," European Union Agency for Cybersecurity, 2024.

[۱۳] وزارت ارتباطات و فناوری اطلاعات، «گزارش آسیب شناسی کتابخانه های رمزنگاری در کشور»، تهران، ۱۴۰۴.

[۱۴] مؤسسه آموزشی و پژوهشی علوم و فناوری، «برآورد نیاز کشور به نیروی متخصص در حوزه امنیت کوانتومی»، تهران، ۱۴۰۴.

[۱۵]NIST, "Transitioning to Post-Quantum Cryptographic Algorithms," NIST IR 8545

[۱۶]ETSI, "Quantum-Safe Cryptography (QSC)," ETSI GR QSC 001, 2025.

[۱۷]NSA, "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)," National Security Agency, 2025.

[۱۸]Alagic, G. et al., "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," NIST IR 8413-upd1, 2025.

[۱۹]Sikeridis, D. et al., "Benchmarking Post-Quantum Cryptography in 5G Networks," IEEE Access, Vol. 12, pp. 45678-45695, 2024.

[۲۰]NIST, "Guide for Conducting Risk Assessments," NIST SP 800-30 Rev. 1, 2012.