هو النّور

« حضوری گر همی خواهی از او غایب مشو حافظ »

دانشکده علوم ریاضی

گروه علوم کامپیوتر

پایان‌نامه

برای دریافت درجه کارشناسی ارشد

در رشته علوم کامپیوتر گرایش سیستم‌های کامپیوتری

عنوان

پیشنهاد یک روش امن تبادل کلید سه طرفه

استاد راهنما

دکتر جابر کریم‌پور

استاد مشاور

پروفسور دکتر آیاز عیسی‌زاده

پژوهشگر

مسعود اقدسی‌فام

بهمن ۱۳۹۳

تقدیم به

هر آنکه با کلامش، نگاهش، قلمش ... و عشق

مرا کلمه‌ای آموخت.

« ای رستخیز ناگهان وی رحمت بی‌منتها
ای آتشی افروخته در بیشه‌ی اندیشه‌ها
خورشید را حاجب تویی اومید را واجب تویی
مطلب تویی طالب تویی هم منتها هم مبتدا »

بر لوح دل جای دارند و قدردانشان هستم

پدر، مادر و برادرانم؛ همواره این کوچکترین را پشتوانه بوده‌اند.
گام‌هایم را محترم داشته؛ آرزوهایم را ارج نهاده‌اند.
دکتر جابر کریم‌پور؛ استادی که معلمی را برادرانه به جای آورد و
بر آتش شوق دروغم دمید.
پروفسور آیانر عیسی‌زاده؛ بزرگی که عاشقانه بشارتمان می‌دهد به
دنیای نور و شور و عشق.

نام خانوادگی دانشجو: **اقدسی‌فام** نام: **مسعود**

عنوان پایان‌نامه: **پیشنهاد یک روش امن تبادل کلید سه طرفه**

استاد راهنما: **دکتر جابر کریم‌پور ینگجه**

استاد مشاور: **پروفسور دکتر آیاز عیسی‌زاده**

مقطع تحصیلی: **کارشناسی ارشد** رشته: **علوم کامپیوتر** گرایش: **سیستم‌های کامپیوتری**

دانشگاه: **دانشگاه تبریز** دانشکده: **علوم ریاضی**

تاریخ فارغ‌التحصیلی: **بهمن ۱۳۹۳** تعداد صفحه: **۹۱**

کلیدواژه‌ها: **امنیت داده‌ها، تبادل امن کلید، تبادل کلید سه طرفه، رمزنگاری پسا کوانتومی، رمزنگاری مشبکه‌مبنا و رمزنگاری NTRU**

چکیده: **تبادل امن کلید در پروتکل‌های مبتنی بر روش‌های رمزنگاری متقارن یکی از پارامترهای مهم تامین محرمانگی انتقال اطلاعات در ارتباطات شبکه‌ای است. این فرآیند به طور عمومی با استفاده از سامانه‌های رمزنگاری کلید نامتقارن صورت می‌گیرد که مبتنی بر سختی حل مسائل ریاضی مانند مسأله‌ی لگاریتم گسسته (DLP) و مسأله‌ی تجزیه‌ی اعداد صحیح (IFP) هستند. پس از ارائه‌ی الگوریتم «شور» در سال ۱۹۹۶ امکان حل این مسائل سخت در زمان قابل قبول توسط سامانه‌های کوانتومی مطرح شد که باعث گردید شاخه‌ی جدیدی از تحقیقات بر روی روش‌های مقاوم در برابر حملات کوانتومی شکل گیرد. از طرفی، فرآیند تبادل نیاز به شاخصه‌ای برای تایید هویت طرف مقابل دارد. روش‌های تبادل امن کلید سه طرفه، شاخه‌ای از روش‌های تبادل امن کلید هستند که علاوه بر دو طرف ارتباط یک طرف سوم واسط و مورد اعتماد در فرآیند تبادل کلید نقش ایفا می‌کند، تا علاوه بر افزودن امکان احراز هویت طرفین ارتباط، کارایی روش‌ها را نیز برای استفاده در شبکه‌های بزرگ بهبود بخشد.**

در این پایان‌نامه یک راهکار نوین تبادل کلید سه طرف مبتنی بر رمزنگاری مشبکه مبنا ارائه و امنیت آن بحث شده است. این راهکار در مقابل حملات کوانتومی شناخته شده تا کنون مقاوم بوده و ادعا می‌شود تمام خواص مورد نیاز برای امن بودن یک روش تبادل کلید را دارد.

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

فصل ۱

مقدمه

رمزنگاری[1] و حفظ محرمانگی اطلاعات سابقه‌ای چند هزار ساله دارد که در زمان‌های گذشته محدود به مسائل نظامی و امور مدیریت کشوری می‌شد. اما امروزه با پیشرفت فناوری و استفاده از انواع و اقسام سامانه‌های نرم‌افزاری و سخت‌افزاری برای مدیریت انواع مختلف اطلاعات روزمره‌ی زندگی، تامین امنیت عملکرد و حفظ محرمانگی اطلاعاتشان بسیار مورد توجه قرار گرفته است. در عصر کنونی علاوه بر به شبکه‌های ارتباطی گسترده مانند اینترنت، وجود فناوری‌های سخت‌افزاری نوینی همچون ماهواره‌ها و شبکه‌های بی‌سیم لزوم حساسیت در مورد حفظ محرمانگی اطلاعات را بیش از پیش مشخص می‌کند؛ چرا که در این فناوری‌های نوین، داده‌ها به صورت آزاد در فضای مشخصی پخش شده و هر شنونده‌ای با تجهیزات نه چندان حرفه‌ای قادر به دریافت داده‌ها هستند. بهترین و ساده‌ترین روش محرمانه کردن اطلاعات، استفاده از روش‌های مختلف رمزنگاری داده‌ها است. آن دسته از این روش‌ها که بر اساس تکنیک‌های کلید متقارنعمل می‌کنند، نیاز به ساختاری دارند که بتوان توسط آن در مورد کلید رمز تبادل اطلاعات از سوی طرفین به توافق رسید. اهمیت و نقش این مسأله در حالتی که برای هر نشست کلید مجزایی نیاز باشد، بیشتر به چشم می‌خورد.

در این فصل مسأله‌ی بررسی شده در این پایان‌نامه و هدف از آن شرح داده می‌شود.

[1] cryptography

۱.۱ اصطلاحات

رمزنگاری[۱]: یک الگوریتم کارا (از لحاظ زمان و ترجیحا حافظه‌ی مصرفی) است که اطلاعات آشکار و با مفهوم را طی یک فرآیند بازگشت‌پذیر به اطلاعات نامفهوم و گنگ تبدیل می‌کند. در سامانه‌های کامپیوتری این عمل با به هم ریختن ترکیب بیت‌های اطلاعات انجام می‌شود.

کلید رمز[۲]: مقداری است که در فرآیند رمز کردن اطلاعات از آن استفاده شده و رمزگشایی اطلاعات بدون آن ممکن نیست. به همین دلیل امنیت یک فرآیند رمزنگاری به محرمانه ماندن کلید رمز استفاده شده وابسته است.

رمزنگاری کلید متقارن[۳]: آن دسته از روش‌های رمزنگاری هستند که کلید رمز کردن و رمزگشایی یکی بوده یا محاسبه‌ی آنها از روی هم بسیار آسان است. این روش‌ها را روش‌های کلید خصوصی[۴] نیز گویند.

رمزنگاری کلید نامتقارن[۵]: آن دسته از روش‌های رمزنگاری هستند که کلید رمز کردن و رمزگشایی متفاوت بوده و محاسبه‌ی آنها از روی هم بسیار سخت و زمان‌بَر است. این روش‌ها را روش‌های کلید عمومی[۶] نیز گویند.

تبادل کلید[۷]: به فرآیند مشخص شدن کلید رمز مورد استفاده برای رمزنگاری اطلاعات ارسالی بین دو کاربر با استفاده از روش‌های کلید متقارن گویند.

کلید نشست[۸]: کلید رمز روش‌های رمزنگاری متقارن است که تنها در یک جلسه‌ی ارتباطی استفاده شده و در هر ارتباط تغییر می‌کند.

---

[۱] cryptography
[۲] cipher key
[۳] symmetric-key cryptography
[۴] private key
[۵] asymmetric-key cryptography
[۶] public key
[۷] key exchange
[۸] session key

کلید طولانی‌مدت[۱]: کلیدی است که به صورت کاملا محرمانه نگهداری شده و هرگز از طریق کانال‌های ناامن (حتی به صورت رمز شده) منتقل نمی‌شوند. این نوع کلید ممکن است در تراکنش‌های مختلف بدون تغییر استفاده شود و نقش معرف مالک آن را داشته باشد.

حمله[۲]: هر گونه تلاش برای دسترسی غیرمجاز به اطلاعات رمز شده را گویند. این تلاش می‌تواند برای کشف کلید رمز، متن (حتی بخشی از آن) یا هر پارامتر محرمانه‌ی دیگر باشد.

پروتکل[۳]: به مجموعه قراردادهایی گفته می‌شود که بین طرفین ارتباط توافق می‌شود تا از یک جزئیات مشخص (مانند اندازه‌ی پارامترها، اندازه‌ی پیام‌ها) در تعاملات بین خود استفاده کنند. این قراردادها به منزله‌ی قوانینی هستند که اجرای آنها برای اجرای و اتمام درست عملیات اجباری است.

مسأله‌ی سخت[۴]: در این پایان‌نامه به مسائلی اشاره دارد که در رده‌ی NP-Complete قرار دارند.

۲.۱ بیان مسأله

تا کنون روش‌های بسیاری برای تبادل امن کلید معرفی شده‌اند. روش‌های اولیه‌ی تبادل کلید رمز، قدرت کافی برای تامین عامل‌های مختلف امنیتی را ندارند. در چنین روش‌هایی، مسائلی مانند احراز هویت طرف مقابل مد نظر نمی‌گیرد و مورد تهدید حمله‌ی مرد میانی[۵] قرار می‌گیرند. از سوی دیگر، پس از معرفی الگوریتم «شور[۶]» برای تجزیه‌ی اعداد با مرتبه‌ی زمانی قابل قبول توسط ماشین‌های کوانتومی[۷]، خطر شکست‌پذیری پروتکل‌های رایج مبتنی بر تجزیه‌ی اعداد و هر نوع مسأله‌ی کاهش‌پذیر به آن این سوال را پیش آورد که آیا امکان طراحی سامانه‌های مقاوم در برابر حملات کوانتومی با ساختارهای ریاضی و مسائل سخت دیگر وجود

[۱] long-term key
[۲] attack
[۳] protocol
[۴] hard problems
[۵] man in the middle attack
[۶] Shor
[۷] quantum computers

دارد؟ تلاش محققان برای پاسخگویی به این سوال باعث به وجود آمدن راهکارهای نویتی همانند سامانه‌های رمزنگاری مشبکه مبنا موسوم به سامانه‌های «پسا کوانتومی[۱]» شد.

مبنای تحقیقاتی این پایان‌نامه پاسخ به سه پرسش است:

۱. یک روش امن تبادل کلید باید شامل چه خصوصیاتی باشد؟

۲. روش‌های تبادل کلید کنونی تا چه میزان امن هستند؟

۳. آیا امکان ارائه‌ی روش تبادل کلید جدید و امن‌تر وجود دارد؟

۳.۱ اهداف

هدف از این پایان‌نامه بررسی امکان ارائه‌ی راهکار نوین تبادل امن کلید سه طرفه پسا کوانتومی با در نظر گرفتن اهم معیارهای امنیتی است. روش‌های تبادل کلید سه طرفه[۲] آن دسته از این روش‌ها هستند که با وارد کردن عامل سوم در فرآیند تبادل کلید، احراز هویت طرفین تبادل کننده‌ی کلید و مدیریت تبادل کلید بین انبوهی از کاربران یک شبکه را تسهیل می‌کنند.

۴.۱ نظریه

با توجه به موارد بحث شده در بخش ۲.۱، انتظار می‌رود بتوان راهکار نوینی برای تبادل امن کلید سه طرفه با در نظر گرفتن معایب روش‌های قبلی و همینطور رویکردهای جدید محاسباتی و سخت‌افزاری ارائه داد. در این راه می‌توان از روش‌های رمزنگاری پسا کوانتومی مانند گروه‌های مشبکه نیز استفاده کرد و راهکاری ارائه داد که ضمن کارا بودن از لحاظ محاسباتی، امنیت بیشتری نیز فراهم آورد.

[۱] post-quantum

[۲] 3-party key exchange protocols

۵.۱ سازمان گزارش

پایان‌نامه از چهار فصل تشکیل یافته است. فصل دوم شامل پیشینه‌های پژوهشی مورد نظر برای ورود به توضیحات راهکار پیشنهادی است. در این فصل ابتدا مرور کوتاهی بر مفاهیم اولیه رمزنگاری و ریاضیات آنها صورت می‌گیرد. مفاهیم رمزنگاری شامل انواع روش‌های رمزنگاری و روش‌های حمله، و مفاهیم ریاضی شامل مواردی مانند مفاهیم بخشپذیری، گروه‌ها، حلقه‌ها و فضاهای برداری است. بخش اعظم فصل دوم معرفی راهکاری پیشین برای تبادل امن کلید دو یا سه طرفه از ابتدا تا سال‌های اخیر است. این دسته روش‌ها به چهار دسته‌ی کلی تقسیم شده است. در انتهای فصل نیز جمع‌بندی نتایج حاصل از تحلیل راهکارها آمده است. فصل سوم معرفی راهکار پیشنهادی NTRU-3PAKE برای توافق کلید امن سه طرفه و تحلیل‌های کارآیی و امنیتی آن است. فصل چهارم نیز نتیجه‌گیری کلی مباحث ارائه شده در پایان‌نامه و بررسی موارد پژوهشی پیشنهادی برای کارهای آتی است.

فصل ۲

پیشینه‌ی پژوهشی

در این فصل ابتدا مفاهیم اولیه شامل مفاهیم ساختارهای رمزنگاری، تبادل کلید، حملات به سامانه‌های امنیتی و همینطور مفاهیم ریاضی معرفی شده و در ادامه چهار دسته از راهکاری موجود برای تبادل کلید مورد بررسی قرار می‌گیرند.

۱.۲ مفاهیم اولیه

فرآیند تامین امنیت اطلاعات شامل مراحل و بخش‌هایی است که هر کدام یکی از عامل‌های امنیتی سامانه را تضمین می‌کنند؛ به عنوان مثال می‌توان به موارد زیر اشاره کرد:

- **محرمانگی**[۱]: حفظ اطلاعات از دسترسی غیرمجاز
- **جامعیت**[۲]: حفظ اطلاعات از تحریف و تشخیص آن در صورت وقوع
- **دسترسی**[۳]: در دسترس بودن اطلاعات در هر زمان مورد نیاز
- **احراز هویت**[۴]: اطمینان از هویت طرف مقابل ارتباط
- **سطوح دسترسی**[۵]: بررسی امکان و اجازه‌ی دسترسی کاربر به اطلاعات درخواستی

[۱] confidentiality
[۲] integrity
[۳] availability
[۴] authentication
[۵] authorization

این ویژگی‌ها توسط حملاتی مانند استراق سمع[۱] (علیه محرمانگی)، تحریف[۲] (علیه جامعیت)، جعل[۳] (علیه احراز هویت) و وقفه[۴] (علیه دسترسی) در تهدید هستند. رمزنگاری اطلاعات دسترسی به اطلاعات مذکور تنها برای افراد مجاز مقدور باشد. تفکیک افراد مجاز از غیرمجاز به صرف استفاده از یک الگوریتم بسیار پیچیده برای در هم ریختن اطلاعات کافی نیست و باید از یک کلید رمز[۵] استفاده کرد. این کلید رمز در الگوریتم رمز کردن یا آشکار کردن رمز به عنوان یکی از پارامترها وارد شده و به ترتیبی در محاسبات اعمال می‌شود که با تغییر کلید رمز، خروجی متفاوتی تولید شود.

آگوست کرکهف[۶] در سال ۱۸۸۳ مقاله‌ای در مجله‌ی علوم نظامی فرانسه[۷] منتشر کرد و شش اصل را برای یک سیستم رمزنگاری موفق لازم دانست:

۱. سیستم رمزنگاری اگر نه از لحاظ نظری که در عمل باید غیر قابل شکست باشد.

۲. **سیستم رمزنگاری نباید هیچ نکته‌ی پنهان و محرمانه‌ای داشته باشد. تنها چیزی که سری نگه داشته می‌شود کلید رمز است.**

۳. کلید رمز باید به گونه‌ای انتخاب شود که اولا راحت بتوان آن را عوض کرد و ثانیا بتوان آن را به خاطر سپرد و نیاز به یادداشت کردن کلید رمز نباشد.

۴. متون رمز شده باید از طریق خطوط تلگراف قابل مخابره باشند.

۵. دستگاه رمزنگاری یا اسناد رمز شده باید توسط یک نفر قابل حمل باشد.

۶. سیستم رمزنگاری باید بدون نیاز به آموزش‌های خاص و انجام دستورالعمل‌های مفصل به آسانی قابل راه‌اندازی باشد.

---

[۱] interception

[۲] modification

[۳] fabrication

[۴] interruption

[۵] cipher key

[۶] Auguste Kerchoffs

[۷] Journal des sciences militaires