فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال چهارم، شماره چهار، زمستان ۱۳۹۹

طرح‌ریزی راهبردیِ رمزنگاری پساکوانتومی برای مقابله با تأثیرات رایانش کوانتومی بر روی رمزنگاری‌ها

مهران فاضلی[۱]، سید نصیب اله دوستی مطلق[۲]

تاریخ دریافت: ۱۳۹۹/۰۸/۱۷ تاریخ پذیرش: ۱۴۰۰/۰۱/۲۰

چکیده

با ظهور رایانه‌های کوانتومی و شکسته شدن رمزنگاری‌های امروزه‌ی ما و با توجه به عدم نیاز رمزنگاری‌های پساکوانتومی به زیرساخت‌های کوانتومی، امکان پیاده‌سازی آن بر روی زیرساخت‌های فعلی، و همچنین مقاومت در برابر رایانه‌های کلاسیک و کوانتومی، تنها راه باقی‌مانده برای حفاظت از ما، در عصر انتقال به کوانتوم، رمزنگاری پساکوانتومی خواهد بود. بنابراین در این پژوهش بر آن شدیم تا به مطالعه رایانه‌های کوانتومی، و رایانه و رمزنگاری‌های کلاسیک پرداخته و ضمن معرفی انواع مختلف رمزنگاری‌های پساکوانتومی، دلایل و لزوم به‌کارگیری آن‌ها بیان شده است. سپس با استفاده از روش **SWOT** و ارائه پرسشنامه و تحلیل شکاف، راهبردها و راهکارهای لازم در جهت به‌کارگیری رمزنگاری پساکوانتومی در کشور ارائه شده است.

نتایج به دست آمده نشان می‌دهند که ایران در ناحیه‌ی **WT** قرار گرفته است و راهبردهای متناسب برای مقابله با تهدیدات و پوشاندن نقاط ضعف این ناحیه به صورت خلاصه شده شامل این موارد هستند: ۱) ایجاد یک مرکز ملی برای تعیین و تصویب رمزنگاری‌های پساکوانتومی استاندارد و مورد تائید، ۲) ایجاد تمایل به همکاری در بین متخصصان و نخبگان ایرانی رمزنگاری پساکوانتومی، ۳) جذب بودجه و توجه ارگان‌های دولتی و خصوصی در زمینه اهمیت پیاده‌سازی این روش رمزنگاری، ۴) فراهم کردن زیرساخت آموزشی و تبادل اطلاعات.

واژگان کلیدی: رمزنگاری پساکوانتومی، شماهای کلید عمومی جایگزین، رایانش کوانتومی، راهبرد.

[۱] پژوهشگر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، mehranfazeli@gmail.com

[۲] استادیار، عضو هیات علمی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، نویسنده مسئول، doustimotlagh@chmail.ir

کلیات

رایانه‌های کلاسیک که امروزه جزئی جدایی‌ناپذیر از زندگی ما شده‌اند، درواقع ماشین‌های محاسباتی سریع و دقیقی هستند که مزایایی مانند راحت‌تر و سریع‌تر کردن کارها و ممکن ساختن کارهای محاسباتی و یا منطقی پیچیده را برای ما به ارمغان آورده‌اند. نکته حائز اهمیت در رابطه با رایانه‌های کلاسیک این است که با تمامی امکانات و فواید، از انجام برخی عملیات عاجز هستند. ازاین‌دست عملیات می‌توان تجزیه یک عدد صحیح بزرگ به عوامل اول آن یا محاسبه لگاریتم گسسته را نام برد. منظور از ناتوانی در حل این مسائل در رایانه‌های کلاسیک، افزایش نمایی زمان محاسبات در این عملیات است. نتیجه این ناتوانی در رایانه‌های کلاسیک، ممکن شدن رمزنگاری‌های امروزی است که امنیت آن‌ها بر پایه این مسائل غیرقابل‌حل در رایانه‌های کلاسیک بود.

ولی با پیدایش کامپیوترهای کوانتومی، امنیت سیستم‌های رمزنگاری کنونی به خطر می‌افتد، زیرا همان‌گونه که بیان شد، این سیستم‌ها بر پایه مفاهیم ریاضی ازجمله تجزیه یک عدد به عوامل اول آن طراحی شده‌اند که با سیستم‌های امروزی، از نظر محاسباتی امن محسوب می‌شوند؛ ولی با استفاده از کامپیوترهای کوانتومی می‌توان این مفاهیم را در زمان چندجمله‌ای حل کرد و درنتیجه تمامی رمزهای امروزه را می‌توان در هم شکست و عملاً بی‌فایده کرد. بنابراین با ظهور رایانه کوانتومی و با سرعت بیشتری که به ارمغان می‌آورند، تبدیل به تهدیدی جدی برای امنیت کلیه سیستم‌های رمزنگاری مانند کاربردهای نظامی، امنیتی، بانکداری مجازی، امضاهای دیجیتال، تجارت الکترونیک، گواهینامه‌های دیجیتال، رمز یک‌بارمصرف و غیره می‌شوند. درواقع با ساخت کامپیوترهای کوانتومی در مقیاس بزرگ، امنیت اکثر سیستم‌های رمزنگاری و پروتکل‌ها با تزلزل مواجه می‌شوند.

بنابراین به نوع جدیدی از رمزنگاری نیاز است تا جایگزین سیستم‌های رمزنگاری کنونی شود که امنیت آن بر پایه مفاهیمی باشد که توسط پردازش‌های کوانتومی در زمان چندجمله‌ای قابل‌حل نباشند. یکی از راه‌حل‌های ممکن، ساخت سیستم‌های رمزنگاری بر اساس فناوری کوانتوم یا همان رمزنگاری کوانتومی است. ولی محدودیت مهم، عدم وجود سیستم‌های کوانتوم هست و تا زمانی که رایانه‌های کوانتومی در دسترس نباشند، نمی‌توان از این روش استفاده کرد و درصورتی‌که تا زمانی صبر کنیم که سیستم‌های کوانتومی در دسترس باشند، برای مدت‌زمان زیادی امنیت رمزنگاری ما از بین رفته و اطلاعات حساس فردی، اجتماعی و ملی ما نشت پیدا خواهد کرد. بنابراین بی‌شک احتیاج به روش‌هایی خواهیم داشت که از رمزنگاری‌های غیر کوانتومی استفاده کنند ولی در مقابل مفروضات پردازش کوانتوم امنیت رمزنگاری ما را تأمین کنند. این روش‌ها رمزنگاری پساکوانتومی نام دارند.

انجام این پژوهش منجر به دستاوردهای زیر خواهد شد:

۱- با توجه به مشکلات بیان‌شده و شکسته شدن تمامی رمزهای مرسوم نامتقارن امروزی مانند رمزهای مبتنی بر نظریه اعداد همچون **RSA** و یا **ECC** و کاهش امنیت رمزهای نامتقارن مانند **AES** و **DES**۳، باید به دنبال روش‌های رمزنگاری نوین بود تا در زمان مناسب با رایانه‌ها و پردازش‌های کوانتومی، مقابله کنیم. راه‌حل غلبه بر این مشکل، توسعه الگوریتم‌های ایمن پساکوانتومی است، که حتی با ظهور رایانه‌ها و پردازش کوانتومی، همچنان قابل‌اطمینان باشند. بنابراین انجام این پروژه و استفاده از رمزنگاری‌های پساکوانتومی، به حفظ امنیت اطلاعات ما در سطوح مختلف فردی، اجتماعی و ملی، و کاربردهای متفاوت نظامی، امنیتی، تجاری و غیره، قبل از ظهور و بعد از ظهور رایانه‌های کوانتومی کمک خواهد کرد.

۲- انجام این پژوهش در راستای سیاست‌های کلی نظام در بخش «پدافند غیرعامل»، مبنی بر "به‌کارگیری اصول و ضوابط پدافند غیرعامل در مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به‌منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای"، راه حفظ و صیانت از شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای را به وجود خواهد آورد. همچنین استفاده از رمزنگاری‌های پساکوانتومی به‌عنوان اقدامی غیرمسلحانه، با ایجاد محرمانگی اطلاعات موجب افزایش بازدارندگی، با ایجاد محرمانگی و صحت اطلاعات باعث کاهش آسیب‌پذیری و با ایجاد

دسترس‌پذیری اطلاعات باعث تداوم فعالیت‌های ضروری، در مقابله با حملات صورت گرفته توسط دشمن به‌وسیله رایانه کوانتومی می‌گردد.

۳- در زمینه سیاست‌های کلی نظام در بخش «امنیت فضای تولید و تبادل اطلاعات»، انجام این پژوهش به‌عنوان "پایش" تهدیدات رایانش کوانتومی و "پیشگیری و دفاع" از امنیت اطلاعات کشور اهمیت ویژه‌ای خواهد داشت و به "ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای ایمن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات، و ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور" کمک شایانی خواهد کرد.

۴- این پژوهش در راستای "توسعه فن‌آوری اطلاعات (به‌ویژه حفاظت از اطلاعات) و آینده‌نگری در خصوص آثار تحولات فن‌آوری اطلاعات در سطح ملی و جهانی و گسترش مطالعات و تحقیقات "، که بخشی از سیاست‌های کلی نظام در بخش «شبکه‌های اطلاع‌رسانی رایانه‌ای» است، اقدام خواهد کرد. زیرا با آینده‌نگری درباره خطرات ناشی از تحولات رایانش کوانتومی و به جهت حفاظت از اطلاعات رمز شده به توسعه رمزنگاری‌های پساکوانتومی خواهد پرداخت.

۵- با توجه به گستردگی پیاده‌سازی رمزنگاری‌های پساکوانتومی در تمامی بخش‌ها، ارگان‌ها، سازمان‌ها، برنامه‌ها و کاربردهای کشور، اقدام در راستای راهبردهای بیان شده در این پژوهش با توجه به حجم نیروی انسانی مورد نیاز، منجر به اشتغال‌زایی و به کارگیری بسیاری از جوانان و افراد کشور عزیزمان ایران خواهد شد.

عدم توجه و اهمال در مورد این پژوهش و این زمینه نوظهور عواقب زیر را به دنبال خواهد داشت:

۱- در دنیای امروزی به‌غیراز ایجاد محرمانگی، رمزنگاری‌ها از طریق امضای دیجیتال، خدمات دیگر همچون تشخیص هویت فرستنده و عدم انکار را نیز ارائه می‌دهند. این خدمات در زمینه‌های نظامی، دولت الکترونیک، بهداشت و درمان، صنعت، تجارت و همچنین دیگر زمینه‌ها کاربرد فراوان دارد. در صورت سهل‌انگاری در زمینه رمزنگاری‌های پساکوانتومی، این خدمات نیز در زمان پساکوانتوم غیرقابل‌اعتماد و بی‌استفاده خواهند شد و با توجه به شکست رمزنگاری‌های نامتقارن مورد استفاده در امضاهای دیجیتال و فاش شدن کلیدهای خصوصی، اطمینان از منبع ارسال‌کننده پیام به‌طور کامل از بین خواهد رفت.

۲- نکته مهم و اضطراری که در اینجا باید مدنظر قرار داد، این حقیقت است که شاید از هم‌اکنون نیز امنیت ما دچار اختلال شده باشد؛ زیرا درصورتی‌که اقدامات عملی لازم در مورد استفاده از رمزنگاری‌های پساکوانتومی در سطح کشور صورت نپذیرد، متخاصمان و دشمنان می‌تواند داده‌های رمزی‌شده امروز ما را ذخیره و در آینده با پردازش کوانتومی آن‌ها را بشکنند و اطلاعاتی که گمان می‌کنیم محرمانگی آن‌ها حفظ شده است، به‌راحتی به دست دیگران بیفتد.

۳- با توجه به توانایی‌های پردازش کوانتومی، در زمینه شکستن رمزهایی که در حال استفاده از آن‌ها هستیم و همچنین استفاده‌های گسترده امنیتی و حساس که رمزنگاری در تمامی نقاط کشور به‌خصوص در تأمین امنیت فردی، اجتماعی و ملی دارد، بررسی و آماده‌سازی برای پردازش‌های کوانتومی بسیار حیاتی و حساس خواهد بود. ازآنجایی‌که این رایانه‌ها می‌توانند تمامی رمزنگاری‌های مرسوم ما را به‌یک‌باره فاقد ارزش کنند و تمامی اطلاعات ازجمله اطلاعات امنیتی کشور، اطلاعات مالی تمامی بانکداری‌ها و حتی امنیت فرد فرد ما را مخدوش سازند، باید پیش از سر رسیدن عصر رایانه‌های کوانتومی برای آن آماده بود و درصورتی‌که اقدام در مورد پژوهش‌هایی مانند پژوهش پیش رو را به تعویق بیندازیم و تا موعد ساخته‌شدن رایانه‌های کوانتومی صبر کنیم، زمان بهبود کارایی، اطمینان و بهبود استفاده از رمزنگاری‌های پساکوانتومی یا به عبارتی سال‌های بحرانی تحقیقات را از دست خواهیم داد و به‌یک‌باره باید تمامی چالش‌های آن‌ها را مورد بررسی قرار داد و رفع کرد.

۴- در صورت عدم تمکین به انجام پژوهش‌هایی ازاین‌دست در سطح کشور، ناچار به تأمین نیاز کشور در این زمینه از کشورهای بیگانه خواهیم شد و با توجه به موقعیت استراتژیک جمهوری اسلامی ایران در جهان و منطقه و عدم

وجود دانش رمزنگاری پساکوانتومی در داخل کشور، امکان خرابکاری و وجود نواقص عمدی در سیستم‌های خارجی وجود خواهد داشت، که با توجه به اهمیت غیر قابل انکار و اغماض کاربردهای رمزنگاری و همچنین وجود تجربه حملاتی چون استاکس نت به کشورمان، این موضوع خطر و تهدیدی فزاینده برای ما به وجود خواهد آورد.

۱-۱. مقدمه و هدف

رایانه کوانتومی ماشینی است که از پدیده‌ها و قوانین مکانیک کوانتوم مانند برهم‌نهی و درهم‌تنیدگی برای انجام محاسباتش استفاده می‌کند. کامپیوترهای کوانتومی با کامپیوترهای فعلی که با ترانزیستورها کار می‌کنند تفاوت اساسی دارند. ایده اصلی که در پس کامپیوترهای کوانتومی نهفته است این است که می‌توان از خواص و قوانین فیزیک کوانتوم برای ذخیره‌سازی و انجام عملیات روی داده‌ها استفاده کرد.

گرچه محاسبات کوانتومی تازه در ابتدای راه قرار دارد، اما آزمایش‌هایی انجام‌شده، که در طی آن‌ها عملیات محاسبات کوانتومی روی تعداد بسیار کمی از کیوبیت‌ها اجرا شده است. تحقیقات نظری و عملی در این زمینه ادامه دارد و بسیاری از مؤسسات دولتی و نظامی از تحقیقات در زمینه‌ی کامپیوترهای کوانتومی چه برای اهداف غیرنظامی و چه برای اهداف امنیتی (مثل تجزیه و تحلیل رمز) حمایت می‌کنند. ساخت کامپیوترهای کوانتومی در مقیاس بزرگ، می‌تواند مسائل خاصی را با سرعت خیلی زیاد حل کنند (برای مثال مسأله تجزیه یک عدد به عوامل اول توسط الگوریتم شُور).

مانند هر فناوری دیگری، محاسبات کوانتومی همراه با یک سری پیامدهای مثبت و منفی با دنیای ما عجین شده و خواهند شد. از جوانب مثبت این فناوری، این فناوری سرعت پردازش اطلاعات را به شکل محسوسی افزایش می‌دهد و به ما کمک می‌کند تا مسائل زمان‌بر و پیچیده امروزی را به ساده‌ترین شکل حل کنیم. این فناوری به‌ویژه در ارتباط با تجهیزات هوشمندی که سرعت در آن‌ها حرف اول را می‌زند کمک‌کننده خواهد بود.

در بعد امنیتی مهم‌ترین دستاورد محاسبات کوانتومی در ارتباط با رمزنگاری است. رمزنگاری ارائه‌شده از سوی این مدل از محاسبات کاملاً پیچیده و قدرتمند است، به‌طوری‌که بعضی کارشناسان عنوان کرده‌اند که عملاً شکستن آن‌ها امکان‌پذیر نخواهد بود. اما در طرف مقابل این فناوری چالش‌های امنیتی مختلفی را نیز به وجود خواهد آورد. شکسته شدن رمزنگاری‌هایی که در حال حاضر از سوی سازمان‌ها مورد استفاده قرار می‌گیرند، ابتدایی‌ترین پیامد منفی است که بسیاری از کارشناسان به آن اشاره کرده‌اند.

قدرت پردازش سیستم‌های کوانتومی، آن‌ها را قادر می‌سازد تا علاوه بر کاربردهایی مانند هوش مصنوعی و هواشناسی و غیره، توانایی در هم شکست رمزنگاری‌های معمول امروزی را داشته باشند. طبق تحقیقات انجام شده و پیش‌بینی‌های انجام شده توسط متخصصان این زمینه، محاسبات کوانتومی قادر خواهند بود تا سامانه‌های رمزنگاری کلید عمومی امروزی را در آینده نزدیک درهم بشکنند. همچنین، این مدل محاسبات به‌احتمال ۵۰ درصد تا سال ۲۰۳۱ تمام ابزارهای رمزنگاری که امروزه مورد استفاده قرار می‌گیرند و متکی به روش‌های رمزنگاری کلید عمومی هستند را بدون مصرف خواهد کرد(مانند **RSA-2048**).

بنابراین همان‌گونه که اشاره شد تنها دو راه‌حل در مقابل کارشناسان و متخصصان برای مقابله با این تهدید وجود دارد. یکی از این راه‌حل‌ها ساخت سیستم‌های رمزنگاری بر اساس تکنولوژی کوانتوم یا همان رمزنگاری کوانتومی است، که به دلیل در دسترس نبودن سیستم‌های مبتنی بر کوانتوم، فعلاً برای محافظت از داده‌ها امکان‌پذیر نیست و باید تا پایان پژوهش‌های رمزنگاری‌های کوانتومی و عملی شدن آن‌ها منتظر بمانیم و تا آن زمان در خطر از دست دادن اطلاعات در مقابل پردازش کوانتومی باشیم. همچنین به دلیل اینکه ممکن است داده‌های حساس یا طبقه‌بندی رمز شده ما، امروز توسط دشمنان ذخیره شوند و در آینده و با در دست داشتن رایانه کوانتومی مناسب توسط آن‌ها شکسته شود، باید همین‌الان اقدامات اساسی را انجام بدهیم و سال‌های بحرانی تحقیقات و بررسی کارایی و صحت رمزنگاری‌های جانشین را از دست

ندهیم. بنابراین تنها راه‌حل در دسترس، استفاده از روش‌های رمزنگاری غیر کوانتومی است که علاوه بر مقاومت در برابر حملات کلاسیک، در مقابل مفروضات پردازش کوانتوم نیز امنیت رمزنگاری ما را تأمین کنند. نام این نوع رمزنگاری‌ها، رمزنگاری پساکوانتومی است. بدیهی است که رمزنگاری‌های کوانتومی با توجه به توضیحات بیان‌شده از حوزه این پژوهش خارج هستند.

رمزنگاری پساکوانتومی به زمینه‌ای از رمزنگاری اشاره می‌کند که تلاش می‌کند اطلاعات را به‌گونه‌ای رمزگذاری و رمزگشایی کند که امنیت اطلاعات در مقابل حملات کلاسیک و کوانتومی مقاوم بماند. این رمزنگاری‌ها بدون بهره بردن از رایانه‌های کوانتومی و بر روی رایانه‌های کلاسیک قابل پیاده‌سازی هستند. به همین دلیل برای این روش‌ها، مفروضات سختی محاسبات به‌غیراز مفروضات مورد استفاده در رمزنگاری‌های امروزی نیاز است.

امنیت در مقابله با حملات کوانتومی در این سیستم‌ها بدین معناست که تاکنون هیچ‌کس نتوانسته راهی برای استفاده از یک الگوریتم کوانتومی(مانند الگوریتم شور) برای شکستن آن‌ها استفاده کند. این بدین معناست که ممکن است حملات موفق‌تری در آینده بر روی یکی از این سیستم‌ها پیدا بشود. به همین دلیل است که جامعه رمز این میزان تلاش و زمان، بر روی این سیستم‌ها می‌گذارد. [۱]

روش‌های رمزنگاری پساکوانتومی بر اساس تقسیم‌بندی مدنظر برنشتاین، به چهار دسته رمزنگاری‌های کد مبنا، رمزنگاری‌های مشبکه مبنا، رمزنگاری‌های مبتنی بر چکیده و رمزنگاری‌های چند متغیره تقسیم می‌شوند. [۱]

در بخش ۲-۲ به مقایسه ویژگی‌های رمزنگاری‌های کلاسیک، کوانتومی و پساکوانتومی پرداخته‌ایم و مزایا و معایب روش‌های رمزنگاری پساکوانتومی را بیان کرده‌ایم.

هدف اصلی پژوهش، ارائه راهبردهای لازم برای استقرار رمزنگاری‌های پساکوانتومی در تمام کشور و رفع چالش‌های کاربردی آن‌هاست.

۲-۱. روش تحقیق یا اصول و تئوری مقاله

نوع پژوهش پیشرو به دلیل بررسی رمزنگاری‌های کلاسیک، رایانش کوانتومی، نقاط ضعف روش‌های رمزنگاری کلاسیک در مقابل رایانش کوانتومی و ماهیت رمزهای پساکوانتومی، و همچنین به دلیل تلاش برای بهبود و تقویت رمزنگاری‌های مورد استفاده در نیروهای مسلح کشور و سایر نقاط استفاده‌کننده از رمزنگاری، از نوع پژوهش بنیادی و کاربردی است. همچنین پارادایمی که برای این پژوهش در نظر گرفته شده را می‌توان در دسته پارادایم انتقادی یا پسا ساختارگرایی دسته‌بندی کرد که از رویکرد تحقیق کمی و کیفی بهره خواهد برد. روش انجام این پژوهش نیز روشی کتابخانه‌ای، توصیفی و تحلیلی است.

مکان انجام این پژوهش در کشور عزیزمان ایران است و قلمرو مکانی آن شامل ایران و سایر کشورها و سازمان‌های سراسر جهان است که در زمینه رمزنگاری‌های پساکوانتومی فعالیتی داشته‌اند. قلمرو اثر این پژوهش نیز تمامی سازمان‌ها، ارگان‌ها، بخش‌ها و کاربردهای جمهوری اسلامی ایران است که از رمزنگاری و امضای دیجیتال بهره می‌برند. زمان انجام این پژوهش در بازه دی‌ماه ۱۳۹۷ تا مهرماه ۱۳۹۹ هجری شمسی است. و اگرچه در این پژوهش مواردی شامل گستره تحقیقات پیشین در زمینه فیزیک کوانتوم، رایانش کوانتومی و رمزنگاری کلاسیک، مورد بررسی قرار گرفته است ولی قلمرو زمانی این تحقیق را می‌بایست از اولین طرح پساکوانتومی پیشنهادی که متعلق به مک الیس است و در سال ۱۹۷۸ ارائه شده است، تا کنون بیان کرد. قلمرو زمانی اثر این پژوهش نیز تا افق چشم‌انداز ۱۴۰۴ خواهد بود. قلمرو موضوعی تحقیق شامل رمزنگاری‌ها و انواع آن‌ها، پردازش کوانتومی، تأثیرات پردازش کوانتومی و علوم و فناوری‌های کوانتومی بر روی رمزنگاری‌های فعلی، مقابله با تأثیرات سوء آن‌ها بر روی رمزنگاری و امنیت ملی، اجتماعی و فردی و روش‌های رمزنگاری پساکوانتومی است. همچنین مباحث علوم انسانی چون ماتریس **SWOT**، تحلیل شکاف و مدیریت راهبردی نیز بخشی از قلمرو موضوعی این پژوهش خواهند بود.

جامعه آماری مخاطب این پژوهش شامل ۳۱ نفر از خبرگان، متخصصان، پژوهشگران، اعضای هیئت علمی دانشگاه‌ها و افراد فعال در زمینه علوم کوانتومی و فناوری اطلاعات و رمزنگاری می‌شود که برای سادگی در طول

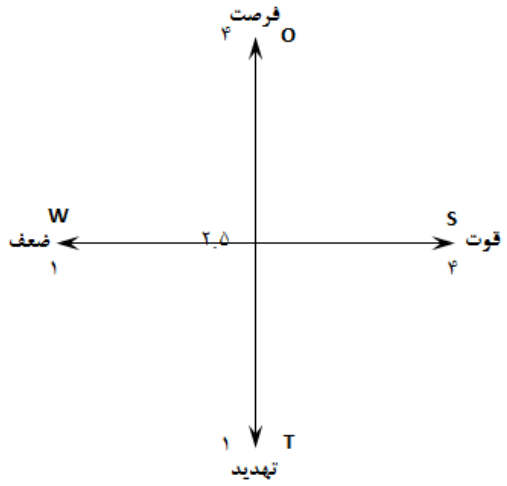
پژوهش این عزیزان، نخبگان و خبرگان خوانده می‌شوند. این نخبگان و خبرگان، صاحب‌نظرانی هستند که در حوزه‌های علوم راهبردی امنیتی و علوم کوانتوم و فناوری اطلاعات خبره هستند و ضمن شناخت ابعاد و مؤلفه‌های دینی و ملی و کار عملی در سطوح راهبردی، با جرائم و آسیب‌های اجتماعی نیز از نزدیک آشنا هستند. مدرک تحصیلی این نخبگان و خبرگان، حداقل کارشناسی ارشد است. به سبب رویکرد دفاعی و امنیتی پژوهش، محدود بودن تعداد نخبگان، خبرگان و اعضای هیئت علمی دانشگاه‌ها در حوزه‌ی مورد مطالعه و دشواری دسترسی به همه‌ی آن‌ها، این تعداد از عزیزان، حاضر به همکاری در این پژوهش شدند.

همچنین ابزار گردآوری داده‌های این پژوهش از طریق منابع کتابخانه‌ای و برگزاری جلسات هم‌اندیشی با نخبگان و خبرگان و روش دلفی(طی ۱۲ پرسشنامه) انجام شده است.

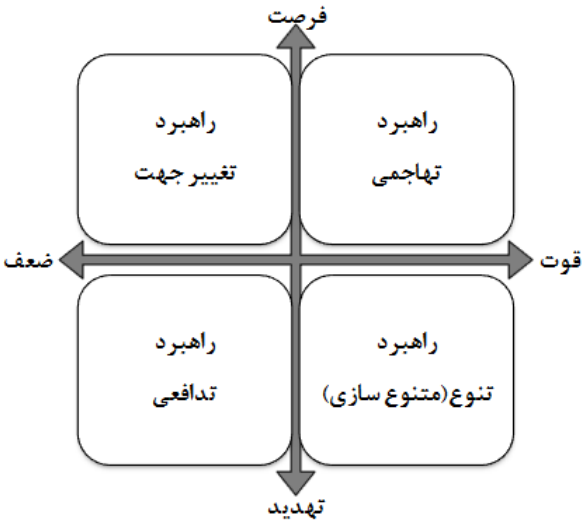
به‌منظور طراحی و پیاده‌سازی مراحل مختلف پرسشنامه‌های این تحقیق، از مقاله‌ی [۲] استفاده شده است. این الگو که چارچوب ۷۱۶ نام دارد، در راستای تدوین راهبرد از ۷ گام و ۱۶ فعالیت بهره می‌گیرد.

در گام اول، مأموریت یا هدف منحصربه‌فرد تعیین گردید. در گام بعد عوامل خارجی و پس از آن عوامل داخلی مورد بررسی قرار گرفتند. سپس امتیازات به دست آمده، جایگاه کشور بر روی محور معادلات زیر را مشخص می‌نماید.

سپس با توجه به جایگاه کشور نوع راهبردهای مناسب انتخاب می‌شود.



شکل ۱ - دستگاه مختصات SWOT



شکل ۲ - دسته‌بندی راهبرد بر اساس جایگاه بر روی دستگاه SWOT

نوع راهبردهایی که باید از آن‌ها بهره ببریم باید به گونه‌ای باشد که با استفاده از نقاط قوت خود از فرصت‌ها بهره ببرد، نقاط ضعف را بپوشاند و تهدیدها را از بین ببرد یا کمینه سازد و در نهایت این راهبردها را بر اساس ۷ معیار، مناسب بودن، عملی بودن، قابل‌پذیرش بودن، سازگاری با سیاست‌ها، تناسب داخلی روش و هدف، تناسب داخلی روش و منابع و تناسب داخلی هدف و منابع اولویت بندی می‌کنیم.

یافته‌ها

در این بخش ابتدا به بررسی رصدهای صورت گرفته در اقدامات کلیه کشورهای جهان و منطقه در زمینه استانداردسازی و به‌کارگیری رمزنگاری‌های پساکوانتومی می‌پردازیم. در ادامه به مقایسه بین سه دسته‌بندی رمزنگاری کلاسیک، کوانتومی و پساکوانتومی می‌پردازیم و درخت دانش رمزنگاری پساکوانتومی را ارائه می‌دهیم. در قسمت پایانی این فصل نیز به بیان راهبردهای مناسب برای دستیابی جمهوری اسلامی ایران به رمزنگاری پساکوانتومی می‌پردازیم.

۲-۱. فعالیت‌های جهانی در زمینه پیشرفت و پیش‌بینی آینده رمزنگاری پساکوانتومی

۲-۱-۱. رویه استانداردسازی رمزنگاری پساکوانتومی توسط موسسه ملی فناوری و استانداردها

موسسه ملی فناوری و استانداردها در حال انجام رویه‌ای برای انتخاب الگوریتم‌های رمزنگاری کلید عمومی از طریق یک رویه مسابقه مانند عمومی است. استانداردهای رمزنگاری

کلید عمومی جدید یک یا چند الگوریتم برای رمزنگاری کلید عمومی، توزیع کلید و امضای دیجیتال را مشخص می‌کنند. قصد انجام این رویه، مشخص کردن الگوریتم‌هایی است که قادر به محافظت از اطلاعات حساس دولت ایالات‌متحده در آینده قابل پیش‌بینی، شامل زمان پس از اختراع رایانه‌های کوانتومی، باشد. [۳]

پیش از آغاز رویه استانداردسازی رمزنگاری پساکوانتومی توسط موسسه ملی فناوری و استانداردها، این موسسه یک کارگاه آموزشی برای مباحثه درباره رمزنگاری پساکوانتومی و استانداردسازی‌های بالقوه آن در آینده را در آوریل ۲۰۱۵ برگزار کرد. [۳] یک سال بعد این موسسه، **NISTIR 8105** را منتشر کرد که درک **NIST** از وضعیت رایانش کوانتومی و رمزنگاری پساکوانتومی را به اشتراک می‌گذاشت و نقشه ابتدایی این موسسه برای حرکت در این زمینه را مشخص می‌کرد. این موسسه، معیارهای ارزیابی و نیازمندی‌ها را برای دریافت اظهارنظر عمومی در رابطه با آن‌ها، در قالب یک اعلامیه فدرال در سال ۲۰۱۷ پیشنهاد کرد. این نیازمندی‌ها و معیارهای ارزیابی، بر اساس بازخورد عمومی به‌روزرسانی شد و در اعلامیه دوم در همان سال منتشر شدند. این اعلامیه یک درخواست ارسال عمومی برای الگوریتم‌های رمزنگاری پساکوانتومی بود و رویه استانداردسازی رمزنگاری پساکوانتومی **NIST** را آغاز کرد. [۳]

ارسال نامزدهای استانداردسازی تا تاریخ ۳۰ نوامبر ۲۰۱۷ بود که تا این زمان موسسه ملی فناوری و استانداردها، ۸۲ بسته پیشنهادی را دریافت کرد. این یک پاسخ بزرگ از انجمن‌های رمزنگاری جهانی بود که برای رقابت انتخاب **AES** در سال ۱۹۹۸، ۲۱ الگوریتم پیشنهادی و برای رقابت **SHA-3** در سال ۲۰۰۸، ۶۴ بسته ارسال کرده بودند. از ۸۲ بسته پیشنهادی، موسسه ۶۹ مورد را که هم نیازمندی‌های ارسال و هم معیارهای پذیرش را داشت، پذیرفت. این ۶۹ مورد شامل ۲۱ شمای امضای دیجیتال و ۴۸ شمای کلید عمومی یا مکانیسم کپسوله سازی کلید می‌شد [۳].

NIST اولین اجلاس استانداردسازی خود را در سال ۲۰۱۸ برگزاری کرد. در این اجلاس ارسال‌کننده‌هایی که پیشنهاد آن‌ها برای دور اول اجلاس پذیرفته‌شده بود، دعوت شدند تا الگوریتم خود را ارائه دهند. همچنین **NIST** اعلام کرد که در نظر دارد برای متمرکز کردن توجه جامعه رمز، تعداد نامزدها را کمتر کند و دور دوم از رویه استانداردسازی را آغاز کند. [۳]

بر اساس بازخورد عمومی و بازبینی‌های داخلی که بر روی نامزدهای دور اول انجام شد، **NIST** اعلام کرد که ۲۶ الگوریتم را به‌عنوان نامزدهای دور دوم انتخاب کرده است. این الگوریتم‌ها در ۳۰ ژانویه ۲۰۱۹ معرفی شدند. [۴]

در جدول ۱ پیشنهادهای ارسالی برای **NIST** بر اساس مسأله سختی موردبررسی در آن‌ها بیان شده است. اعداد داخل پرانتز، تعداد الگوریتم‌های پذیرفته‌شده برای دور دوم را مشخص می‌کند.

جدول ۱ – دسته‌بندی پیشنهادهای ارسالی برای NIST [۴]

مجموع	KEM	امضا	مسأله سختی	PQC
28 (12)	23 (9)	5 (3)	یافتن کوتاه‌ترین بردار، نزدیک‌ترین بردار	مشبکه
20 (7)	17 (7)	3 (0)	کدگشایی کد خطی تصادفی	کد
10 (4)	2 (0)	8 (4)	حل کردن معادلات درجه دوم چندمتغیره	چندمتغیره
3 (2)	0 (0)	3 (2)	مقاومت پیش تصویر دوم تابع هش	هش
1 (1)	1 (1)	0 (0)	یافتن نگاشت ایزوژن بین خم‌های بیضوی با تعداد برابر نقاط	ایزوژن
7 (0)	5 (0)	2 (0)	-	دیگر موارد
69 (26)	48 (17)	21 (9)	-	مجموع

همچنین در جدول ۲ الگوریتم‌های راه‌یافته به دور دوم رویه استانداردسازی **NIST** آورده شده‌اند.

جدول ۲ – الگوریتم‌های راه‌یافته به دور دوم رویه استانداردسازی رمزنگاری‌های پساکوانتومی NIST [۴]

BIKE	LEDAcrypt	Rainbow
Classic McEliece	LUOV	ROLLO
CRYSTALS-DILITHIUM	MQDSS	Round5
CRYSTALS-KYBER	NewHope	RQC
FALCON	NTRU	SABER
FrodoKEM	NTRU Prime	SIKE
GeMSS	NTS-KEM	SPHINCS+
HQC	Picnic	Three Bears
LAC	qTESLA	

ارسال‌کننده‌هایی که پیشنهاد آن‌ها در دور دوم پذیرفته‌شده است، اجازه داشتند که در صورت علاقه، پیشنهادهای خود را تغییر داده و بهبود ببخشند و هر ناسازگاری، نقصان یا مشکلی را از بین ببرند. هر تغییری در یک بسته پیشنهادی باید تا تاریخ ۱۵ مارس ۲۰۱۹ برای **NIST** ارسال می‌شد. [۳]

موسسه ملی فناوری و استانداردها در نظر دارد که در سال ۲۰۲۰، یا فینالیست‌های دور نهایی را مشخص کند یا تعداد نامزدهای مناسب برای استانداردسازی را کاهش دهد [۳].

۲-۱-۲ اتحادیه اروپا

یک برنامه تحقیق و نوآوری که اتحادیه اروپا در حال پیگیری آن است **H2020** یا افق ۲۰۲۰ است. این برنامه ۷ ساله، بزرگ‌ترین برنامه نوآوری و تحقیق اتحادیه اروپا است. ازآنجایی‌که **H2020**، به‌عنوان ابزاری برای پیشبرد رشد اقتصادی و خلق موقعیت شغلی دیده می‌شود، از پشتیبانی سیاسی رهبران اروپا و اعضای پارلمان اروپا بهره می‌برد. [۵]

پروژه معماری‌های امن برای رمزنگاری‌های نوظهور آینده یا **SAFEcrypto** و پروژه رمزنگاری پساکوانتومی برای امنیت طولانی‌مدت یا **PQCRYPTO**، دو مورد از پروژه‌های برنامه **H2020** در زمینه رمزنگاری پساکوانتومی هستند که هر کدام حدوداً بودجه‌ای برابر با ۴ میلیون یورو در اختیار داشتند [۶] [۷].

هدفی که برای پروژه **SAFEcrypto** بیان شد، ارائه یک نسل جدید از راه‌حل‌های رمزنگاری پساکوانتومی عملی، قوی و امن از منظر فیزیکی است که برای سیستم‌ها، سرویس‌ها و کاربردهای **ICT** آینده، امنیت بلندمدت را تأمین کنند. این پروژه منجر به ۳۰ مقاله چاپ‌شده و پیاده‌سازی یک شما و یک کتابخانه شد. [۷] موسسات همکاری که در این پروژه شرکت داشته‌اند به همراه بودجه اعلام شده و کشور آن‌ها در جدول ۳ آورده شده‌اند.

جدول ۳- برخی از مؤسسات و شرکت‌های همکار در پروژه SAFEcrypto [۷]

نام مرکز	بودجه (یورو)	کشور
THE QUEEN'S UNIVERSITY OF BELFAST	۱۰۳۶۴۰۵	انگلیس
RUHR-UNIVERSITAET BOCHUM	۴۹۴۸۵۰	آلمان
UNIVERSITA DELLA SVIZZERA ITALIANA	-	سوئیس
INSTITUT NATIONAL DE RECHERCHE ENINFORMATIQUE ET AUTOMATIQUE	۳۴۱۹۹۷,۲۵	فرانسه
THALES UK LIMITED	۵۹۱۳۰۰	انگلیس
EMC INFORMATION SYSTEMS INTERNATIONAL	۳۹۹۱۲۵	ایرلند
H W COMMUNICATIONS LIMITED	۴۰۳۲۵۰	انگلیس
IBM RESEARCH GMBH	-	سوئیس

همچنین هدفی که برای پروژه **PQCRYPTO** عنوان شد، ایجاد توانایی انتقال به رمزنگاری پساکوانتومی برای کاربران بود، به سیستم‌هایی که نه‌تنها امروزه امن خواهند بود، بلکه در طولانی‌مدت در مقابل حملات رایانه‌های کوانتومی نیز امن خواهند ماند. خروجی این پروژه بیش از ۱۵۰ مقاله و تز چاپ‌شده و عنوان ۱۳ شمای رمزنگاری و ۹ شمای امضای دیجیتال است. [۶] موسسات همکاری که در این پروژه شرکت داشته‌اند به همراه بودجه اعلام شده و کشور آن‌ها در جدول ۴ آورده شده‌اند.

جدول ۴ – برخی از مؤسسات و شرکت‌های همکاری در پروژه PQCRYPTO [۶]

نام مرکز	بودجه (یورو)	کشور
TECHNISCHE UNIVERSITEIT EINDHOVEN	۷۰۸۹۵۸,۵۰	هلند
BUNDESDRUCKEREI GMBH	۲۱۷۸۲۲,۵۰	آلمان
DANMARKS TEKNISKE UNIVERSITET	۳۸۳۳۹۲,۵۰	دانمارک
INSTITUT NATIONAL DE RECHERCHE ENINFORMATIQUE ET AUTOMATIQUE	۴۶۳۷۵۰	فرانسه
KATHOLIEKE UNIVERSITEIT LEUVEN	۳۵۹۳۷۵	بلژیک
NXP SEMICONDUCTORS BELGIUM NV	۳۲۱۴۶۰	بلژیک
RUHR-UNIVERSITAET BOCHUM	۳۴۲۷۵۵	آلمان
STICHTING KATHOLIEKE UNIVERSITEIT	۳۵۲۴۴۵	هلند
TECHNISCHE UNIVERSITAT DARMSTADT	۳۵۸۴۴۰	آلمان
UNIVERSITY OF HAIFA	۳۴۳۳۹۲۵۰	رژیم صهیونیستی
ACADEMIA SINICA	-	تایوان

۲-۱-۳ ناتو

بر اساس سایت ناتو، برنامه دانش برای صلح و امنیت ناتو در حال حمایت از دو پروژه برای امن‌سازی ارتباطات دیجیتال در عصر پساکوانتوم است. یکی از این پروژه‌ها که در مالت پیاده‌سازی می‌شوند، توسعه و پیاده‌سازی پروتکل و روش‌های رمزنگاری پساکوانتومی است. این پروژه به دنبال یافتن یک راه‌حل امن برای ارتباطات رمزنگاری‌شده کامپیوتری است تا برای حفاظت از اطلاعات حساس استفاده شود. متخصصان دانشگاه مالت، دانشگاه اسلوواک، دانشگاه فلوریدا و دانشگاه شاه خوان کارلوس اسپانیا در حال پیشبرد این پروژه هستند [۸].

۲-۱-۴ نهاد استانداردهای مخابراتی اروپا

گروه کاری سایبری رمزنگاری مقاوم در برابر کوانتوم نهاد استانداردهای مخابراتی اروپا، با در نظر گرفتن وضعیت فعلی تحقیقات رمزنگاری دانشگاهی و تحقیقات در زمینه الگوریتم‌های کوانتومی و همچنین نیازمندی‌های صنعتی برای پیاده‌سازی‌های عملی، سعی در ارزیابی و انجام توصیه برای پیاده‌سازی الگوریتم‌های رمزنگاری مقدماتی که در برابر کوانتوم مقاوم هستند دارد. بر اساس اعلام نهاد استانداردهای مخابراتی اروپا، تمرکز آن‌ها بر روی پیاده‌سازی عملی از مقدمات رمزنگاری مقاوم در برابر کوانتوم، شامل ملاحظات کارایی، توانایی‌های پیاده‌سازی، پروتکل‌ها، محک زدن و ملاحظات معماری‌های عملی برای کاربردهای خاص است. همچنین بیان داشتند که هدف آن‌ها شامل توسعه مقدمات رمزنگاری نخواهد شد. [۹]

این گروه بیان می‌کند که ویژگی‌های امنیتی الگوریتم‌ها و پروتکل‌های پیشنهادی را در کنار ملاحظات عملی، همچون هزینه‌های جایگزینی فناوری و معماری امنیتی بسط پذیر که اجازه می‌دهد این توصیه‌ها در موارد کاربرد متنوع صنعتی کاربرد داشته باشند، بررسی می‌کند. طبق بیان آن‌ها، این گروه با مقایسه عملی و ارائه توصیه‌های منسجم، در زمینه انتخاب و به‌کارگیری بهترین الگوریتم‌های مقاوم در برابر کوانتوم در دسترس، به انجمن‌های فناوری جهانی یاری خواهد رساند. [۹]

۲-۱-۵ انجمن رمزنگاری چینی

انجمن رمزنگاری چینی نیز در حال برگزاری رقابت طراحی هستند که منجر به انتخاب الگوریتم‌های رمزنگاری کلید عمومی و خصوصی شود. آن‌ها به‌تازگی ۲۲ الگوریتم کلید خصوصی و ۳۸ الگوریتم کلید عمومی را در سایت "اتحادیه چینی برای تحقیقات رمزنگاری" (**CACR**) منتشر کردند. هدف نهایی بیان شده برای انجمن، اتمام انتخاب نهایی تا انتهای سال ۲۰۱۹ است. تمامی وب سراچه‌های مرتبط به این تلاش انجمن رمزنگاری برای طراحی کلید عمومی و خصوصی به زبان چینی هستند [۱۰].

۲-۱-۶ کشورهای شورای همکاری خلیج‌فارس

بر اساس یک گزارش که در سایت **wamda** منتشر شد، کشورهای شورای همکاری خلیج‌فارس در حال همکاری با شرکت‌های پیشرو در زمینه فناوری‌های کوانتومی هستند. شرکت‌های به نامی چون **IBM**، گوگل، مایکروسافت و **D-Wave** نمونه‌ای از این شرکت‌ها هستند که با کشورهای عضو این شورا در حال همکاری هستند. از پروژه‌هایی که توسط شرکت‌های بین‌المللی در این کشورها در حال انجام است، انجام تحقیقات بر روی رمزنگاری‌های کوانتومی و پساکوانتومی برای داشتن برتری و دست بالاتر در منطقه است [۱۱].

۲-۱-۷ شماری دیگر از سازمان‌های ایالات متحده آمریکا

طبق اعلام آژانس امنیت ملی ایالات‌متحده آمریکا، این آژانس در زمینه رمزنگاری پساکوانتومی به صورت کامل به رویه استانداردسازی موسسه ملی فناوری و استانداردها متکی خواهد بود و آن را به عنوان روش منتخب برخواهد گزید. اگرچه این آژانس امنیتی اعلام کرد که خود تمامی تحلیل‌های امنیتی و مشخصه‌های کارایی پیشنهادهای رویه استانداردسازی موسسه ملی فناوری و استانداردها را بررسی کرده و به شماهای مشبکه مبنا که بر اساس مسائل ریاضی مطالعه شده هستند اطمینان دارند و همچنین امضاهای مبتنی بر چکیده را برای راه‌حل‌های خاصی مناسب می‌دانند. [۱۲]

همچنین بنا بر اعلام این آژانس، آن‌ها نیازی مبنی بر تائید روش‌های دیگر رمزنگاری پساکوانتومی برای سیستم‌های امنیت ملی نمی‌بینند ولی در نظر خواهند داشت که شرایط ممکن است با گذر زمان تغیر کند. آن‌ها بر این باورند که عوامل متنوعی چون اطمینان به امنیت و کارایی، عملیاتی بودن، مهندسی سیستم، بودجه، تدارکات و دیگر عوامل ممکن است بر روی این تصمیم‌گیری تأثیر بگذارند. [۱۲]

سازمان‌های دیگری چون کارگروه مهندسی اینترنت یا همان **IETF**، که یک سازمان استانداردسازی ناسودبر است و معمولاً مدیران آن توسط حامیانی مانند آژانس امنیت ملی تعیین می‌شوند نیز هدف خود را در زمینه رمزنگاری پساکوانتومی بیان کرده است. براین اساس این سازمان نیز اگرچه منتظر خروجی رویه استانداردسازی موسسه ملی فناوری و استانداردهای ایالات‌متحده آمریکا خواهد ماند، ولی خود نیز دست از تلاش برای یافتن و پیاده‌سازی رمزنگاری‌های پساکوانتومی مناسب برای جانشینی رمزنگاری‌های فعلی برنخواهند داشت. [۱۳]

۲-۱-۸ بررسی اسناد راهبردی چین و آمریکا در زمینه فناوری‌های کوانتوم

طبق مسیر راه استراتژیک اعلام‌شده در سال ۲۰۰۷، **DARPA** اعلام کرد علوم کوانتوم را در هسته نیروهای پیشرانه استراتژیک خود قرار داده است. [۱۴] همچنین در سال ۲۰۱۵، **DARPA** «تلاش‌ها برای تحت کنترل درآوردن قدرت فیزیک کوانتوم» را در بین «فناوری‌های پیشرفته اولویت‌دار برای امنیت ملی» دسته‌بندی کرده است. [۱۵]

ولی بر اساس گزارشی که در سال ۲۰۱۶ توسط یک گروه دولتی بین سازمانی در آمریکا منتشر شد، ظاهراً پیشرفت‌های علوم اطلاعاتی کوانتوم در آمریکا توسط مسائلی مانند بودجه، محدودیت‌های کیفری و سازمانی سخت‌گیرانه، نیروی کاری و ارتباط با صنعت کمی دچار شده است. [۱۶]

چین برخلاف آمریکا، علوم اطلاعاتی کوانتوم را به‌عنوان یکی از بخش‌های مرکزی استراتژی امنیت ملی قرار داده است. [۱۷] علی‌الخصوص بعد از نشت اطلاعاتی که توسط ادوارد اسنودن صورت پذیرفت، دولت چین به‌صورت جدی‌تر به اهمیت و بهره‌بری از فناوری‌های کوانتوم توجه کرد. افشاگری‌های اسنودن گسترش توانایی‌های اطلاعاتی آمریکا را نشان داد که باعث شد نگرانی‌های رهبران چین در رابطه با امنیت اطلاعات محلی چین و مورد ظن بودن آن‌ها در مقابله با جاسوسی و همچنین تأثیرات سایبر، افزایش یابد.

در همین راستا شی جین پینگ نیز به اهمیت استراتژیک فناوری‌های کوانتوم در امنیت ملی و به‌صورت بخصوص در امنیت سایبر، تأکید کرده است. [۱۷]

در نوامبر ۲۰۱۵ و در ۱۸مین کنگره حزبی، شی جین پینگ، ارتباطات کوانتومی را در لیست پروژه‌های علوم و فناوری‌های مهم قرار داد، که برای پیشرفت‌های بزرگ تا سال ۲۰۳۰ در اولویت قرار دارند و اهمیت آن‌ها برای ضرورت‌های استراتژیک بلندمدت را اعلام کرد.

در ۱۳مین برنامه ۵ ساله ملی چین، علوم اطلاعاتی کوانتومی ترویج و بیان شده است. این برنامه علاوه بر لزوم ترویج و استفاده از فناوری‌های کوانتومی، شامل تمرکز بر روی فناوری‌های کوانتومی می‌شود، که چین را به سطح حاکمیت توسعه علمی بین‌المللی در این زمینه می‌رساند.

همچنین ارتش جمهوری خلق چین، به اهمیت استراتژیک شبکه‌های ارتباطات کوانتومی اشاره می‌کند. ارتش جمهوری خلق چین نه‌تنها به دنبال استفاده روزافزون از شبکه‌های ارتباطی کوانتومی پیچیده، برای ایجاد اطمینان از صحت ارتباطات حساس در زمان صلح است؛ بلکه به دنبال برتری اطلاعاتی نامتقارن در زمان جنگ نیز هست. [۱۷]

۲-۲. مقایسه بین رمزنگاری کلاسیک، کوانتومی و پساکوانتومی و مزایای رمزنگاری پساکوانتومی

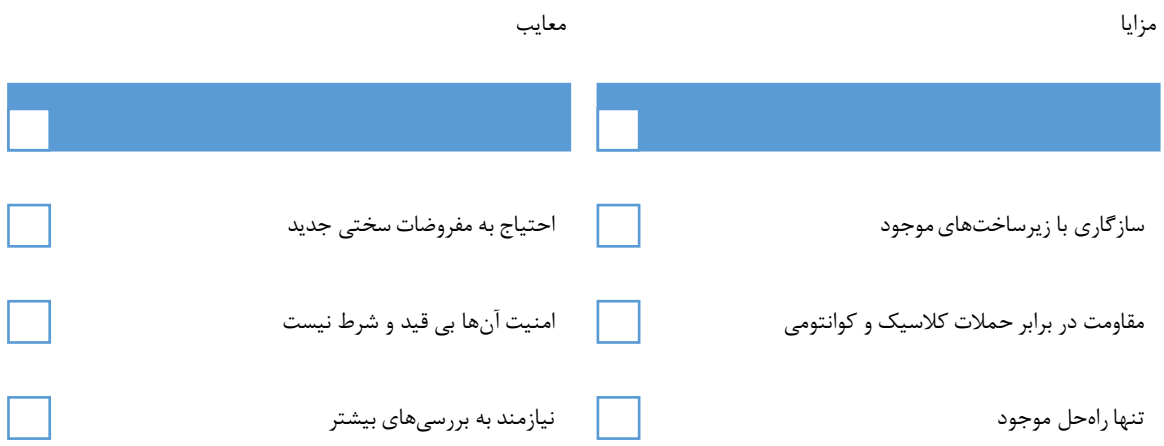
در طی تحقیقات انجام شده و برای بررسی برتری و ضعف رمزنگاری‌های مختلف و احتمالی نسبت به یکدیگر، به بررسی و مقایسه اصول رمزنگاری‌های کلاسیک، کوانتومی و پساکوانتومی با یکدیگر کردیم(شکل ۳). این مقایسه می‌تواند پایه‌ای در زمینه علت به‌کارگیری هر یک و دلایل سوق به هرکدام از رمزنگاری‌ها باشد و در روند تصمیم‌گیری کمک شایانی بکند.

همان‌گونه که پیش‌تر نیز بیان کردیم، رمزنگاری‌های پساکوانتومی نیز مانند روش‌های کلاسیک مبتنی بر پیچیدگی محاسبات هستند، ولی مبتنی بر انواع دیگری از پیچیدگی‌های محاسباتی هستند که پردازش کوانتومی توانایی حل این دسته از مسائل در زمان چندجمله‌ای را دارا نیست، بنابراین به مفروضات سختی جدیدی نیازمند است. روش‌های رمزنگاری کلاسیک مبتنی بر پیچیدگی‌هایی مانند محاسبه لگاریتم گسسته یا فاکتورگیری از اعداد صحیح بزرگ هستند که این دست از مسائل توسط پردازش کوانتومی و با بهره از روش‌هایی چون الگوریتم شور حل خواهند شد. ولی رمزنگاری‌های کوانتومی از آنجایی که مبتنی بر قوانین مکانیک کوانتوم هستند، امنیت آن‌ها در مقابل پردازش کوانتوم اثبات‌پذیر بوده ولی برخلاف دو روش دیگر برای پیاده‌سازی نیاز به سخت‌افزارهای کوانتومی دارند و نمی‌توان آن‌ها را بر روی سخت‌افزارهای در دسترس پیاده‌سازی کرد.

بنابراین رمزنگاری‌های پساکوانتومی، دارای مزایا و معایب شکل ۴ هستند، که با توجه به شرایط فعلی، امکانات و تجهیزات موجود و خطرهای بالقوه، حرکت به سوی رمزنگاری پساکوانتومی اجتناب‌ناپذیر به نظر می‌رسد.

بعد قیاس	کلاسیک	پساکوانتومی	کوانتومی
روش امن سازی	مبتنی بر پیچیدگی محاسبات	مبتنی برپیچیدگی محاسبات	مبتنی بر قوانین پذیرفته شده مکانیک کوانتومی
امنیت در مقابله با رایانه‌های کوانتومی	ندارد	حدس زده می‌شود که دارد	دارد
نیاز به سخت افزار کوانتومی	ندارد	ندارد	دارد
تشخیص شنود	ندارد	ندارد	دارد
سیستم پیاده‌سازی	نرم افزار	نرم افزار	سخت افزار

شکل ۳ – مقایسه انواع رمزنگاری‌ها



شکل ۴ – مزایا و معایب رمزنگاری پساکوانتومی

۲-۳. راهبردهای مناسب برای دستیابی جمهوری اسلامی ایران به رمزنگاری پساکوانتومی

برای تجزیه و تحلیل محیط و درون کشور، به عوامل تأثیرگذار احتمالی در دستیابی کشور به رمزنگاری پساکوانتومی نیاز است. برای این منظور عوامل زیر در پی مطالعات تخصصی منابع معتبر و همچنین انجام جلسات هم‌اندیشی و پرسش و پاسخ با نخبگان و خبرگان، به دست آمدند.

۱- عدم‌حمایت مالی از نخبگان
۲- عدم آشنایی متخصصان با اسناد بالادستی
۳- سرمایه‌گذاری کم در مقایسه با کشورهای پیشرو
۴- عدم وجود استانداردهای لازم برای به‌کارگیری رمزنگاری‌های پساکوانتومی در کشور
۵- عدم تمایل نخبگان به همکاری با واحدهای نظامی
۶- وجود سلسله‌مراتب دست‌وپاگیر در مراحل اداری
۷- مهاجرت رو به رشد نخبگان و متخصصین
۸- شناخت بازارهای داخلی و بین‌المللی رمزنگاری پساکوانتومی
۹- عدم دسترسی کامل به اطلاعات آخرین پیشرفت‌ها در زمینه رمزنگاری پساکوانتومی
۱۰- عدم اطلاع مدیران سازمان‌ها از اهمیت رمزنگاری پساکوانتومی

۱۱- عدم اعتماد به نخبگان در جهت دسترسی به اطلاعات حساس و محرمانه کشور
۱۲- افزایش تعداد متخصصین حوزه رمزنگاری پساکوانتومی
۱۳- عدم وجود توان رقابتی محصولات داخلی با نمونه‌های خارجی
۱۴- توجه به مسیر حرکت جهانی در زمینه رمزنگاری
۱۵- توجه به دانش‌های روز در اسناد بالادستی
۱۶- متغیر بودن زمان مورد نیاز جهت پیاده‌سازی انواع رمزنگاری پساکوانتومی
۱۷- تبادل علمی و فنی با دیگر کشورها
۱۸- داشتن تجربه‌های قبلی رویارویی با حملات سایبری مانند استاکس نت
۱۹- افزایش امنیت و اقتدار ملی
۲۰- افزایش قدرت پدافندی کشور
۲۱- آگاه نبودن کشور از اهمیت رمزنگاری پساکوانتومی
۲۲- عدم برگزاری همایش‌های مرتبط با رمزنگاری پساکوانتومی
۲۳- ایجاد فرصت‌های شغلی جدید برای متخصصان رمزنگاری یا علوم کوانتومی
۲۴- ربایش اطلاعات در زمان فعلی برای رمزگشایی در آینده با استفاده از رایانه کوانتومی مناسب
۲۵- تحریم‌های موجود علیه ایران
۲۶- ایجاد ناامیدی در جوانان
۲۷- بازار غیرنظامی قوی برای محصولات رمزنگاری پساکوانتومی
۲۸- هماهنگی بین دانشگاه‌های نظامی کشور
۲۹- تبلیغ سوء علیه متخصصین داخلی
۳۰- هزینه پایین به‌کارگیری رمزنگاری پساکوانتومی نسبت به راه‌حل‌های جایگزین مانند رمزنگاری کوانتومی
۳۱- عدم جذب متخصصین حاضر در خارج از کشور
۳۲- نبود سامانه یکپارچه ملی برای بیان پیشرفت‌های حاصله
۳۳- نگرش منفی نسبت به آینده در بین جوانان
۳۴- ایجاد دید منفی نسبت به سطح سواد متخصصان داخلی
۳۵- عدم وابستگی سیاسی متخصصین
۳۶- شکسته شدن رمزنگاری‌های کلاسیک به دست رایانه کوانتومی
۳۷- وجود زمان تا ساخت رایانه کوانتومی در مقیاس مناسب
۳۸- وجود فاصله بین خروجی دانشگاه‌ها با صنعت
۳۹- لزوم حفظ امنیت داده‌های رمز شده کشور برای مدت‌زمان زیاد
۴۰- بزرگنمایی شکست رمزنگاری کلاسیک توسط شرکت‌های فعال در رمزنگاری پساکوانتومی
۴۱- کاربردهای متنوع نظامی، امنیتی و تجاری رمزنگاری پساکوانتومی
۴۲- عدم اطمینان به خروجی اعلام شده توسط فراخوان‌های دولتی دیگر کشورها مانند **NIST**
۴۳- تعطیلی‌های مقطعی در سطح کشور و جهان به دلیل بیماری کووید ۱۹
۴۴- همکاری کشورهای منطقه با شرکت‌های پیشرو در زمینه کوانتوم و رمزنگاری پساکوانتومی
۴۵- نبود استارت‌آپ یا شرکت دانش‌بنیان در زمینه رمزنگاری پساکوانتومی
۴۶- عدم وجود خروجی‌های مرتبط با رمزنگاری پساکوانتومی از دانشگاه‌ها

سپس برای بررسی مربوط بودن و تأثیرگذار بودن موارد فوق نظرات نخبگان در رابطه با تأثیرگذار بودن این عوامل از طریق پرسشنامه اول پرسیده شد. عواملی که بیش از نیمی از نخبگان و خبرگان آن را مؤثر نمی‌دانستند، در این مرحله باید حذف می‌شد ولی تمامی عوامل توسط نخبگان مؤثر دانسته شد و در نتیجه هیچ‌کدام از عوامل در این مرحله حذف نگردیدند.

سپس از طریق سؤال دوم نظر نخبگان در رابطه با کنترل یا عدم کنترل کشور بر روی هریک از این عوامل پرسیده شد، که تعداد ۲۹ عامل از نظر نخبگان به‌عنوان عامل داخلی شناخته شد و تعداد ۱۷ عامل نیز از نظر آن‌ها به‌عنوان عامل خارجی تشخیص داده شد. در ادامه این بخش به بررسی و تجزیه و تحلیل این ۱۷ عامل خارجی می‌پردازیم و در سپس عوامل داخلی را مورد بررسی قرار می‌دهیم.

دو مورد از عوامل خارجی بیان شده، از منظر نخبگان تأثیر کمتر از ۳، بر روی دستیابی به رمزنگاری پساکوانتومی دارند. به همین دلیل این موارد از ادامه مسیر تحلیل بازخواهند ماند. این عامل‌ها در زیر آورده شده‌اند. در پرانتز امتیاز تأثیر به دست آمده برای هرکدام نوشته شده است.

۳۵- عدم وابستگی سیاسی متخصصین (۲,۷۷)
۴۰- بزرگنمایی شکست رمزنگاری کلاسیک توسط شرکت‌های فعال در رمزنگاری پساکوانتومی (۲,۹۷)

با توجه به امتیازات به دست آمده برای عوامل داخلی، میزان موافقت نخبگان با سه مورد از عوامل بیان شده کمتر از ۳ است. به همین دلیل این موارد از ادامه مسیر تحلیل بازخواهند ماند. این عامل‌ها در زیر آورده شده‌اند. در پرانتز امتیاز تأثیر به دست آمده برای هر کدام نوشته شده است.

۲۶- ایجاد ناامیدی در جوانان (۲,۷۴)

۳۰- هزینه پایین به‌کارگیری رمزنگاری پساکوانتومی نسبت به راه‌حل‌های جایگزین مانند رمزنگاری کوانتومی (۲,۸۷)

۳۳- نگرش منفی نسبت به آینده در بین جوانان (۲,۶۵)

با توجه به داده‌های به دست آمده و پاسخ‌های نخبگان، از ۱۵ عامل خارجی باقی‌مانده، ۵ عامل به‌عنوان فرصت و ۱۰ عامل به‌عنوان تهدید در محیط خارجی شناسایی شدند.

پس از محاسبه اوزان نرمال و به دست آوردن امتیاز واکنش، در جدول ۵ تحت عنوان ماتریس ارزیابی عوامل بیرونی یا **EFE**، امتیاز کشور در پاسخ به عوامل خارجی یا همان تهدیدها و فرصت‌ها ، به دست می‌آوریم.

جدول ۵ - ماتریس ارزیابی عوامل بیرونی یا EFE

ماهیت عامل	شناسه عامل	شرح عامل خارجی	وزن نرمال	امتیاز واکنش	امتیاز موزون
فرصت	O16	متغیر بودن زمان مورد نیاز جهت پیاده‌سازی انواع رمزنگاری پساکوانتومی	۰,۰۵	۳	۰,۱۵
	O27	بازار غیرنظامی قوی برای محصولات رمزنگاری پساکوانتومی	۰,۰۵	۳	۰,۱۵
	O37	وجود زمان تا ساخت رایانه کوانتومی در مقیاس مناسب	۰,۰۹	۴	۰,۳۶
	O41	کاربردهای متنوع نظامی، امنیتی و تجاری رمزنگاری پساکوانتومی	۰,۰۸	۳	۰,۲۴
	O43	تعطیلی‌های مقطعی در سطح کشور و جهان به دلیل بیماری کووید ۱۹	۰,۰۲	۳	۰,۰۶
تهدید	T9	عدم دسترسی کامل به اطلاعات آخرین پیشرفت‌ها در زمینه رمزنگاری پساکوانتومی	۰,۱۰	۱	۰,۱۰
	T24	رباییش اطلاعات در زمان فعلی برای رمزگشایی در آینده با استفاده از رایانه کوانتومی مناسب	۰,۱۶	۱	۰,۱۶
	T25	تحریم‌های موجود علیه ایران	۰,۰۲	۲	۰,۰۴
	T36	شکسته شدن رمزنگاری‌های کلاسیک به دست رایانه کوانتومی	۰,۱۵	۱	۰,۱۵
	T38	وجود فاصله بین خروجی دانشگاه‌ها با صنعت	۰,۰۴	۲	۰,۰۸
	T39	لزوم حفظ امنیت داده‌های رمز شده کشور برای مدت‌زمان زیاد	۰,۱۴	۱	۰,۱۴
	T42	عدم اطمینان به خروجی اعلام شده توسط فراخوان‌های دولتی دیگر کشورها مانند NIST	۰,۰۱	۲	۰,۰۲
	T44	همکاری کشورهای منطقه با شرکت‌های پیشرو در زمینه کوانتوم و رمزنگاری پساکوانتومی	۰,۰۷	۱	۰,۰۷
	T46	عدم وجود خروجی‌های مرتبط با رمزنگاری پساکوانتومی از دانشگاه‌ها	۰,۰۵	۲	۰,۱۰
جمع			۱	-	۱,۸۲

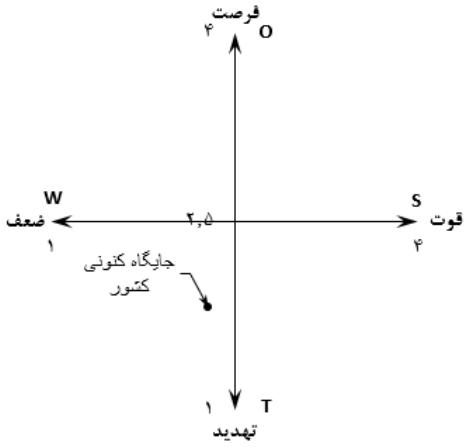
همچنین با توجه به داده‌های به دست آمده و پاسخ‌های نخبگان، از ۲۶ عامل داخلی باقی‌مانده، ۱۰ عامل به‌عنوان قوت و ۱۶ عامل به‌عنوان ضعف در داخل کشور شناسایی شدند.

پس از محاسبه اوزان نرمال و به دست آوردن امتیاز واکنش، ماتریس ارزیابی عوامل داخلی یا **IFE** طبق جدول ۶ ایجاد می‌شود و امتیاز کشور در پاسخ به عوامل داخلی یا همان قوت‌ها و ضعف‌ها را ، به دست می‌آوریم.

جدول ۶ – ماتریس ارزیابی عوامل داخلی یا IFE

ماهیت عامل	شناسه عامل	شرح عامل داخلی	وزن نرمال	امتیاز واکنش	امتیاز موزون
قوت	S8	شناخت بازارهای داخلی و بین‌المللی رمزنگاری پساکوانتومی	۰,۰۲	۳	۰,۰۶
	S12	افزایش تعداد متخصصین حوزه رمزنگاری پساکوانتومی	۰,۰۴	۴	۰,۱۶
	S14	توجه به مسیر حرکت جهانی در زمینه رمزنگاری	۰,۰۶	۴	۰,۲۴
	S15	توجه به دانش‌های روز در اسناد بالادستی	۰,۰۴	۳	۰,۱۲
	S17	تبادل علمی و فنی با دیگر کشورها	۰,۰۳	۴	۰,۱۲
	S18	داشتن تجربه‌های قبلی رویارویی با حملات سایبری مانند استاکس نت	۰,۰۳	۳	۰,۰۹
	S19	افزایش امنیت و اقتدار ملی	۰,۱۰	۳	۰,۳۰
	S20	افزایش قدرت پدافندی کشور	۰,۰۹	۳	۰,۲۷
	S23	ایجاد فرصت‌های شغلی جدید برای متخصصان رمزنگاری یا علوم کوانتومی	۰,۰۵	۳	۰,۱۵
	S28	هماهنگی بین دانشگاه‌های نظامی کشور	۰,۰۱	۳	۰,۰۳
ضعف	W1	عدم‌حمایت مالی از نخبگان	۰,۰۲	۲	۰,۰۴
	W3	سرمایه‌گذاری کم در مقایسه با کشورهای پیشرو	۰,۰۵	۱	۰,۰۵
	W4	عدم وجود استانداردهای لازم برای به‌کارگیری رمزنگاری‌های پساکوانتومی در کشور	۰,۰۶	۲	۰,۱۲
	W5	عدم تمایل نخبگان به همکاری با واحدهای نظامی	۰,۰۲	۲	۰,۰۴
	W6	وجود سلسله‌مراتب دست و پاگیر در مراحل اداری	۰,۰۱	۲	۰,۰۲
	W7	مهاجرت رو به رشد نخبگان و متخصصین	۰,۰۷	۱	۰,۰۷
	W10	عدم اطلاع مدیران سازمان‌ها از اهمیت رمزنگاری پساکوانتومی	۰,۰۴	۱	۰,۰۴
	W13	عدم وجود توان رقابتی محصولات داخلی با نمونه‌های خارجی	۰,۰۴	۲	۰,۰۸
	W21	آگاه نبودن کشور از اهمیت رمزنگاری پساکوانتومی	۰,۰۷	۱	۰,۰۷
	W22	عدم برگزاری همایش‌های مرتبط با رمزنگاری پساکوانتومی	۰,۰۱	۲	۰,۰۲
	W31	عدم جذب متخصصین حاضر در خارج از کشور	۰,۰۶	۱	۰,۰۶
	W32	نبود سامانه یکپارچه ملی برای بیان پیشرفت‌های حاصله	۰,۰۴	۲	۰,۰۸
	W45	نبود استارت‌آپ یا شرکت دانش‌بنیان در زمینه رمزنگاری پساکوانتومی	۰,۰۶	۱	۰,۰۶
جمع			۱	-	۲,۲۹

همان‌گونه که در بخش قبل اشاره شد، مقادیر به دست آمده از دو گام فوق، به ترتیب طول و عرض جایگاه فعلی کشور در زمینه رمزنگاری پساکوانتومی را بر روی دستگاه معادلات موسوم به **SWOT** نمایان می‌کند. بنا بر امتیازات به دست آمده از تحلیل عوامل خارجی، امتیاز کشور بر روی محور تهدید–فرصت ۱,۸۲، و بر اساس امتیازات تحلیل عوامل داخلی، امتیاز کشور بر روی محور ضعف–قوت ۲,۲۹ است. بنابراین شکل ۵، جایگاه کنونی کشور بر روی دستگاه مختصات **SWOT**، در زمینه رمزنگاری پساکوانتومی را مشخص می‌نماید.



شکل ۵ – جایگاه کشور در زمینه رمزنگاری پساکوانتومی بر روی دستگاه مختصات SWOT

از آنجایی که یکی از الزامات تدوین راهبردها، تعیین و تحلیل شکاف بین وضعیت گذشته، وضعیت موجود و وضعیت‌های ممکن و مطلوب است، ما نیز برای تحریر راهبردها، از فن تحلیل شکاف بهره بردیم. در این راستا با بررسی فرصت‌ها و تهدیدها، نقاط قوت و ضعف، جایگاه کشور و برگزاری جلسات با خبرگان و نخبگان، عوامل تأثیرگذار زیر در دستیابی به اهداف بلندمدت و راهبردهای کشور در زمینه رمزنگاری پساکوانتومی، استخراج شدند.

۱- تلاش برای پیاده‌سازی روش‌های گوناگون رمزنگاری مقاوم در برابر رایانش کوانتومی

۲- تمایل به مهاجرت بین نخبگان و متخصصان

۳- میزان سرمایه‌گذاری دولت و بخش خصوصی در زمینه بهبود امنیت و رمزنگاری

۴- وجود زیرساخت تبادل اطلاعات و اشتراک‌گذاری پیشرفت‌ها در زمینه رمزنگاری پساکوانتومی

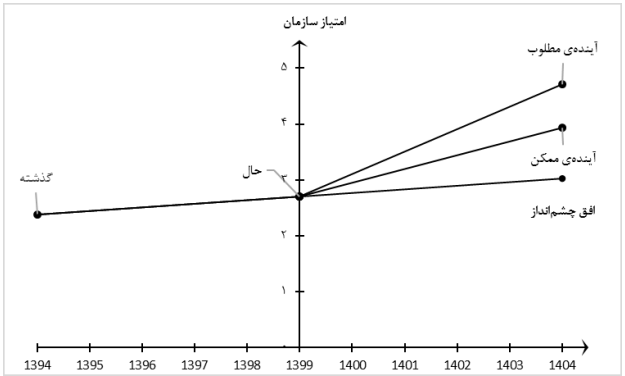
۵- میزان آگاهی مسئولان و مدیران کشور از تهدیدهای نوظهور در زمینه رمزنگاری

۶- وجود استانداردهای ملی برای تعیین انواع رمزنگاری و سطوح امنیت متناسب با شرایط کشور

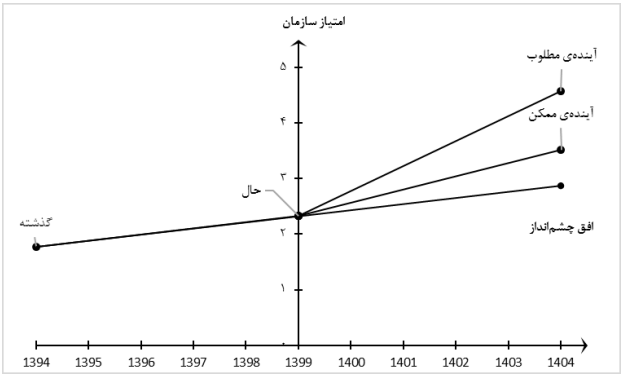
۷- میزان تمایل به همکاری و سرمایه‌گذاری شرکت‌های دانش‌بنیان و خصوصی در زمینه رمزنگاری پساکوانتومی

در ادامه تحلیل شکاف صورت گرفته بر روی هر عامل بر اساس نظر نخبگان و خبرگان زمینه، آورده شده است.

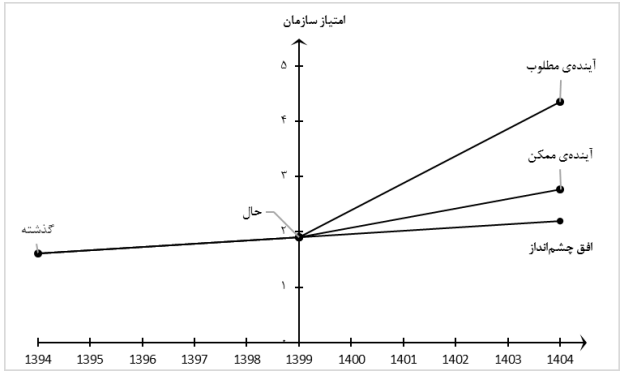
شکل ۶ – تحلیل شکاف تلاش برای پیاده‌سازی روش‌های گوناگون رمزنگاری مقاوم در برابر رایانش کوانتومی



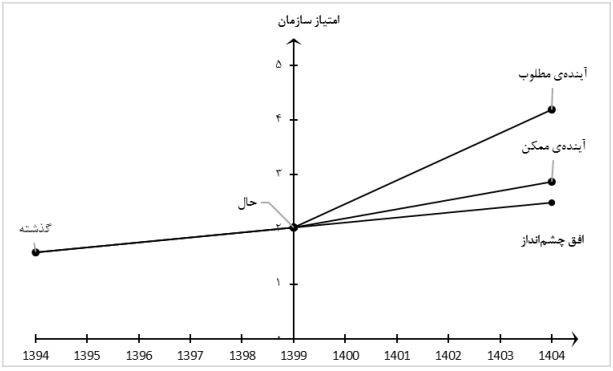
شکل ۷ – تحلیل شکاف تمایل به مهاجرت بین نخبگان و متخصصان



شکل ۸ - تحلیل شکاف میزان سرمایه‌گذاری دولت و بخش خصوصی در زمینه بهبود امنیت و رمزنگاری

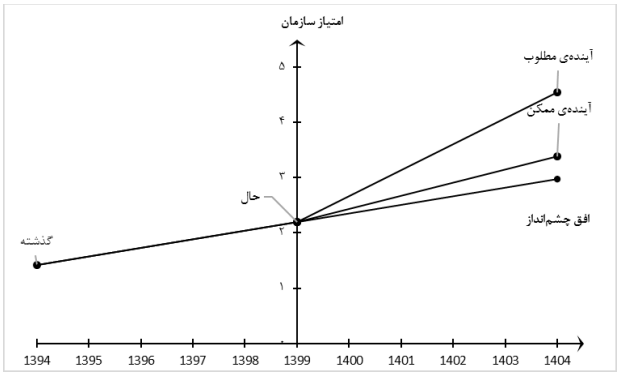


شکل ۹ - تحلیل شکاف وجود زیرساخت تبادل اطلاعات و اشتراک‌گذاری پیشرفت‌ها در زمینه رمزنگاری پساکوانتومی



شکل ۱۰ - تحلیل شکاف میزان آگاهی مسئولان و مدیران کشور از تهدیدهای نوظهور در زمینه رمزنگاری

شکل ۱۱ - تحلیل شکاف وجود استانداردهای ملی برای تعیین انواع رمزنگاری و سطوح امنیت متناسب با شرایط کشور



شکل ۱۲ - تحلیل شکاف میزان تمایل به همکاری و سرمایه‌گذاری شرکت‌های دانش‌بنیان و خصوصی در زمینه رمزنگاری پساکوانتومی

سپس در این گام و با توجه به تحلیل‌های انجام شده در گام‌های پیشین و جایگاه کنونی کشور در زمینه رمزنگاری پساکوانتومی و انجام جلسات نخبگی و خبرگی، راهبردهای مناسب برای دستیابی کشور به اهداف خود در زمینه رمزنگاری پساکوانتومی، به‌صورت زیر ارائه می‌شود.

۱ ایجاد یک مرکز ملی زیر نظر انجمن رمز ایران برای تعیین و تصویب رمزنگاری‌های پساکوانتومی استاندارد و مورد تائید برای دستیابی به سطح امنیت مقبول در کاربردهای مختلف رمزنگاری با هدف مقابله با تهدید رایانش کوانتومی برای رمزنگاری و امنیت با بهره بردن از توجه اسناد بالادستی به دانش‌های روز و تبادلات علمی و فنی با کشورهای پیشرو

۲ ایجاد تمایل به همکاری در بین متخصصان و نخبگان ایرانی رمزنگاری پساکوانتومی در داخل و خارج از کشور از طریق حمایت‌های مالی، ایجاد اشتغال در زمینه رمزنگاری پساکوانتومی، تصویب قوانین حمایت‌کننده، حذف بروکراسی‌های ماشینی اداری و ایجاد فضای مشارکت، رشد و پیشرفت در زمینه رمزنگاری پساکوانتومی برای جبران فاصله با کشورهای پیشرو

۳ جذب بودجه و توجه ارگان‌های دولتی و خصوصی در زمینه اهمیت پیاده‌سازی، آزمون و کسب اطمینان از عملکرد رمزنگاری پساکوانتومی و توسعه این شاخه در داخل کشور توسط شرکت‌های دانش‌بنیان و استارت‌آپ‌ها و ایجاد سازوکار همکاری بین آن‌ها و مراکز دانشگاهی و آکادمیک مانند انجمن رمز ایران

۴ فراهم کردن زیرساخت آموزشی و تبادل اطلاعات زیر نظر انجمن رمز ایران برای به اشتراک‌گذاری آخرین وضعیت و پیشرفت‌های صورت گرفته در زمینه رمزنگاری پساکوانتومی در سطح ملی و جهانی در بین متخصصین و نخبگان و ارائه اطلاعات تعیین‌کننده و تصمیم‌ساز به مسئولین امر به‌صورت دوره‌ای یا رویدادی

همان‌طور که در بخش قبل بیان کردیم در این مرحله راهبردهای ارائه شده در مرحله ششم را از منظر ۷ معیار زیر در بین نخبگان و خبرگان به پرسش می‌گذاریم(جدول ۷). در ادامه مجدداً به این ۷ معیار اشاره می‌کنیم.

- مناسب بودن (آیا رسیدن به آن تأثیرات مطلوب و موردنظر را در بر خواهد داشت؟) -- مربوط به اهداف
- عملی بودن (آیا عمل موردنظر، توسط ابزار موجود قابل پشتیبانی است؟) -- مربوط به روش/ تدبیر
- قابل‌پذیرش بودن (آیا نتایج احتمالی موردنظر آن‌قدر مهم هستند تا توجیهی برای هزینه‌های موردنظر باشند؟) -- مربوط به منابع
- سازگاری با سیاست‌ها
- تناسب داخلی روش و هدف
- تناسب داخلی روش و منابع
- تناسب داخلی هدف و منابع

پس از طی این مراحل و مشخص شدن اولویت راهبردها، در جدول ۸ به توضیح راهکارهای متناسب با راهبردهای بیان شده می‌پردازیم.

جدول ۷- امتیاز جذابیت راهبردهای دستیابی کشور به رمزنگاری پساکوانتومی

شناسه راهبرد	امتیاز جذابیت هر راهبرد							امتیاز نهایی میزان جذابیت
	مناسب بودن	عملی بودن	قابل‌پذیرش بودن	سازگاری با سیاست‌ها	تناسب داخلی روش و هدف	تناسب داخلی روش و منابع	تناسب داخلی هدف و منابع	
۱	۴,۰۶	۴,۰۶	۴,۲۶	۳,۷۴	۳,۷۷	۳,۸۷	۳,۸۱	۲۷,۵۸
۲	۳,۹۴	۳,۵۸	۳,۹۰	۳,۶۸	۳,۶۱	۳,۵۸	۳,۷۱	۲۶,۰۰
۳	۴,۲۹	۳,۵۲	۳,۸۱	۳,۶۸	۳,۶۵	۳,۸۱	۳,۸۴	۲۶,۵۸
۴	۴,۲۶	۴,۰۶	۳,۸۱	۳,۸۷	۳,۵۵	۳,۷۴	۴,۰۰	۲۷,۲۹

جدول ۸ – جدول راهبردها و راهکارهای متناظر

راهبرد	راهکار
۱- ایجاد یک مرکز ملی زیر نظر انجمن رمز ایران برای تعیین و تصویب رمزنگاری‌های پساکوانتومی استاندارد و مورد تائید برای دستیابی به سطح امنیت مقبول در کاربردهای مختلف رمزنگاری با هدف مقابله با تهدید رایانش کوانتومی برای رمزنگاری و امنیت با بهره بردن از توجه اسناد بالادستی به دانش‌های روز و تبادلات علمی و فنی با کشورهای پیشرو.	- حضور نمایندگانی از شورای هماهنگی اطلاعات، سازمان‌های حفاظت اطلاعات، وزارت اطلاعات، انجمن رمز ایران، فعالین داخلی و معتمد این حوزه و نمایندگان شرکت‌های مادر در این مرکز - بررسی مستمر پیشرفت‌ها و سیاست‌های جدید در این حوزه و خروجی‌های مراکز استانداردسازی معتبر جهانی مانند موسسه ملی فناوری و استانداردها - بررسی تهدیدات موجود (مانند سرمایه‌گذاری زیاد کشورهای عضو شورای همکاری خلیج‌فارس و همکاری آن‌ها با شرکت‌های پیشرو در زمینه رایانش و رمزنگاری‌های کوانتومی) بر روی کاربردهای مختلف با بهره بردن از روش پیشنهادی در پژوهش پیش رو - انتخاب روش‌های جایگزین اضطراری برای کاربردهایی که با توجه به روش موسکا و روش پیشنهادی پژوهش پیش رو، در خطر نشت اطلاعات حساس قرار گرفته‌اند. - برای جلوگیری از بروز تجربیاتی مشابه با حملات استاکس نت، در صورت اجبار به خرید برخی محصولات برای برخی از کاربردها از کشورها و سازمان‌های خارجی، بررسی صحت اطلاعات، ریسک‌ها، خطرات و خرابکاری‌های احتمالی، پایش سامانه‌ها و سیستم‌های مختلف موجود و آزمون و ایجاد اطمینان از کارکرد صحیح این سامانه‌ها و محصولات، باید از وظایف این مرکز باشد. - ارائه پیشنهادها و روش‌های لازم، برای کاربردهای مختلف رمزنگاری، در جهت استفاده از روش‌های مختلف رمزنگاری پساکوانتومی یا آماده‌سازی زیرساخت‌ها برای به‌کارگیری روش‌های رمزنگاری پساکوانتومی، با توجه به نیازمندی‌های امنیتی هر کاربرد و متغیر بودن زمانی که برای پیاده‌سازی هر یک از روش‌ها نیاز است. - بهره بردن از دانش متخصصین معتمد عضو مرکز، توجه راهگشای اسناد بالادستی به دانش‌های روز و تأکید این اسناد بر مرتفع ساختن خطرات روزافزون ناشی از پیشرفت‌های علمی و فناوری، شناخت اطلاعاتی اعضای مرکز که عضو دستگاه‌های امنیتی هستند، از شرایط کشور و منطقه و همچنین شناخت اعضای مرکز که عضو شرکت‌های مادر هستند از شرایط عملی موجود در شرکت‌های کشور، برای فراهم کردن شرایط تصمیم‌گیری با در نظر گرفتن تمامی جوانب

۲- ایجاد تمایل به همکاری در بین متخصصان و نخبگان ایرانی رمزنگاری پساکوانتومی در داخل و خارج از کشور از طریق حمایت‌های مالی، ایجاد اشتغال در زمینه رمزنگاری پساکوانتومی، تصویب قوانین حمایت‌کننده، حذف بروکراسی‌های ماشینی اداری و ایجاد فضای مشارکت، رشد و پیشرفت در زمینه رمزنگاری پساکوانتومی برای جبران فاصله با کشورهای پیشرو.	- حمایت مالی و فراهم کردن شرایط کاری مساعد برای محققان و متخصصان داخلی رمزنگاری پساکوانتومی (مانند دکتر اقلیدس که علاوه بر سابقه درخشان رمزنگاری در دانشگاه صنعتی شریف، سوابق مدیریت آزمایشگاه‌ها و افراد را نیز داراست)، محققان ایرانی رمزنگاری پساکوانتومی که به تازگی از ایران خارج شده‌اند (مانند دکتر حسنی کرباسی) که باعث حفظ نیروی انسانی کارآمد و دلسوز، جلوگیری از پیوستن این نیروهای انسانی کارآمد به کشورهای رقیب، هزینه کمتر نسبت به خرید فناوری از کشورهای پیشرو و ایجاد درآمد از طریق همکاری مستشاری و فروش محصولات رمزنگاری پساکوانتومی خواهد شد. - استفاده از دانش متخصصان خارجی کشورهایی که روابط خوبی با آن‌ها داریم برای برگزاری کارگاه‌ها و انتقال تجارب (مانند دکتر اردم آلکیم از کشور ترکیه که تجربه حضور در رویه استانداردسازی موسسه ملی فناوری و استانداردها و ارائه روش موفق رمزنگاری پساکوانتومی به نام NewHope (Alkim, 2016) را دارد) - ایجاد اشتغال و متخصصان و نخبگان زمینه‌های رمز و کوانتوم و بسیاری دیگر از جوانان کشور عزیزمان ایران از طریق جذب در مرکز ملی تصویب رمزنگاری‌ها و تأسیس شرکت‌های فعال در زمینه رمزنگاری پساکوانتومی با توجه به بازار مالی قوی این زمینه.
۳- جذب بودجه و توجه ارگان‌های دولتی و خصوصی در زمینه اهمیت پیاده‌سازی، آزمون و کسب اطمینان از عملکرد رمزنگاری پساکوانتومی و توسعه این شاخه در داخل کشور توسط شرکت‌های دانش‌بنیان و استارت‌آپ‌ها و ایجاد سازوکار همکاری بین آن‌ها و مراکز دانشگاهی و آکادمیک مانند انجمن رمز ایران.	- پیاده‌سازی آزمایشی برخی روش‌های رمزنگاری تائید شده توسط مرکز ملی تصویب رمزنگاری‌های پساکوانتومی در کاربردهای مختلف با همکاری همه جانبه شرکت‌ها و بررسی امنیت و بهبود کارایی و استفاده از آن‌ها - ساماندهی و مدیریت ارگان‌های دولتی و خصوصی و استفاده از علم موجود در شرکت‌های دانش‌بنیان و بهره بردن از چابکی استارت‌آپ‌ها، زیر نظر مرکز ملی استانداردسازی رمزنگاری‌های پساکوانتومی، برای بهره بری در کاربردهای فراوان نظامی و امنیتی و بازار غیرنظامی قوی و ایجاد اشتغال فراوان در کشور - حل مشکلاتی همچون وجود فاصله بین صنعت و دانشگاه، عدم فعالیت دانشگاه‌ها بر روی رمزنگاری پساکوانتومی و عدم تمایل برخی نخبگان و خبرگان به همکاری با واحدهای نظامی، که به دلیل محدودیت‌های امنیتی اعمال شده بر روی آن‌ها است، با جذب سرمایه و توجه شرکت‌های دانش‌بنیان و استارت‌آپ‌ها و دخیل کردن صنعت در این زمینه - تأمین نیازهای داخلی در مورد رمزنگاری‌های پساکوانتومی و بهره‌مندی از بازارهای خارجی با ایجاد رقابت با نمونه‌های خارجی این زمینه، با تأسیس و راه‌اندازی این استارت‌آپ‌ها،

	سرمایه‌گذاری شرکت‌های خصوصی و دولتی و ساماندهی همه این تلاش‌ها در زیر یک مجموعه برای جبران فاصله با کشورهای پیشرو، که علاوه بر افزایش قدرت پدافندی و بازدارندگی کشور، اقتدار و صلابت ملی کشور عزیزمان ایران را در سطح جهانی را بیش از پیش بهبود خواهد بخشید.
۴- فراهم کردن زیرساخت آموزشی و تبادل اطلاعات زیر نظر انجمن رمز ایران برای به اشتراک‌گذاری آخرین وضعیت و پیشرفت‌های صورت گرفته در زمینه رمزنگاری پساکوانتومی در سطح ملی و جهانی در بین متخصصین و نخبگان و ارائه اطلاعات تعیین‌کننده و تصمیم‌ساز به مسئولین امر به‌صورت دوره‌ای یا رویدادی.	- هماهنگی بین تلاش‌های صورت گرفته و اجتناب از دوباره‌کاری در اقدامات جداگانه در سطح کشور از طریق این زیرساخت - جمع‌آوری و ارائه اطلاعات مفید و تصمیم‌ساز برای مدیران و مسئولین در رده‌های مختلف کشور با در نظر گرفتن طبقه‌بندی اطلاعات، در جهت ایجاد زمینه تصمیم‌گیری درخور شرایط واقعی کشور و جهان - ارائه اطلاعات مفید با توجه به رعایت طبقه‌بندی اطلاعات، برای افراد و سازمان‌ها در قالب وبینارهای دوره‌ای، برای جذب سرمایه‌گذاری بیشتر، افزایش آگاهی عمومی بین فعالین این حوزه، علاقه‌مندان و استعدادهای این زمینه، شناسایی مجدد افراد مستعد و جذب این افراد

۲-۴. نتیجه‌گیری و پیشنهاد

به طور کلی می‌توان امنیت را حفاظت از آنچه برای ما ارزشمند است تعریف کرد. این حفاظت دارای سه ویژگی اساسی، محرمانگی، صحت و دسترس‌پذیری است. برای برقراری و حفظ این سه ویژگی، استفاده از رمزنگاری و امضای دیجیتال امن، امری حیاتی و غیرقابل‌اغماض است. بنابراین در هرکجا که نیاز به امنیت اطلاعات و ارتباطات باشد، مجبور به استفاده از رمزنگاری و امضاهای دیجیتال هستیم.

امروزه و در سراسر دنیا، از انواع روش‌های رمزنگاری متقارن و نامتقارن استفاده می‌شود. ولی از آنجایی که طبق قانون شانون، برای حفظ محرمانگی کامل، اندازه فضای کلید باید بزرگ‌تر یا مساوی اندازه فضای پیام باشد، ایجاد محرمانگی کامل در عمل ناممکن است و روش‌های رمزنگاری مورد استفاده که به آن‌ها اشاره داشتیم، در عمل محرمانگی محاسباتی برای ما ایجاد می‌کنند. محرمانگی محاسباتی بدین معنا که با استفاده از رایانه‌های کلاسیک امروزی نمی‌توان این رمزها در زمانی قابل قبول شکست. ولی این محدودیت مختص به رایانه‌های کلاسیک است و اثبات شده است که رایانه‌های کوانتومی با استفاده از الگوریتم‌هایی مانند شور و گروور از این محدودیت عبور می‌کنند و می‌توانند رمزنگاری‌هایی که برای سال‌ها امن بوده و از آن‌ها استفاده می‌شده است را در هم بشکنند. در این صورت امنیت اطلاعات و ارتباطات در تمامی زمینه‌هایی که از رمزنگاری استفاده می‌کنند(اعم از نظامی، تجاری، شخصی و ...)، خدشه‌دار خواهد شد و می‌توان گفت سطوح امنیت مورد نظر توسط رمزنگاری‌های مورد استفاده تأمین نخواهد شد. موضوع مهم دیگر دراین‌بین، امکان ربوده شدن اطلاعات رمز شده در زمان حال است که متخاصمان و دشمنان می‌توانند این اطلاعات رمز شده را نگهداری کنند تا بعداً و در زمان ظهور رایانه‌های کوانتومی قدرتمند، این اطلاعات را شکسته و استخراج کنند.

بنابراین استفاده از روش‌های رمزنگاری مقاوم در برابر رایانش کوانتومی امری غیرقابل‌اجتناب است.

روش‌های رمزنگاری پساکوانتومی و روش‌های رمزنگاری کوانتومی، از راهکارهای رمزنگاری هستند که به نظر می‌رسد در مقابل رایانش کوانتومی مقاوم خواهند بود. ولی روش‌های رمزنگاری کوانتومی برای پیاده‌سازی نیازمند زیرساخت، تجهیزات و سخت‌افزارهای کوانتومی هستند که فعلاً به آن‌ها دسترسی وجود ندارد و درصورتی‌که بخواهی تنها به روش‌های رمزنگاری کوانتومی اکتفا کنیم، احتمالاً زمانی به آن‌ها دسترسی داریم که رایانه‌های کوانتومی نیز پا به عرصه گذاشته‌اند و امنیت اطلاعات ما را از بین برده‌اند و در آن هنگام نیز باز باید زمانی را صرف ایجاد زیرساخت و پیاده‌سازی پایه‌های استفاده از رمزنگاری کوانتومی بکنیم. پس اگرچه ممکن است در بلندمدت استفاده از روش‌های رمزنگاری کوانتومی پاسخ بشر برای مقابله با تهدید رایانش کوانتومی برای امنیت باشد، ولی اکنون امکان بهره‌برداری از این روش‌ها را نداریم. بنابراین تنها راه‌حل در دسترس برای حفظ امنیت خود در زمان ظهور رایانه‌های کوانتومی، استفاده از رمزنگاری‌های پساکوانتومی است. به علاوه بسیاری از متخصصین و صاحب‌نظران زمینه رمزنگاری و امنیت، آینده رمزنگاری جهان را به‌صورت ترکیبی از رمزنگاری پساکوانتومی و کوانتومی پیش‌بینی می‌کنند.

روش‌های رمزنگاری پساکوانتومی با بهره بردن از زیرساخت‌ها و سخت‌افزارهای مورد استفاده فعلی، می‌توانند به‌راحتی جانشین رمزنگاری‌های مورد استفاده فعلی قرار بگیرند. و به دلیل اینکه تنها نیاز به تغییرات نرم‌افزاری دارند، هزینه کمتری نسبت به دیگر روش‌ها بر ما تحمیل می‌کنند. همچنین ذکر این نکته نیز ضروری است که این روش‌ها نیازمند بررسی‌های بیشتر در جهت کسب اطمینان از عملکرد و بهبود استفاده و کارایی هستند. به همین دلیل بدون انجام اقدامات عاجل در زمان حال، درصورتی‌که نیاز حیاتی و فوری به این روش‌ها پیدا کنیم، زمانی که باید صرف برنامه‌ریزی، تحلیل، آماده‌سازی، پیاده‌سازی و آزمون این روش‌ها می‌کردیم را از دست خواهیم داد.

بنابراین در این پژوهش بر آن شدیم که با بررسی حوزه‌ی رمزنگاری پساکوانتومی و موارد فنی آن و با بهره بردن از نظر نخبگان و خبرگان زمینه فناوری اطلاعات، کوانتوم و امنیت، از روش **SWOT** برای این زمینه بهره برده و راهبردهای لازم برای حفاظت از امنیت اطلاعات کشور در تمامی بخش‌ها و در مقابل رایانش کوانتومی را ارائه دهیم. همچنین این راهبردها را اولویت‌بندی کردیم و راهکارهای لازم برای هر یک از این راهبردها را ارائه دادیم تا به هدف نهایی خود یعنی مقابله با خطرات امنیتی گسترده رایانش کوانتومی در سطح فردی، اجتماعی و ملی، دست پیدا کنیم و با استفاده هرچه سریع‌تر از رمزنگاری‌های پساکوانتومی، همچنان بتوانیم از تمامی مزایای رمزنگاری در کاربردهای نظامی و غیرنظامی بهره ببریم. ذکر این نکته باز هم حائز اهمیت هست، که امنیت ما ممکن است همین الان نیز تهدید شده باشد و اطلاعات رمزشده ما به سرقت رفته و در آینده مورد استفاده متخاصمان قرار بگیرد.

مراجع (References)

1. Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In Post-quantum cryptography (pp. 1-14). Springer.

۲. ارائه الگوی مدیریت تحول آفرین تکاملی و روش شناسی طرح ریزی راهبردی. آقامحمدی, شهاب و شریفی, داوود. ۱۳۹۸, مطالعات مدیریت راهبردی دفاع ملی.

3. Alagic, Gorjan, et al., et al. Status report on the first round of the NIST post-quantum cryptography standardization process. s.l. : US Department of Commerce, National Institute of Standards and Technology, 2019.

4. NIST Post-Quantum Cryptography-A Hardware Evaluation Study. Basu, Kanad, et al., et al. 2019, IACR Cryptology ePrint Archive, Vol. 2019, p. 47.

5. Horizon 2020. official website of the European Union. [Online]October 27, 2015. https://ec.europa.eu/programmes/horizon2020/en.

6. Post-quantum cryptography for long-term security. CORDIS EU research results. [Online] May 30, 2017. https://cordis.europa.eu/project/rcn/194347/en.

7. Secure Architectures of Future Emerging Cryptography. CORDIS EU research results. [Online] June 3, 2019. https://cordis.europa.eu/project/rcn/194240/es.

8. NATO works on quantum cryptography with Malta: NATO Web site. NATO Web site. [Online] April 16, 2019. https://www.nato.int/cps/en/natohq/news_165733.htm.

9. Quantum-Safe Cryptography (QSC): ETSI Web site. ETSI Web site. [Online] https://www.etsi.org/technologies/quantum-safe-cryptography.

10. CACRNET Web site. CACRNET Web site. [Online] https://www.cacrnet.org.cn/.

11. Buller, Alicia. The Gulf embraces quantum power: WAMDA Web site. WAMDA Web site. [Online] June 2, 2019. https://www.wamda.com/2019/06/quantum-computing-english.

12. Post-Quantum Cybersecurity Resources: NSA Web site. NSA Web site. [Online] https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/.

13. Paterson, Kenny. Post Quantum Cryptography: IETF Web site. IETF Web site. [Online] https://www.ietf.org/proceedings/99/slides/slides-99-saag-post-quantum-cryptography-01.

14. DARPA, "Strategic Plan,". (2007). Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a468784.pdf

15. Prabhakar, A. (2015). Breakthrough Technologies for National Security. Defense Advanced Research Projects Agency (DARPA), Tech. Rep .

16. Interagency Working Group on Quantum Information Science of the Subcommittee on Physical Sciences, "Advancing Quantum Information Science: National Challenges and Opportunities (2016).

17. Kania, E. B., & Costello, J. K. (2017). Quantum technologies, US-China Strategic Competition, and future dynamics of cyber stability. 2017 International Conference on Cyber Conflict (CyCon US) (pp. 89-96). IEEE.