دریافت مقاله: ۱۳۹۵/۰۱/۱۵
پذیرش مقاله: ۱۳۹۵/۰۸/۱۵

فصلنامهٔ مدیریت نظامی
سال شانزدهم، شمارهٔ ۲، تابستان ۱۳۹۵
ص ص ۴۷-۶۴

مدیریت اطلاعات و منابع در مقابله با حمله‌ها و دستگاه‌های غیرایده‌آل با استفاده از فیزیک کوانتوم

سید عیسی کرانیان[۱]، علی‌اصغر پرویزی[۲]

چکیده

جنگ جهانی اول بیشتر در حوزهٔ جنگ‌های شیمیایی و تسلیحات شیمیایی مطرح بود؛ اما در جنگ جهانی دوم، دنیای فیزیک اتمی و داشتن متخصصان اتمی و مولکولی اهمیت ویژه‌ای پیدا کرد. در دنیای امروز، متخصصان پیش‌بینی می‌کنند که جنگ‌های آینده، جنگ‌های اطلاعات و انفورماتیک خواهد بود و برتری با کشوری است که دارای متخصصان علوم مرتبط با فناوری اطلاعات باشد. از این رو، هدف این پژوهش مدیریت سازمانی، انتقال و نگهداری اطلاعات به صورتِ امن و مطمئن با توجه به پیشرفت‌های اخیر علمی و فناورانه در سازمان‌های نظامی است. در این مقاله با توجه به روش علمی- فیزیکی، ضمن تأکید بر تغییر پارادایم (الگوواره) در مدیریت و تمرکز بر پارادایم کوانتومی، پروتکل (قرارداد)های مختلف رمزنگاری کوانتومی مقایسه می‌شوند. با استفاده از روش شبیه‌سازی و نموداری در کنار تحلیل فیزیکی، قوت‌ها و ضعف‌های هر پروتکل (قرارداد) بیان می‌شود و مدیریت کوانتومی می‌تواند از بسترِ عدم قطعیت و اغتشاشِ ذاتی دنیای کوانتومی به صورت بهینه استفاده کند. نتایج حاصل نشان می‌دهد که بهتر است برای بالا بردن کیفیتِ تجهیزات و دستگاه‌های ارتباطی در مدیریت اطلاعات محرمانه و امنیتی، به جای مقابله با شنودکننده‌ها، تمرکز سازمان بر روی منابع مالی و انسانی قرار گیرد.

واژه‌های کلیدی: پارادایم کوانتومی، مدیریت کوانتومی، تک‌فوتون، رمزنگاری کوانتومی، امنیت اطلاعات، شبیه‌سازی، کیوبیت

---

۱. دانشجوی دکتری نانوفیزیک، عضو هیئت علمی دانشگاه افسری امام علی(ع) (نویسندهٔ مسئول)، ✉ seiedisa.karanian@gmail.com
۲. کارشناس ارشد فیزیک نظری، مدرس دانشگاه افسری امام علی(ع)

مقدمه

در سازمان‌های پیچیده امروزی، روش‌های سنتی مهارت‌های مدیریت از جمله برنامه‌ریزی، سازمان‌دهی، مدیریت و کنترل- که با سرعت زیاد در حال حرکت و تغییر است- مناسب نیستند. توسعهٔ علوم انسانی باید در کنار و هم‌قدم با توسعهٔ علوم طبیعی باشد. برای این منظور اندیشمندان حوزهٔ مدیریت سعی دارند که از مفاهیم فیزیک جدید از جمله مکانیک کوانتومی در جهت مدیریت سیستم‌های پیچیده بهره بگیرند. این امر باعث می‌شود که مدیران محدودیت‌های ناشی از تفکّر مکانیکی و قطعی را کنار زده و مدیران تغییر شوند (شلتون و دارلینگ ۲۰۰۱؛ کاراکاس و فهری، ۲۰۰۹).

از دیرباز کشورها و نظامیان برای انتقال اطلاعات محرمانه از زبان رمز استفاده می‌کردند که به تبعِ آن، شکستن کد و رمز، ضربات جبران‌ناپذیری را به همراه داشته است. سازمان‌های امنیتی و نظامی همیشه در پی روشی بوده‌اند که اطلاعاتشان را به صورت امن و رمزگونه انتقال دهند؛ به گونه‌ای که اگر بیگانگان به آن دست یابند، نتوانند اطلاعات محرمانه را از پیام رمزگذاری شده استخراج کنند. رمزنگاری، هنر تولید پیام است؛ به شکلی که برای افراد غیرمجاز قابل‌فهم نباشد. رمزنگاری، قسمتی از حوزهٔ تحلیل رمز است که شامل شکستن نیز می‌شود. برای شکستن رمز و فهمیدن پیام، باید پیام رمزشده همراه با یک کلید به یک الگوریتم ریاضی داده شود تا پیام قابل‌فهم به دست آید. برای اینکه سیستم رمزنگاری امنیت داشته باشد باید از کلید حفاظت کرد؛ به طوری که الگوریتم ریاضی بدون کلید قابل شکستن نباشد. از آنجایی که امکان دارد کشورها به الگوریتم‌های پیچیدهٔ ریاضی برای شکستن رمز دست پیدا کرده باشند، لزوم حفاظت از کلید و اطمینان از امن بودن آن اهمیت زیادی دارد.

یکی از کلاس‌های مهم سیستم‌های رمزنگاری، سیستم‌های غیرمتقارن است که از کلیدهای مختلفی برای رمزگذاری و شکستن رمز استفاده می‌کند. این سیستم‌ها، به سیستم «کلید عمومی» معروف است. در این سیستم هر شخص یک کلید عمومی و یک کلید خصوصی دارد. کلید عمومی از روی کلید خصوصی ساخته می‌شود و در اختیار همه قرار می‌گیرند. حتی کلیدهای عمومی افراد مختلف را می‌توان در یک دفترچه ارائه داد. اگر شخص «آ» بخواهد به شخص «ب» یک پیام رمزی مخابره کند، به دفترچهٔ راهنما مراجعه می‌کند و با توجه به کلید عمومی شخص «ب» پیام خود را به صورت رمز در می‌آورد؛ سپس شخص «ب» با استفاده از یک الگوریتم ریاضی و کلید عمومی و

خصوصی‌اش، پیام رمز شده را تحلیل و سپس دریافت می‌کند. سیستم‌های رمزنگاری متقارن، همانند سیستم رمزنگاری RSA، طرفداران زیادی دارند (راجرز، ۲۰۱۰).

امنیت سیستم‌های کلید عمومی بر پایهٔ پیچیده بودن و طولانی بودن محاسبات ریاضی استوار است؛ برای مثال امنیت سیستم رمزنگاری RSA بر پایهٔ محاسبه و فاکتورگیری اعداد اول استوار است؛ هر چه اعداد بزرگ‌تر باشند، این محاسبات طولانی‌تر و الگوریتم‌ها پیچیده‌تر خواهند بود. در مجموع امنیتِ سیستم رمزنگاری با کلید عمومی از منظر ریاضی اثبات نشده است. از طرفی سیستم‌های متقارن که برای هر فرد از یک کلید متفاوت برای رمزنگاری و شکستن رمز استفاده می‌کنند، از نظر ریاضی سیستم‌های امنی هستند (همانند سیستم One-Time Pad) (بوخمان، ۲۰۰۴). با این حال در سیستم‌های کلید خصوصی (یا سیستم‌های متقارن) امنیت و انتقال امن کلید و همچنین تولید تصادفی کلید اهمیت فراوانی دارد. در این روش نمی‌توان برای همهٔ پیام‌ها از یک کلید استفاده کرد؛ چون امکان دارد فرد سوم یا شخص شنودکننده با استفاده از پیام‌های رمز شدهٔ مختلف، کلید را به دست آورد. به همین دلیل، در سیستم‌های متقارن باید برای هر پیام یک رمز جداگانه تولید کرد و رمز مورد نظر را به شخص «ب» که مقصد انتقال پیام مهم است، فرستاد. در این مرحله است که پارادایم (الگوواره) کوانتومی مدیریت نقش ایفا می‌کند و مدیریت اطلاعات با پذیرش ماهیت غیر قطعی سیستم با استفاده از رمزنگاری کوانتومی به کمک سیستم‌های رمزنگاری کلاسیکی می‌آید و با فراهم کردن بستر کوانتومی، امکان انتقال کلید به صورت امن را فراهم می‌کند.

همیشه سازمان‌های نظامی و نهادهای امنیتی، به حفاظت اطلاعات و انتقال این اطلاعات به صورت محرمانه علاقه‌مند بوده‌اند. با پیشرفتِ فناوری و ابزارهای رایانه‌ای در دهه‌های اخیر، رمزنگاری و انتقال اطلاعاتِ محرمانه و امن مشکل‌ساز شده و روش‌های سنتی امنیتِ کافی را ندارد. با افزایش قدرت محاسباتی رایانه‌ها، هر رمزی قابل شکستن است و پیام‌های رمزنگاری شده توسط هکرها و کدشکن‌ها قابل شکستن می‌باشند (اسعدی، ۱۳۹۲). امروزه سیستم‌های امنیتی و دانشکده‌های فیزیک آمریکا و کانادا در پی استفاده از رمزنگاری کوانتومی به عنوان روشی نوین و امن در انتقال و رمزنگاری اطلاعات هستند؛ به طوری که دیگر حتی با افزایش قدرت ابررایانه‌ها امنیت پیام‌ها به مخاطره نیفتد. رمزنگاری کوانتومی با استفاده از قوانین بنیادی فیزیک کوانتوم بستری مناسب برای ارتباطات امن فراهم می‌کند.

دو روش اصلی برای رمزنگاری کوانتومی وجود دارد: نخست روشی است به نام BB84 که بنت[1] و برسرد[2] (۱۹۸۴) آن را ارائه کردند. در حالت دیگر از درهم‌تنیدگی[3] حالت‌های کوانتومی فوتون‌ها برای انتقال کیوبیت[4] استفاده می‌کنند (ایکارت، ۱۹۹۱؛ واکس و زیوی، ۲۰۰۲؛ تیتل و همکاران، ۲۰۰۰ و ژنوین و همکاران، ۲۰۰۰). در این مقاله به بررسی روش اول می‌پردازیم و ویژگی‌ها و توانایی‌های نظری و عملی این روش بررسی می‌شود.

بیان مسئله و اهمیت پژوهش

شروع قرن ۲۱ را می‌توان از نظر فناوری «عصر کوانتوم» نامید. رایانه‌ها، اینترنت، بارکد خوان‌ها و جراحی‌های لیزری، تنها چند نمونه از پیامدهای جدید و نوآوری‌های نظریهٔ فیزیک قرن بیستم هستند که «مکانیک کوانتوم» نامیده می‌شوند (شلتون و دارلینگ، ۲۰۰۱).

در مکانیک کوانتوم با رفتارهای رندوم و پیش‌بینی نشده روبه‌رو هستیم که بیان می‌کند: هر کنش همواره با واکنشی به همان اندازه ولی در جهت مخالف همراه نیست. این خصوصیت به این معنا نیست که رفتارهای کوانتومی کاملاً رندوم و اتفاقی هستند، بلکه بیان‌کنندهٔ این واقعیت است که قطعی نیستند. تحقیقات سال‌های اخیر در بیولوژی، روان‌شناسی و فیزیولوژی اعصاب پیشنهاد می‌کند که انسان یک موجود کوانتومی است (دایر، ۱۹۹۵). نه از نظر ابعاد، بلکه از نظر ذهن و اعصاب که تحت تأثیر اصول مکانیک کوانتومی است. محققان حوزهٔ مدیریت بر این باورند که روش‌های مدیریت جدید باید همگام با عصر کوانتوم باشد؛ به‌طوری که به جای استفاده از روش‌های قطعی و قدیمی کنش و واکنش، باید روش‌هایی را مناسب با عدم قطعیت و اغتشاش ناشی از سرعت زیاد تغییرات اتخاذ کنیم.

به طور خلاصه، اصول مکانیک کوانتومی باعث می‌شود که مدیران نگاهشان را به واقعیت وارونه کرده و سعی کنند با نگاهی از درون به بیرون، اختلال و اغتشاش را در مدیریت خود وارد کنند. بدین منظور شلتون (۲۰۰۱) با این فرض که قوانین کوانتومی بر هر چیزی در دنیا حاکم هستند، یک مجموعه از مهارت‌های مدیریتی را بر اساس مفاهیم کوانتومی به صورت زیر معرفی

1. Bennett
2. Brassard
3. entanglement
4. Q-bit

می‌کند: ۱. دیدن کوانتومی؛ ۲. تفکّر کوانتومی؛ ۳. احساس کوانتومی؛ ۴. شناخت کوانتومی؛ ۵. عمل کوانتومی؛ ۶. اعتماد کوانتومی؛ ۷. وجود کوانتومی (شلتون و دارلینگ، ۲۰۰۱)؛

برای اینکه از این دست مهارت‌های کوانتومی- مدیریتی به درستی در سازمان‌ها و انتقال داده‌ها استفاده شود، باید بدانیم:

الف) ما از نظر کوانتومی در دنیایی هوشمند زندگی می‌کنیم؛

ب) همه چیزی در این دنیا با یکدیگر همبسته هستند؛

ج) دنیا از اغتشاش و آشوب برای نظم بخشیدن استفاده می‌کند.

پرسش‌های پژوهش

پرسش اصلی: در مقابل شنودکننده‌ها و نواقص تجهیزاتی برای انتقال اطلاعات نظامی و امنیتی با استفاده از قوانین فیزیک کوانتومی و ماهیت آشوب‌ناک داده‌ها، کدام یک از پروتکل‌های انتقالِ داده، امینت بهتری را برای خطوط ارتباطی فراهم می‌کنند؟

پرسش فرعی: مفاهیم و اصول بنیادی فیزیک کوانتوم چه کاربرد و دستاوردی در حوزهٔ مدیریت سازمانی و اطلاعاتی دارد؟

نگاه نظری پژوهش

توضیح کوانتومی کلید با استفاده از حالت‌های تک فوتون

همان‌طور که در نظریهٔ کلاسیک اطلاعات، هر بیت دو ارزش صفر و یک دارد، کیوبیت (بیت‌های کوانتومی) را هم می‌توان با استفاده از سیستم‌های کوانتومی دوحالتی $|1>$ و $|0>$ تشکیل داد (لد و همکاران ۲۰۱۰). به طوری که حالت کوانتومی یک سیستم دوحالتی را می‌توان به صورت زیر نشان داد:

$$|\psi>= \alpha\,|0> + \beta|1> \qquad (۱)$$

به طوری که آلفا و بتا اعدادی مختلط هستند و $|\psi>$ تابع حالت کیوبیت در فضای دو بعدی مختلط هیلبرت است. علاوه بر اینکه تابع $|\psi>$ دو حالت صفر و یک دارد، که در مجموع احتمال یک دارند، $|\alpha|^2 + |\beta|^2 = 1$، متغیر دیگری هم وجود دارد که فاز بردار مختلط $|\psi>$ را مشخص می‌کند؛ طوری که دو تابع حالت $|\psi>$ و $e^{i\phi}|\psi>$ مقدار یکسانی داشته باشند.

به طور سنتی، حالت‌های قطبش امواج الکترومغناطیسی را می‌توان توسط بردارهای مختلط دوبعدی نمایش داد. در حالت کوانتومی نیز به همین صورت می‌توان حالت‌های قطبش تک

فوتون را توسط یک بردار قطبش دوبعدی مختلط که دو ویژه‌مقدار دارد، در فضای هیلبرت نمایش داد (کولمیتز و پیوک، ۲۰۱۰). چون الکترومغناطیس یک نظریهٔ پیمانه‌ای است، می‌توان نشان داد که بردار توانِ الکترومغناطیسی دو درجهٔ آزادی دارد؛ در نتیجه این دو درجهٔ آزادی خود را در هیلسیتی[1] فوتون نشان می‌دهد، به طوری که حالت‌های قطبش تک فوتون دو ویژه‌مقدار خواهند داشت و از این دو ویژه‌مقدار برای نمایش کیوبیت‌های صفر و یک استفاده می‌کنند (گیسین و همکاران، ۲۰۰۲؛ بنت، ۱۹۹۲).

حالت‌های قطبش عمودی و افقی تک فوتون بر اساس دو بردار حالت هرمیتی زیر نمایش داده می‌شوند:

$$|\psi>_H=\begin{pmatrix}1\\0\end{pmatrix}.\ |\psi>_V=\begin{pmatrix}0\\1\end{pmatrix} \qquad (۲)$$

بر اساس نمایش ماتریسی در مکانیک کوانتومی، می‌توانیم حالت‌های دیگر قطبش را با توجه به این دو بردار پایه به صورت برهمنی از این دو بردار ساخته می‌شوند:

$$|\psi>_{+45}=\frac{1}{\sqrt{2}}\left(|\psi>_H+|\psi>_V\right) \qquad (۳\text{-الف})$$

$$|\psi>_{-45}=\frac{1}{\sqrt{2}}\left(|\psi>_H-|\psi>_V\right) \qquad (۳\text{-ب})$$

$$|\psi>_R=\frac{1}{\sqrt{2}}\left(|\psi>_H+i|\psi>_V\right) \qquad (۳\text{-ج})$$

$$|\psi>_L=\frac{1}{\sqrt{2}}\left(|\psi>_H-i|\psi>_V\right) \qquad (۳\text{-د})$$

به طوری که $|\psi>_L$ و $|\psi>_R$ مربوط به قطبش دایروی راست‌گرد و چپ‌گرد است. اکنون با دانستن اطلاعات پایه‌ای مکانیک کوانتوم در مورد قطبش تک فوتون، می‌توانیم روش رمزنگاری کوانتومی مورد نظر را به طور خلاصه تشریح کنیم.

پروتکل مورد نظر به شکل زیر است:

۱- شخص «آ» (آلیس) یک کیوبت را در یکی از چهار حالت کوانتومی قطبش عمودی، افقی، ۴۵- درجه و ۱۳۵- درجه می‌فرستد (شکل ۱).

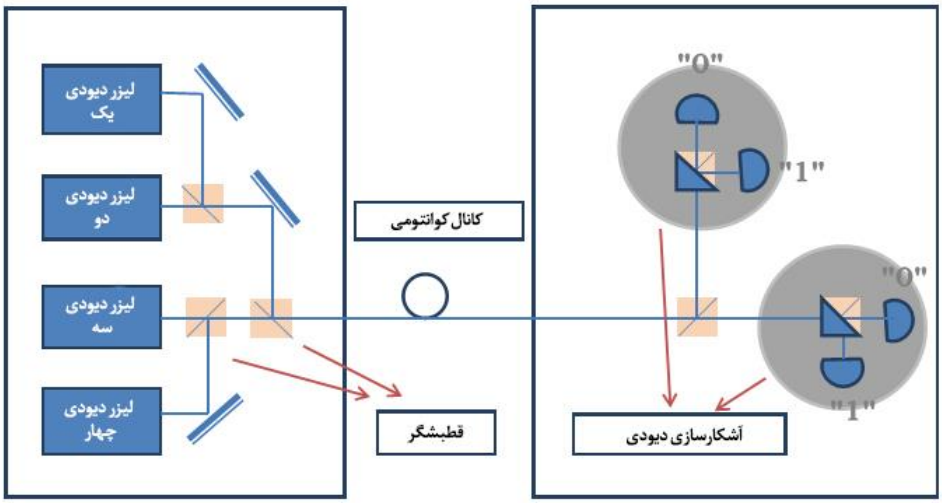
۲- فرد «ب» (باب) به صورت اتفاقی کیوبیت دریافتی را در یکی از حالت‌های پایه می‌بیند و با

1. Helicity

توجه به ویژه‌مقدار حالت مورد نظر ارزش صفر یا یک را به سیگنال دریافتی می‌دهد (شکل ۱).

۳- در مرحلهٔ بعد آلیس و باب با استفاده از یک کانال عمومی پایه‌هایی که بر اساس آنها کیوبیت‌های خود را دریافت و ارسال کرده‌اند به یکدیگر اعلام می‌کنند.

۴- در مرحلهٔ پایانی بر اساس نظریهٔ اطلاعات و آنتروپی سیستم‌های اتفاقی، دو فرایند اصلاح خطا[1] و افزایش امنیّت[2]، را بر روی کیوبیت‌های دریافتی اعمال می‌کنند؛ به این منظور که از خطاهای سیستم‌های اتفاقی کم کرده و از فاش شدن اطلاعات به شخص سوم جلوگیری کنند (مایرز، ۲۰۰۱؛ لوتکنهاوس، ۱۹۹۹).



شکل ۱: قسمت‌های مختلف دستگاه فرستنده و گیرندهٔ سیگنال‌های کوانتومی و کیوبیت‌ها

روش‌شناسی

الف) ماهیت پارادایم

اولین قدم برای پاسخ به پرسش فرعی پژوهش شناخت پارادایم کوانتومی است. در علم و فلسفه

1. error correction
2. privacy amplification

پارادایم مجموعه‌ای از مفاهیم، الگوهای فکری، نظریه‌ها، روش‌های تحقیق و مفروضات است. توماس کوهن در کتاب «ساختار انقلاب‌های علمی» بیان می‌کند که پارادایم، مجموعه دستاوردهای علمی تأیید شده است که در یک بازهٔ زمانی، مجموعه‌ای از مسائل و راه‌حل‌ها را برای جامعه علمی مورد نظر فراهم می‌کند (کوهن، ۲۰۱۲). از جمله:

- آنچه باید دیده شود و مورد تحقیق قرار بگیرد و چه پیش‌بینی‌هایی توسط تئوری انجام می‌شود که در آزمایشی قابل تحقیق است.

نخستین گام در تشریح پارادایم کوانتومی، شناخت ماهیت آن در نقش یک پارادایم است. پارادایم‌ها از محتوا و کارکردهای معیّنی برخوردارند. این محتوا و کارکردها را می‌توان از تعاریفی که برای پارادایم ارائه شده استنباط کرد. هر پارادایم، محدوده‌ای از عالم و قواعد آن را تبیین می‌کند.

رویدادهای جدید و عجیب می‌تواند شروعِ یک پارادایم جدید را نوید دهد. این رویدادها پارادایم‌های قدیمی را به چالش می‌کشند و نیاز به یک پارادایم جدید را به محققان حوزه مورد نظر یادآوری می‌کنند. نقش مکانیک کوانتومی در توضیح و توجیه پدیده‌های ابتدای قرن بیستم و ناکارآمدی فیزیک کلاسیک، نمونه‌ای از این تغییر پارادایم است. به دلیل قدرت جدیدی که فیزیک کوانتوم در نگرش و نحوهٔ تفکر علوم طبیعی فراهم کرد، به مرور در قرن بیستم نفوذ مفاهیم مکانیک کوانتومی در دیگر حوزه‌های علوم طبیعی رشد کرد؛ تا جایی که محققان حوزهٔ علوم انسانی نیز از نگرش جدید استقبال کرده و در توضیح و تشریح یک نوع جدید از مدیریت به نام «مدیریت کوانتومی» از آن بهره برده‌اند (اورمن، ۱۹۹۶). پارادایم کوانتومی سعی دارد با استفاده از چهارچوب مفهومی و نگرشی که ارائه می‌کند، بستری مناسب برای علم مدیریت فراهم کرده و از این طریق با رویکردی نوین، مدیریت مسائل پیش‌رو را بررسی کرده و روشی جدید برای برخورد با سازمان‌های امروزی فراهم کند. برای درک بهتر پارادایم کوانتومی و تحقیق حاضر، شناخت فرضیه‌های این پارادایم مهم است:

ب) فرضیه‌ها

دومین قدم برای پاسخ پرسش فرعی پژوهش، شناخت فرضیه‌های پارادایم کوانتومی است. هر پارادایم نگرش اعضای جامعه علمی را تحت تأثیر قرار می‌دهد. در پارادایم کوانتومی این فرضیه‌ها برگرفته از مکانیک کوانتومی و اصول موضوعِ کوانتوم است. استفاده از فیزیک کوانتوم در رمزنگاری خصوصیات ویژه‌ای را در اختیار ما قرار می‌دهد که در ادامه به آنها اشاره می‌شود:

۱- هر مشاهده‌ای حالت‌های سیستم را مختل می‌کند.

۲- به دلیل همبستگی، نمی‌توان به طور هم‌زمان قطبش یک فوتون را در پایه‌های افقی- عمودی و قطری اندازه‌گیری کرد.

۳- نمی‌توان یک حالت کوانتومی ناشناخته را کپی کرد.

در پاسخ به پرسش فرعی پژوهش، کاربرد پارادایم کوانتومی این است که شخص «آ» و «ب» می‌توانند امن بودن خط خود را با فرستادن کیوبیت کنترل کنند و با تبادل سیگنال‌های کوانتومی متوجه شوند که آیا خطوط انتقال اطلاعات امن است و یا توسط یک شنونده در حال شنود است. بدین صورت اگر شنودکننده‌ای سیگنال‌های کوانتومی را ببیند، باعث اختلال در حالت‌های سیگنال‌ها می‌شود و این اختلال توسط «آ» و «ب» قابل‌مشاهده است. در نظریهٔ کوانتوم، جهان اساساً مجموعه‌ای از علائم و یا میدان‌های اطلاعات است؛ بنابراین در ارتباط بودن و تعامل مشخصه ذاتی پدیده‌های کوانتومی است.

دستاورد مدیریتی پارادایم کوانتومی- به عنوان بخش دوم جواب سؤال فرعی پژوهش- بیان می‌کند که پدیده‌های کوانتومی با یکدیگر همبسته و وابسته هستند که از ویژگی‌های پارادایم کوانتومی بوده و در مدیریت کوانتومی جدید مورد توجه قرار گرفته است. خاصیتی که برخلاف دیدگاه‌های جزئی‌نگر کلاسیکی، نگرش کل‌گرایانه دارد و روابط میانِ اجزا را مورد توجه قرار می‌دهد. در این پارادایم فکری، اجزا هویّت مستقل و جداگانه‌ای ندارند که بتوان با استفاده از روش‌های مدیریتی جز به جز قدیمی کلیت یک سازمان را کنترل کرد. این پارادایم همچنین بیان می‌کند که برای توفیق در راهبرد یک مجموعه، باید کلیت اجزا و روابط را مدنظر قرار داد.

از مَنظر پارادایم کوانتومی، رفتارِ انسان مجموعه‌ای از کنش‌های کوانتومی است؛ از سوی دیگر با توجه به نظریهٔ «همبستگی کوانتومی» رفتارِ انسان همبسته و در ارتباط با اجزا و انسان‌های دیگر تعریف می‌شود. این نگرش یک روش‌شناسی متفاوت از گذشته را برای حیات سازمانی و رفتار سازمانی انسانی ایجاب می‌کند.

مدیریت کوانتومی

پارادایم کوانتومی در مدیریت سعی می‌کند تا مفاهیم و اصول نظریهٔ کوانتومی را جهت توصیف و تبیین پدیده‌های سازمانی و حل مسائل مدیریتی مورد استفاده قرار دهد. مدیریت کوانتومی در

مقابل با مدیریت سنتی از نگرش دنیای کوانتومی به اطراف و ابزارها بهره می‌برد تا به تصمیم‌گیری و نتیجه مناسب‌تری برای الگوهای مدیریتی خود برسد (محمد هادی، ۱۳۹۰؛ افجه و حمزه‌پور، ۱۳۹۴).

روش تحقیق و متغیرهای پژوهش

پارادایم کوانتومی در مدیریت و به‌کارگیری منابع انسانی و مالی رهنمودهای مشخصی را ارائه می‌دهد که در فرایند تجزیه و تحلیل داده‌های پژوهشی راهگشای بسیاری از مسائل و چالش‌های موجود در نظریهٔ اطلاعات و روش‌شناسی موجود در این زمینه است. اکنون زمان آن فرا رسیده که از تمرکز بر روی روش‌های کلاسیکی نظریهٔ اطلاعات فاصله گرفته و با در نظر گرفتن فرضیه‌های پارادایم کوانتومی، وجود اغتشاش و آشوب در سیستم‌ها به رسمیّت شناخته شود و از این ویژگی بنیادی طبیعت در راستای رسیدن به اهداف مورد نظر استفاده شود.

برای هر پارادایم علمی به تناسب زمینه و موضوع آن، روشی خاص وجود دارد که در این مقاله با تکیه بر مدل‌های مکانیک کوانتومی و با استفاده از آنالیز ریاضی داده‌ها سعی شده تا توضیحی مناسب برای اولویت‌های مدیریتی انتقال اطلاعات در بستر پارادایم و نظریه اطلاعات کوانتومی ارائه شود. متغیر پژوهش حاضر احتمال خطای داده‌ها در انتقال اطلاعات از شخص «آ» به «ب» است که با δ نشان داده می‌شود. برای این متغیر تابع امنیت $Q(\delta)$ و $P(\delta)$ برای دو پروتکل متفاوت از طریق قوانین آماری و کوانتومی به دست می‌آید. بازه متغیر پژوهش از طریق رایانه شبیه‌سازی شده و میزان امنیت داده‌ها بر حسب مقادیر شبیه‌سازی شده برای خطای داده‌ها به صورت نمودار گزارش شده است.

دو پروتکل مختلف رمزنگاری کوانتومی

پس از اینکه آلیس و باب، کلید را به صورت بیت‌های کوانتومی به یکدیگر انتقال دادند، کلید مورد نظر شامل خطاهایی است که این خطاها از طریق ناکامل بودن و نواقص فناورانه دستگاه‌های ارتباطی و یا از طریق یک اخلالگر و شنودکننده وارد کلید شده است. این خطاها حدود چند درصد هستند که باید از طریق ملاحظات و روش‌های مختلف از کلید اولیه حذف شوند تا کلید نهایی درست و امن به دست آید (گوبی و همکاران، ۲۰۰۴).

برای این منظور از تابع آنتروپی شنن استفاده می‌شود (شنن، ۲۰۰۱). در نظریهٔ اطلاعات، آنتروپی معیاری برای عدم قطعیت در متغیرهای تصادفی است. آنتروپی شنن مقدار انتظاری

اطلاعاتی که در یک پیام وجود دارد را نشان می‌دهد. تابع آنتروپی شنن برای متغیر تصادفی X با احتمال $P_X(x)$ به صورت زیر تعریف می‌شود:

$$H(X) = -\Sigma_x P_X(x)\ logP_X(x) \qquad (۴)$$

به طوری که برای یک متغیر تصادفی دوتایی δ با توزیع $\{\delta . 1-\delta\}$ می‌شود:

$$H(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta) \qquad (۵)$$

با توجه به استدلال شور[1]- پرسکیل[2] می‌توان فرایندِ اصلاح خطا و تقویت امنیّت را به دو پارامتر δ_b و δ_p مربوط دانست که به ترتیب نرخِ خطای بیت‌ها و نرخِ خطای فازی هستند (شور و پرسکیل، ۲۰۰۰). در صورتی که n تعداد کیوبیت‌های پیام و k تعداد کیوبیت‌های اصلاح شدهٔ پیام باشند، برای به دست آوردن نرخِ تولید کیوبیت‌های مطمئن و امن به صورت زیر عمل می‌کنیم:

$$R = \frac{k}{n} > 1 - H(\delta_b) - H(\delta_p) \qquad (۶)$$

GLLP[3] بر اساس استدلال شور- پرسکیل بیان می‌کنند که اگر دستگاه‌های ما عاری از نواقص فناورانه باشند، یک شنودکننده هیچ اطلاعی از پایه‌های ارسال سیگنال‌های کوانتومی نخواهد داشت؛ در نتیجه مقدار $|\delta_b - \delta_p|$ تقریباً قابل چشم‌پوشی است و میان نرخِ خطای فازی و بیت‌ها یک تعادل و توازن وجود دارد. GLLP این استدلال را توسعه می‌دهند و موارد کلی‌تری را ارائه و معرفی می‌کند (گاتسمان و همکاران، ۲۰۰۴). آنها توضیح می‌دهند که اگر دستگاه‌های ما دارای نواقص باشند، این نواقص می‌توانند اطلاعاتی را در مورد پایه‌های ارسال کیوبیت‌ها به شخص سوم یا شنودکننده بدهد و یک شنودکننده می‌تواند با دانستن پایه‌های استفاده شده توسط آلیس، اطلاعاتی را از کیوبیت‌های ارسال شده به دست آورد و باعث اختلال در انتقال نرخِ کلید شود.

از منظر ریاضی، یعنی اگر سکه‌ای را به هوا پرتاب کنیم، در حالت ایده‌آل، سکه سالم و بدون هیچ‌گونه نقص فیزیکی، احتمال آمدن شیر یا خط با هم برابر است؛ اما اگر این سیستم فیزیکی دارای نواقص باشد، این نواقص توازن احتمال برابر را به هم می‌زند و دیگر احتمال آمدن شیر

1. Shor, P. W.
2. Preskill, J.
3. Gottesman-Lo-Lütkenhaus-Preskill (GLLP)

برابر ۱/۲ نیست. به همین صورت، زمانی که دستگاه‌ها و لیزرهای ما ایده‌آل نباشند و دارای نواقص فناورانه باشند، این نواقص می‌تواند به یک شنودکننده اطلاعاتی را انتقال دهد و باعث به هم خوردن توازن نرخ خطای فازی و بیت‌ها شود، به طوری که خواهیم داشت:

$$\left|\delta_b - \delta_p\right| < 2f(\Delta) \qquad (۷)$$

Δ معیاری از برهم خوردن توازن میان نرخ‌های خطا است. بر این اساس حداقل نرخ تولید کلیدهای امن و مطمئن را به صورت زیر می‌نویسیم:

$$R \geq 1 - H(\delta) - H(\delta + 2f(\Delta)) \qquad (۸)$$

تا اینجا به مسئلهٔ نواقص دستگاه‌ها پرداخته شد. در ادامه به این سؤال پاسخ می‌دهیم که اگر شنودکننده بدون داشتن اطلاعات اولیه دست به اختلال در ارسال سیگنال‌های کوانتومی بزند، چه خواهد شد؟ برای این منظور از نظریهٔ کوانتومی احتمالات برخوردها استفاده می‌شود و پس از اصلاح نرخِ تولید کلید با منظور کردن خطای بیت‌ها، با استفاده از نظریهٔ کوانتومی احتمال برخوردها بخش دیگری از کوبیت‌های کلید را برای افزایش امنیت، خارج کرده و نرخ تولید کلید زیر به دست می‌آید (لوتکنهاوس، ۲۰۰۰):

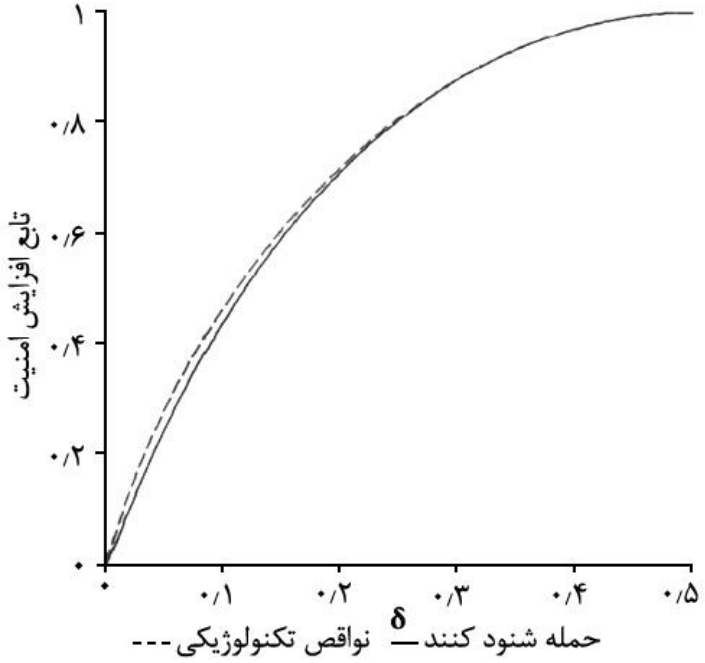
$$R \geq q\{-Q_\mu H_2(\delta) + Q_1[1 - \log_2(1 + 4\delta - 4\delta^2)]\} \qquad (۹)$$

این رابطه بدون در نظر گرفتن خطای دستگاه‌های ارسال کنندهٔ کیوبیت‌ها، خطای حاصل از اختلالات انسانی و مخرب را در مسیر انتقال کلید رمزنگاری ارائه می‌دهد.

یافته‌های پژوهش

در این بخش برای پاسخ به پرسش اصلی پژوهش به مقایسه دو پروتکل مهم رمزنگاری کوانتومی پرداخته و پروتکل‌ها با یکدیگر مقایسه می‌شوند؛ به این هدف که میزان اهمیت نواقص فناورانه و غیر ایده‌آل بودن دستگاه‌ها و اختلالات ناشی از شنودکننده سنجیده شود.

همان‌طور که در روابط (۸) و (۹) دیده می‌شود، نرخِ تولید کلید امن برای دو پروتکل مختلف در دو جملهٔ مربوط به افزایش امنیت متفاوت هستند. در هر دو عبارت، بخش مربوط به اصلاحِ خطا یکسان است ولی در قسمت مربوط به کاهش اطلاعات شنودکننده متفاوت هستند. با استفاده از شبیه‌سازی می‌توان دید که این دو رابطه تا چه حد با یکدیگر تفاوت دارند و در بررسی و اهمیت‌سنجی، کدام یک باید بیشتر مورد توجه قرار گیرد.



شکل ۲ : مقایسه دو پروتکل در تقریب مرتبهٔ صفرم. δ: نرخ خطای بیت‌ها

اگر نرخِ خطای بیت‌ها دست‌خوش تغییرات اندکی باشد و نرخِ خطای بیت‌ها و فازها برابر باشد، شکل ۲ نشان می‌دهد که ایده‌آل گرفتن دستگاه‌ها، با در نظر گرفتن حملهٔ شنودکننده‌ها بدون داشتن اطلاعات اولیه در مورد سیگنال‌های ارسالی «آ» هم‌ارز است. در ادامه به بررسی میزان هم‌ارزیِ این دو پروتکل می‌پردازیم. اگر دستگاه‌ها ایده‌آل نباشند و یا نرخِ خطای کیوبیت‌ها دارای درصدی از تولرانس باشد، این نمودارها چه تغییری می‌کنند؟ آیا باز هم این دو پروتکل با هم برابر خواهند بود یا خیر؟

پروتکل اول (در نظر گرفتن نواقص فناورانه): با در نظر گرفتن دستگاه‌های غیر ایده‌آل و عدم توازن بین پایه‌ها خواهیم داشت:

$$H(\delta+\Delta)=\sum_{i} Q_i(\delta)\Delta^i \qquad (۱۰)$$

به طوری که برای مراتب اولیه تقریب روابط زیر به دست می‌آید:

$$Q_1(\delta) = -\frac{-\ln(1-\delta)+\ln(\delta)}{\ln(2)} \quad (۱۱\text{- الف})$$

$$Q_2(\delta) = \frac{1}{2(\delta-1)\ln(2)\ \delta} \quad (۱۱\text{- ب})$$

$$Q_3(\delta) = -\frac{2\delta-1}{6(\delta-1)^2\ln(2)\ \delta^2} \quad (۱۱\text{- ج})$$

پروتکل دوم (در نظر گرفتن حملات شنودکننده‌ها): برای مراتب تقریب مختلف، تابع کوانتومی احتمالات برخورد به صورت زیر است:

$$\tau(\delta+\Delta) = \sum_i P_i(\delta)\Delta^i \quad (۱۲)$$

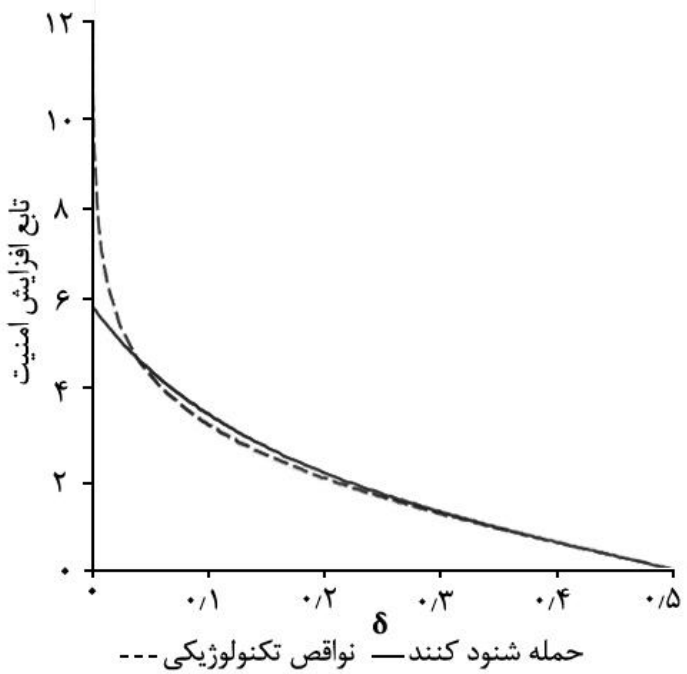
$\tau(\delta)$ تابع احتمالات برخورد کوانتومی بر حسب نرخ خطای بیت‌ها است، به طوری که:

$$P_1(\delta) = \frac{4(2\delta-1)}{\ln(2)(4\delta^2-4\delta-1)} \quad (۱۳\text{- الف})$$

$$P_2(\delta) = -\frac{4(3-4\delta+4\delta^2)}{\ln(2)\,(4\delta^2-4\delta-1)^2} \quad (۱۳\text{- ب})$$

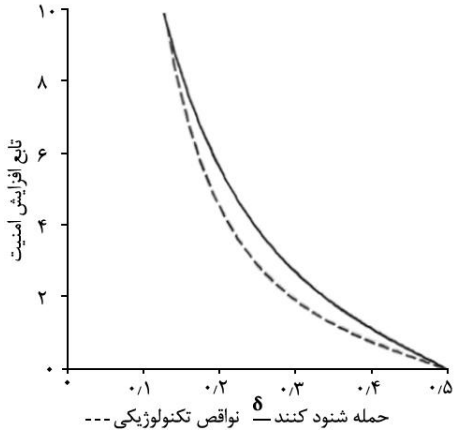
$$P_3(\delta) = \frac{16}{3}\frac{(2\delta-1)(7-4\delta+4\delta^2)}{\ln(2)\,(4\delta^2-4\delta-1)^3} \quad (۱۳\text{- ج})$$

در ادامه پروتکل مورد نظر برای دستگاه‌های غیر ایده‌آل با پروتکل حملهٔ شنودکننده در حالت داشتن اطلاعات اولیه در مورد کیوبیت‌ها در مراتب مختلف تقریب با یکدیگر مقایسه می‌شوند. شکل ۳ مرتبهٔ اول تقریب (رابطه‌های ۱۲- الف و ۱۳- الف) را نشان می‌دهد.

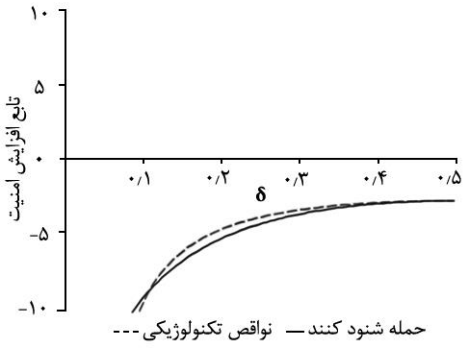


شکل ۳: مقایسه دو پروتکل در تقریب مرتبهٔ اول. $Q(\delta)$ (نمودار آبی‌رنگ) و $P(\delta)$ (نمودار قرمزرنگ)

همان‌طور که در شکل ۳ دیده می‌شود، برای دو تابع امنیت $Q(\delta)$ (نمودار- خط پیوسته) و $P(\delta)$ (نمودار- خط‌چین) زمانی که نرخِ خطای کیوبیت‌ها پایین است، در مرتبهٔ اول تقریب ملاحظات ناشی از غیرایده‌آل بودن دستگاه‌ها (پروتکل اول) اهمیت بیشتری پیدا می‌کنند و نرخ تولید کلید امن را پایین می‌آورند. شبیه‌سازی تقریب‌های مربوط به مراتب دوم و سوم در شکل‌های ۴ و ۵ به نمایش گذاشته شده است. در این مراتب تقریب، این دو پروتکل شبیه به یکدیگر رفتار می‌کنند.



شکل ۴: مقایسه دو پروتکل در تقریب مرتبهٔ دوم



شکل ۵: مقایسه دو پروتکل در تقریب مرتبهٔ سوم

بحث و نتیجه‌گیری

در این مقاله سعی شد، علاوه بر تأکید بر اهمیت استفاده از علوم و فناوری نوین در جنگ‌های الکترونیک امروزی و نقشِ نظریه‌های مدرن فیزیک در مدیریت و رمزنگاری، در بستر پارادایم مدیریت کوانتومی دو پروتکل مهم مربوط به رمزنگاری کوانتومی بررسی و شبیه‌سازی شود. این دو پروتکل هر کدام توسط توابع امنیّت $Q(\delta)$ و $P(\delta)$ به طور جداگانه دو ملاحظهٔ مهم مربوط به رمزنگاری کوانتومی را بررسی کرده‌اند. در یکی نقشِ نواقص فناورانه و مشکلاتی که دستگاه‌های غیره ایده‌آل (همانند لیزرها و آشکارسازهای غیر ایده‌آل) از منظر ریاضی و فیزیکی به وجود می‌آورند؛ (نمودار خط‌چین در اشکال ۲ تا ۵) و در دیگری نقش یک اختلال‌گر و شنودگر را از منظر مکانیک کوانتومی بررسی شد (نمودار خط پیوسته در اشکال ۲ تا ۵). با توجه به نتایج مقالهٔ حاضر، مدیریت کوانتومی با پذیرش نقش عدم قطعیت و اغتشاش در سیستم‌ها، نقش نواقص فناورانه و مشکلات ناشی از دستگاه‌های غیر ایده‌آل را مهم‌تر از اختلالات ناشی از حمله‌کننده‌ها و شنودگرها ارزیابی کرده است. به همین دلیل پیشنهاد می‌شود که در مدیریت انتقال اطلاعات به صورت رمز و استفاده از رمزنگاری کوانتومی به ساخت و طراحی دستگاه‌ها بیشتر توجه شود؛ همچنین تلاش شود تا دستگاه‌ها، لیزرها، قطبش‌گرها و پلورایزرهایی طراحی و ساخته شوند که کمترین نقصِ فنی و بهترین کیفیت را داشته باشند.

اگر پروژه‌های راهبردی رمزنگاری کوانتومی با نگاهی به مبحث مدیریتی و پدافندی طراحی

شوند، آسیب‌پذیری سازمان‌ها در برابر تهدیدات و اقدامات دشمن کاهش می‌یابد. از جمله دستاوردها و نوآوری‌های پژوهش حاضر، استفاده از علوم و فنون نوین و فیزیک جدید در «مدیریت منابع»؛ سرویس‌های نظامی انتقال امن کلید رمز با استفاده از اصول پایه مکانیک کوانتومی؛ طراحی اولیه و امکان‌سنجی یک دستگاه رمزنگاری کوانتومی (شکل ۱)؛ بالا بردن امنیتِ سیستم‌های رمزنگاری در پدافند و امنیّت انتقال اطلاعات راداری و کدشده است.

فهرست منابع

افجه، سید علی‌اکبر؛ حمزه‌پور، مهدی (۱۳۹۳). رهیافتی جامع از نظریه رهبری کوانتومی و کاربردهای آن در سازمان. اندیشه مدیریت راهبردی، ۸(۲)، ۱۶۱-۲۰۴.

محمدهادی، فریبرز (۱۳۹۰). پارادایم کوانتومی در علم مدیریت. مدیریت فرهنگ سازمانی، ۹(۲۳)، ۷۱-۹۴.

Bennett, C. H., & Gilles, B. (1984). *Quantum cryptography: Public key distribution and coin tossing*. *Proceedings of IEEE.* International Conference on Computers, Systems and Signal Processing, 175-179.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters, 68*(21), 3121-3132.

Buchmann, J. (2004). *Introduction to Cryptography*. Second Edition, Springer.

Dyer, W. W. (1995). *Your sacred self*. HarperCollins Audio Books.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters 67*(6), 661-663.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics, 74*(1) 145-159.

Gobby, C., Yuan, Z. L., & Shields, A. J. (2004). Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters, 84*(19), 3762-3764.

Gottesman, D., Lo, H. K., Lütkenhaus, N., & Preskill, J. (2004). *Security of quantum key distribution with imperfect devices*. In Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on (p. 136). IEEE.

Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., & Zeilinger, A. (2000). Quantum cryptography with entangled photons. *Physical Review Letters, 84*(20), 4729-4735.

Karakas, F. (2009). New paradigms in organizational development in the 21st

century: Positivity, spirituality, and complexity. *Organization Development Journal, 27*(1), 245-251.

Kollmitzer, C., & Mario, P. eds. (2010). *Applied quantum cryptography*. Vol. 797. Springer.

Kuhn, T. S. (2012). *The structure of scientific revolutions*. University of Chicago press.

Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. *Nature, 464*(7285), 45-53.

Lütkenhaus, N. (1999). Estimates for practical quantum cryptography. *Physical Review, 59*(5), 3301-3314.

Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Physical Review, 61*(5), 52304-52314.

Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM (JACM), 48*(3), 351-406.

Overman, E. S. (1996). The new science of management Chaos and quantum theory and method. *Journal of Public Administration Research and Theory*, *6*(1), 75-89.

Buchmann, J. (2004). *Introduction to Cryptography*. Springer-Verlag.

Kollmitzer, C., & Pivk, M. (2010). *Applied Quantum Cryptography*. Springer.

Rogers, D. J. (2010). *Broadband Quantum Cryptography*. Morgan and Claypool Publishers.

Tittel, W., Brendel, J., Zbinden, H., & Gisin, N. (2000). Quantum cryptography using entangled photons in energy-time Bell states. *Physical Review Letters, 84*(20), 4737-4740.

Waks, E., Zeevi, A., & Yamamoto, Y. (2002). Security of quantum key distribution with entangled photons against individual attacks. *Physical Review, 65*(5), 52310-52326.