Technovations of Electrical Engineering in Green Energy System
TEEGES
Review Article (2024) 3(1):98-123

A Review of Signal Security Protocols Suitable for Power-Limited Hardware

Mohsen Mousavi[1], *PhD.*

[1] *Faculty of Applied Sciences, Malek-Ashtar University of Technology, Isfahan, Iran.*

Abstract:

Instant messengers have been popularized by users for private and business communication as an alternative to the cheap short message system in mobile phones with limited computing power. However, until recently, most mobile messaging applications did not protect the confidentiality or integrity of messages. Due to reports of communications being intercepted by intelligence services such as the NSA, people have been motivated to look for alternative messengers to maintain the security and privacy of their communications on the Internet. Initially, with Facebook's purchase of the popular messaging app WhatsApp, other apps claiming to offer secure communications gained significant new users. One messaging app that claims to offer secure instant messaging features and has garnered a lot of attention is TextSecure Messenger. Next, Signal Messenger, which is considered the successor of TextSecure, uses the protocols available in this messenger to exchange text messages. Considering that the WhatsApp messenger is based on the signal protocol, in this article a complete description of the encryption complexity of the signal protocol is presented. In the following, a security analysis of the three main components of this protocol including: key exchange, key extraction and authentication in encrypted messages is described. It has also been shown that the process of sending and displaying messages in this protocol can achieve most of the security goals. Finally, the role of quantum attacks that resulted from the computing power of quantum computers in solving classical asymmetric cryptography problems in the security of the key agreement protocol used in the Signal was checked. It is also shown that the use of Post-Quantum key exchange cryptographic protocols can secure the key agreement part of the Signal protocol against attacks by quantum algorithms.

Keywords: Security protocols, Instant messengers, Signal protocol, Key agreement protocols, Post-Quantum cryptography.

Received: 24 October 2023
Revised: 16 December 2023
Accepted: 18 January 2024
Corresponding Author: Dr. Sayed Mohsen Mousavi, m.mousavi@mut-es.ac.ir
DOI: http://dx.doi.org/10.30486/teeges.2024.2004141.1121

مروری بر پروتکل امنیتی سیگنال مناسب برای سخت‌افزارهای توان محدود

فناوری‌های نوین مهندسی برق در سیستم انرژی سبز

TEEGES

مقاله مروری

مروری بر پروتکل امنیتی سیگنال مناسب برای سخت‌افزارهای توان محدود

سید محسن موسوی[1]، دکتری.

۱- مجتمع علوم کاربردی، دانشگاه صنعتی مالک اشتر، اصفهان، ایران

چکیده: پیام‌رسان‌های فوری به‌عنوان جایگزینی برای سیستم پیام کوتاه ارزان‌قیمت در دستگاه‌های تلفن همراه با توان محدود محاسباتی، توسط کاربران جهت ارتباطات خصوصی و تجاری، محبوبیت پیدا نموده است. بااین‌حال تا همین اواخر، اکثر برنامه‌های پیام‌رسان تلفن همراه، از محرمانه بودن یا یکپارچگی پیام‌ها محافظت نمی‌کردند. با توجه به گزارش‌هایی در مورد شنود ارتباطات توسط سرویس‌های اطلاعاتی مانند NSA، این انگیزه در مردم به وجود آمد که به دنبال پیام‌رسان‌های جایگزینی برای حفظ امنیت و حریم خصوصی ارتباطات خود در اینترنت باشند. در ابتدا با خرید برنامه کاربردی پیام‌رسان واتس‌آپ توسط فیس‌بوک که بسیار نیز بین کاربران محبوب بود، برنامه‌های کاربردی دیگری که ادعا می‌کردند ارتباطات ایمن را ارائه می‌دهند کاربران جدید قابل‌توجهی را به دست آوردند. یکی از برنامه‌های پیام‌رسانی که ادعا می‌کند ویژگی پیام‌های فوری ایمن را ارائه می‌دهد و توجه زیادی را نیز به خود جلب کرده است پیام‌رسان TextSecure است. در ادامه پیام‌رسان سیگنال که جانشین TextSecure محسوب می‌شود از پروتکل‌های موجود در این پیام‌رسان برای تبادل پیام‌های متنی استفاده نمود. با توجه به اینکه پیام‌رسان واتس‌آپ بر اساس پروتکل سیگنال است در این مقاله شرح کاملی از پیچیدگی رمزنگاری پروتکل سیگنال ارائه می‌شود. در ادامه یک تجزیه‌وتحلیل امنیتی از سه جزء اصلی این پروتکل شامل: تبادل کلید، استخراج کلید و احراز هویت در پیام‌های رمز شده، شرح داده می‌شود. همچنین نشان داده‌شده که فرایند ارسال و نمایش پیام در این پروتکل می‌تواند به اکثر اهداف امنیتی دست یابد. در پایان نیز، نقش حملات کوانتومی که ناشی از قدرت محاسباتی کامپیوترهای کوانتومی در حل مسائل رمزنگاری نامتقارن کلاسیک بوده را در امنیت پروتکل توافق کلید استفاده‌شده در سیگنال، بررسی می‌گردد. همچنین نشان داده می‌شود که استفاده از پروتکل‌های رمزنگاری تبادل کلید پساکوانتومی می‌تواند بخش توافق کلید پروتکل سیگنال را در برابر حملات الگوریتم‌های کوانتومی ایمن سازد.

واژه‌های کلیدی: پروتکل‌های امنیتی، پیام‌رسان‌های فوری، پروتکل سیگنال، پروتکل‌های توافق کلید، رمزنگاری پساکوانتومی.

تاریخ ارسال مقاله: ۱۴۰۲/۰۸/۰۲

تاریخ بازنگری مقاله: ۱۴۰۲/۰۹/۲۵

تاریخ پذیرش مقاله: ۱۴۰۲/۱۰/۲۸

نویسنده‌ی مسئول: دکتر سید محسن موسوی، m.mousavi@mut-es.ac.ir

DOI: http://dx.doi.org/10.30486/teeges.2024.2004141.1121

۱- مقدمه

در سال‌های اخیر، تمایل به استفاده از برنامه‌های کاربردی موبایلی برای استفاده در زمینه ارتباطات، رشد قابل‌توجهی داشته و به روشی استاندارد و پرکاربرد برای برقراری ارتباط تبدیل‌شده است. در ابتدا برنامه‌های پیام‌رسان جدیدی معرفی شدند و سعی داشتند تا جایگزین مناسبی برای سیستم پیامکی سنتی باشند اما دو مؤلفه امنیت و حفظ حریم خصوصی برای توسعه‌دهندگان این برنامه‌های پیام‌رسان جدید، جدی گرفته نشد. این پیام‌رسان‌های جدید که در سال‌های اخیر استفاده‌شده، از رمزنگاری سرتاسری[۱] پشتیبانی نمی‌کند و فقط ارتباط بین کاربر و سرور رمزگذاری می‌شود و این امر باعث می‌شود که ارائه‌دهندگان خدمات، دسترسی بیش‌ازحد لازمی به اطلاعات خصوصی کاربران داشته باشند [۱].

زمانی که ادوارد اسنودن[۲]، گزارش‌های محرمانه‌ای را در مورد NSA منتشر نمود، کاربران متوجه این مشکل اپراتورها شدند که نظارت گسترده‌ای[۳] بر روی ارتباطات بین کاربران وجود دارد و به همین دلیل، پیام‌رسان‌های امن تلفن همراه از اهمیت و محبوبیت بیشتری برخوردار شدند. به دلیل ظهور تلفن‌های هوشمند و برنامه‌هایی که همیشه برخط هستند پیام‌رسان‌های فوری[۴] که ارتباط ناهمگام[۵] را ارائه نمی‌دهند، به مشکل تبدیل شدند. پروتکل‌های پیام‌رسان ایمن مانند OTR که از پیام‌رسانی ناهمگام پشتیبانی نمی‌کند، این انگیزه را به سایر محققان و توسعه‌دهندگان نرم‌افزارهای پیام‌رسان داد که پروتکل‌های جدیدی را برای ارتباط ناهمگام در نظر داشته باشند. پس از افشاگری‌های اسنودن، برنامه‌های پیام‌رسان ایمن جدیدی مانند سیگنال که از پروتکلی با همین اسم استفاده می‌کند، معرفی شدند. بعد از معرفی پروتکل سیگنال، این پروتکل به دلیل قابلیت پیام‌رسانی ایمن در بین توسعه‌دهندگان و محققان کاملاً محبوب شد و سپس در سایر برنامه‌های کاربردی که فقط از رمزگذاری سرور-مشتری پشتیبانی می‌کنند، مورداستفاده قرار گرفت [۳-۲].

نکته اساسی درباره این موضوع این است که باید توجه داشت ارائه یک تجربه کاربری خوب به کاربران برنامه‌های پیام‌رسان باید به همراه درک آسان ویژگی‌های قابل‌استفاده این پیام‌رسان‌های ایمن نیز باشد. ازیک‌طرف، تجربه کار با پیام‌رسان برای هر برنامه کاربردی بسیار ضروری است و این موضوع درواقع کاربران جدید را به سمت خود جذب می‌کند اما از طرف دیگر جنبه‌های کاربردپذیری از پیام‌رسان، قسمت اساسی برنامه‌ها بوده که ممکن است جنبه‌های امنیتی را نیز تحت‌الشعاع قرار دهد. اگر توسعه‌دهندگان پیام‌رسان‌ها، مؤلفه امنیت را جدی نگیرند آنگاه کاربران نهایی[۶] در معرض خطر قرار می‌گیرند زیرا ممکن است مکالمات آن‌ها موردحمله قرار بگیرد و یا اینکه دشمنان با استفاده از جعل هویت[۷]، به مکالمات دسترسی پیدا کنند [۴].

استفاده نمودن از برنامه‌های پیام‌رسان جدید ایمن استفاده‌شده در تلفن همراه، توسط کاربران نهایی آسان است. درواقع، هر کاربر برای ایجاد یک حساب به یک شماره تلفن احتیاج دارد و این در حالی است که برنامه پیام‌رسان، کلیدهای رمزنگاری مورداستفاده را در پس‌زمینه تولید و مبادله می‌کند بدون اینکه کاربر مجبور به انجام تعامل باشد. نکته قابل‌توجه این است که کاربران هرگز از کلیدهای رمزنگاری مختلفی که در حال استفاده هستند مطلع نیستند و این موضوع برای کاربر عام[۸] مفید است زیرا بدون نیاز داشتن به دانش پیش‌زمینه نحوه کار و تبادل کلیدها، عملیات رمزنگاری سرتاسری انجام می‌شود [۵].

پیام‌رسان‌های فوری دارای ویژگی‌های متفاوتی هستند اما مهم‌ترین ویژگی آن‌ها این است که به شرطی پیام‌ها در زمان واقعی تحویل داده می‌شوند که هر دو طرف برخط باشند. بااین‌حال، برخلاف مکانیسم‌های امنیتی موجود برای ایمیل مانند ویژگی‌های PGP و S/MIME، پیام‌های فوری بدون محافظت ارسال می‌شوند. در ابتدای معرفی پیام‌رسان‌های فوری، بسیاری از نرم‌افزارهای معرفی‌شده مانند MSN MESSENGER و یا YAHOO MESSENGER هیچ مکانیزه امنیتی در تبادل ارتباط‌هایشان بکار نمی‌بردند. پیام‌رسان AOL بعداً یک مکانیسم حفاظتی شبیه به S/MIME را به سرویس IM خود اضافه نمود اما پیام‌رسان SECUREIM Trillian بدون ارائه هیچ‌گونه احراز هویت، داده‌ها را رمزگذاری می‌نمود [۷-۶].

یکی از کاربردهای مهم انرژی‌های تجدید ناپذیر، استفاده در دستگاه‌های با توان محدود محاسباتی است. در طراحی دستگاه‌های توان محدود، نقش رمزنگاری سبک‌وزن از اهمیت ویژه‌ای برخوردار است. در بین مسائل مهم رمزنگاری سبک‌وزن، طراحی پروتکل‌های امنیتی مناسب با سخت‌افزارهای با توان محدود محاسباتی، از تحقیقات به‌روز و چالشی بوده و هست. در این پژوهش، یکی از پروتکل‌های امنیتی بنام پروتکل سیگنال را معرفی و تحلیل نموده که در دسته پروتکل‌های رمزنگاری سبک‌وزن قرار داشته و مناسب برای دستگاه‌های با توان محدود محاسباتی است [۸].

۱-۱- پیش‌زمینه

در طول چند سال گذشته، نیاز به پروتکل‌های پیام‌رسانی ایمن جدی شده است. مردم به‌عنوان کاربران عادی، بیشتر از کاربران دیگر در معرض پیامدهای امنیتی هستند و این موضوع نظارت گسترده نباید موضوعی ساده برای آن‌ها تلقی شود. به‌طور مشخص، ادوارد اسنودن این موضوع را در سراسر جهان حساس و تشدید نموده که به دلیل نظارت گسترده‌ای که چندین کشور و در طول چند دهه انجام داده‌اند، حریم شخصی ما دیگر خصوصی نیست.

برای نشان دادن عمق ماجرای نظارت گسترده سازمان‌ها بر روی ارتباطات، فقط کافی است بر روی اطلاعات منتشرشده در سه‌ماهه اول سال ۲۰۱۷ متمرکز شویم زمانی که ویکی لیکس[۹] اسناد مهمی را در مورد آژانس اطلاعات مرکزی ایالات‌متحده (سیا)[۱۰] افشا[۱۱] نمود. این افشا و نشت اطلاعات بانام تجاری Vault 7 توسط ویکی لیکس منتشر شد که یکی از بزرگ‌ترین رخداده‌ای مربوط به انتشار اسناد محرمانه در مورد آژانس است [۹]. در این اسناد اطلاعاتی در مورد چگونگی دسترسی به تلفن همراه و یا رایانه شخصی افراد بدون اطلاع آن‌ها آورده شده است. درواقع این گزارش نشان می‌دهد که چگونه CIA بدون اطلاع کاربران، این حجم از نظارت گسترده[۱۲] را انجام می‌داد.

پس از افشای اطلاعات توسط اسنودن، استارت آپ‌هایی که مربوط به رمزنگاری و حریم خصوصی کاربران می‌شد افزایش یافت. چندین شرکت، پیاده‌سازی پروتکل‌ها و برنامه‌های پیام‌رسان ایمن را برای مقابله با نظارت گسترده معرفی نمودند. این برنامه‌های معرفی‌شده شامل ارائه یک سیستم پیام کوتاه رمزگذاری شده سرتاسری بود که هیچ اطلاعاتی در مورد محتوای پیام کاربر برای سایر افراد افشا نمی‌شد. بااینکه به این نوع از برنامه‌های پیام‌رسان و پروتکل‌ها نیاز است اما مشکل این برنامه‌ها که شامل جدیدترین پیشرفت در الگوریتم‌های[۱۳] رمزنگاری هستند، موضوع تصویب آن است. درواقع، فناوری‌های Bleeding-Edge دسته‌ای از فناوری به‌قدری جدید است که می‌تواند خطر غیرقابل‌اعتماد بودن زیادی داشته باشد. پس از مدتی، شرکت‌هایی مانند Google، Facebook و Open Whisper Systems با یکدیگر مشارکت نموده و این پروتکل‌های جدید را در برنامه‌های گسترده‌ای مانند WhatsApp که بیش از یک میلیارد کاربر فعال ماهانه دارد پیاده‌سازی نمودند [۱۰].

تا سال ۲۰۱۷ برنامه‌های پیام‌رسان ایمن جدیدی معرفی شدند که این برنامه‌ها قادر هستند تا رمزگذاری سرتاسری را بر روی مکالمات و پیام‌های تلفن همراه انجام دهند؛ اما نکته منفی در مورد این برنامه‌ها این است که آن‌ها اغلب جنبه‌های کاربردی را فدای امنیت می‌کنند. شاید در نگاه اول این مسئله ازنظر امنیتی چیز خوبی به نظر برسد اما به نظر می‌رسد این امکان وجود داشته باشد که به هر دو خواسته خود شامل امنیت و جنبه‌های کاربردی، دست پیدا کنیم. نکته مهم در مورد برنامه‌های پیام‌رسان ایمن جدید این است که این برنامه‌ها باید اطلاعات کافی را در اختیار کاربران قرار دهند تا زمانی که مکالمات آن‌ها رمزگذاری نیست کاربران آگاه شوند. درواقع این امکان وجود دارد که سرور، خدمات فنی لازم برای رمزگذاری داده را از دسترس خارج کند و پیام‌رسان‌ها به‌طور خودکار به‌جای رمزگذاری سرتاسری داده، فقط داده‌ها را انتقال دهد؛ بنابراین لازم است که کاربر از وضعیت رمزگذاری داده در هرلحظه آگاه باشد.

نکته مهمی که باید به آن توجه داشت این است که از وضعیت تکامل پروتکل‌های پیام‌رسان ایمن در طول تحقیقات محققان برای پیاده‌سازی این دسته از پروتکل‌های رمزنگاری سرتاسری، آگاه شویم. در [۱۱] یک تحلیل کاملی از پروتکل‌های امن مختلف انجام‌شده است اما از آن زمان تاکنون پروتکل‌ها تکامل‌یافته‌تر شده و ویژگی‌های امنیتی جدیدی در پیاده‌سازی آن‌ها استفاده‌شده است.

۲-۱- بیان مسئله

کاربرد فناوری رمزگذاری سرتاسری استفاده‌شده در پروتکل‌ها و پیاده‌سازی پیام‌رسان‌ها، اخیراً در پروتکل‌های موجود گسترش‌یافته و همچنین نبود منابع اطلاعاتی مناسب برای درک این حوزه از رمزنگاری باعث شد در این تحقیق به دنبال پاسخ به چالش زیر باشیم:

- یک مطالعه دقیق و درعین‌حال قابل‌فهم از رویکردهای مربوط به فناوری رمزگذاری سرتاسری استفاده‌شده در پیام‌رسان‌ها، با تمرکز بر پروتکل امنیتی بنام پروتکل سیگنال که در بیشتر برنامه‌های کاربردی موجود اجرا می‌شود.

پروتکل سیگنال یکی از پرکاربردترین فناوری رمزنگاری سرتاسری در برنامه‌های کاربردی پیام‌رسانی بوده که در حال حاضر برای تلفن‌های هوشمند و رایانه‌های رومیزی موجود است. به همین دلیل، تمرکز بر روی پروتکل سیگنال از اهمیت بالایی برخوردار است. همچنین پروتکل سیگنال از فنّاوری پیشرفته در رمزگذاری و ایجاد کلید استفاده می‌کند. به دلیل اینکه پروتکل سیگنال، توسعه داده شده پروتکل

TextSecure است در ابتدا یک مرور کوتاه بر پروتکل TextSecure انجام‌گرفته و در ادامه به‌صورت مختصر ساختار پروتکل سیگنال شرح داده می‌شود.

۱-۲-۱- مروری کوتاه بر پروتکل TextSecure

این برنامه توسط گروه Open Whisper Systems توسعه‌یافته و ادعای این برنامه کاربردی این است که از امنیت سرتاسری پیام‌های متنی، پشتیبانی می‌کند. در ابتدا بیشتر تحقیقات متمرکز بر ارتباطات رمزگذاری شده سرویس پیام کوتاه (SMS) بود اما Open Whisper Systemsدر فوریه ۲۰۱۴ پیام‌رسانی مبتنی بر کانال داده را معرفی کرد. بعدازآنکه واتس‌آپ توسط فیس‌بوک خریداری شد برنامه کاربردی TextSecure در بین کاربرانی که به شرایط حریم خصوصی آگاهی دارند بسیار محبوبیت پیدا کرد به‌طوری‌که در حال حاضر این برنامه کاربردی بیش از پانصد هزار بار از طریق گوگل پلی نصب‌شده است. یکی از سیستم‌عامل‌های محبوب اندرویدی منبع باز، برنامه کاربردی CyanogenMod است که در حدود ده میلیون دستگاه اندرویدی نصب‌شده است. قابل‌توجه است که پروتکل پیام‌رسانی رمزگذاری شده TextSecure در سیستم پیامکی CyanogenMod نیز بکار برده شده است. همچنین پروتکل TextSecure در سرویس مشتری واتس‌آپ اندرویدی نیز اجراشده است [۱۲].

باوجودی که پروتکل پیام‌رسانی TextSecure بسیار محبوب بوده اما تاکنون ادعاهای امنیتی طراحان آن به‌دقت بررسی نشده است و این در حالی است که موضوع امنیت این پروتکل می‌تواند بر امنیت صدها میلیون کاربر تأثیر داشته باشد زیرا همان‌طور که گفته شد TextSecureپایه و اساس برخی پروتکل‌های مهم مانند سیگنال بوده و برنامه کاربردی واتس‌آپ بر اساس پروتکل سیگنال طراحی‌شده است. درواقع، باوجودآنکه توسعه‌دهندگان TextSecure سابقه طولانی تحقیقاتی در زمینه امنیت رایانه دارند اما برای بررسی دقیق عملکرد این پروتکل پیام‌رسانی به یک ارزیابی امنیتی جامع نیاز است [۱۲].

در ابتدا TextSecure با پروتکل‌های OTR و SCIMP[۱۴] مقایسه شده بود. پروتکل OTR توسط بوریسوف به‌عنوان روشی برای ایمن‌سازی پیام‌های فوری متداول پیشنهاد شد. پروتکل OTR دو ویژگی بدیع محرمانگی پیشرو و انکارناپذیری را معرفی نمود که این امر باعث شد به‌طور اساسی متفاوت از مکانیسم‌های prKGotection پیام مانند OpenPGP و S/MIME شود. در ادامه نسخه ابتدایی از پروتکل OTR را شرح می‌دهیم که پایه و اساس پروتکل TextSecure است [۱۲].

در ابتدا آلیس عدد تصادفی x_0 را انتخاب نموده و مقادیر $X_0 = g^{x_0}$ و $\sigma_A = sign(sk_A, X_0)$ را محاسبه می‌کند و در ادامه X_0 و σ_A را برای آلیس می‌فرستد. در گام دوم، باب عدد تصادفی y_0 را انتخاب نموده و سپس همانند آلیس مقادیر $Y_0 = g^{y_0}$ و $\sigma_B = sign(sk_B, Y_0)$ را محاسبه نموده و مقادیر Y_0 و σ_B را برای آلیس پس می‌فرستد. در گام سوم، آلیس عدد تصادفی x_1 را انتخاب نموده و مقادیر زیر را محاسبه می‌نماید:

$$X_1 = g^{x_1}, \quad k_{00}^e = H((Y_0)^{x_0}), \quad k_{00}^m = H(k_{00}^e), \quad c_{00} = Enc(k_{00}^e, m_{00}), \quad mac_{00} = MAC(k_{00}^m, (X_1, c_{00})). \quad (۱)$$

پس از محاسبه مقادیر (۱)، آلیس X_1، c_{00} و mac_{00} را برای باب می‌فرستد. در گام چهارم، باب عدد تصادفی y_1 را انتخاب نموده و همانند آلیس مقادیر زیر را به دست می‌آورد:

$$Y_1 = g^{y_1}, \quad k_{10}^e = H((X_1)^{y_0}), \quad k_{10}^m = H(k_{10}^e), \quad c_{10} = Enc(k_{10}^e, m_{10}), \quad mac_{10} = MAC(k_{10}^m, (Y_1, c_{10})). \quad (۲)$$

پس از محاسبه مقادیر (۲)، باب مقادیر Y_1، c_{10} و mac_{10} را برای آلیس پس می‌فرستد. در گام پنجم، آلیس عدد تصادفی x_2 را انتخاب نموده و سپس مقادیر زیر را محاسبه می‌نماید:

$$X_2 = g^{x_2}, \quad k_{11}^e = H((Y_1)^{x_1}), \quad k_{11}^m = H(k_{11}^e), \quad c_{11} = Enc(k_{11}^e, m_{11}), \quad mac_{11} = MAC(k_{11}^m, (X_2, c_{11})). \quad (۳)$$

پس از محاسبه مقادیر داده‌شده در رابطه (۳)، آلیس مقادیر X_2، c_{11}، mac_{11} و k_{00}^m را برای باب می‌فرستد و این فرایند به همین صورت تکرار می‌شود. درواقع، پس از امضای اولیه بر تبادل کلید دفی‌هلمن، این کلید جدید با هر پیام مبادله می‌شود به‌طوری‌که کلید دفی‌هلمن به‌دست‌آمده از آن، به‌طور مداوم تغییر می‌کند.

پروتکل OTR از رمزنگاری انعطاف‌پذیری[۱۵] استفاده می‌کند که در آن بجای استفاده از امضای دیجیتال از MAC ها استفاده‌شده است. ساختار پروتکل OTR به این صورت است که کلیدهای MAC را یک دور بعد برای عموم فاش می‌کند. این خاصیت جهت برقراری قابلیت انکارناپذیری در پروتکل، ضروری است. هرکسی می‌تواند مقدار پیام متن اصلی را تغییر دهد زیرا معکوس شدن بیت‌های پیام رمز شده باعث وارونه شدن بیت‌های مشابه در موقعیت‌های مشابه در متن اصلی می‌شود؛ بنابراین، پیام‌های دریافتی فقط در زمان دریافت آن‌ها

معتبر هستند (درصورتی‌که دو طرف اولین امضا و MAC های بعدی را تائید می‌کنند). ازآنجایی‌که کلیدهای MAC به‌عنوان مقادیر چکیده ساز از کلیدهای رمزنگاری به‌دست‌آمده‌اند، فاش شدن کلیدهای MAC امنیت پیام‌های رمز شده قبلی را به خطر نمی‌اندازد و این امر باعث می‌شود که پیام‌های ردوبدل شده محرمانه باقی بمانند. سهم‌های دفی‌هلمن خصوصی x_i و y_j به‌محض آنکه کلید k_{ij} در حال محاسبه شدن بوده، حذف‌شده است. این محرمانگی پیش رو را تضمین می‌کند زیرا در ادامه بدون این سهم‌های خصوصی نمی‌توان کلیدهای رمزگذاری را از سهم‌های عمومی X_i و Y_j محاسبه نمود.

نشان داده‌شده که اولین نسخه از OTR در برابر حمله کلید مشترک ناشناخته، آسیب‌پذیر است. نسخه دوم از پروتکل OTR با معرفی تکنیکی به نام دست دادن چهار پیام[۱۶] که از پارادایم پروتکل سیگما[۱۷] پیروی می‌کند، این مشکل را برطرف نمود به‌طوری‌که به‌طور چشمگیری حمله کلید مشترک ناشناخته را کاهش داد و همچنین این پروتکل خاصیت انکارناپذیری را به دست می‌آورد. کلیدهای عمومی و امضا از طریق یک کانال محرمانه ردوبدل می‌شود و هیچ اثری جهت دسترسی برای یک شنود کننده باقی نمی‌ماند. بااین‌حال، این قابلیت‌های قوی به قیمت از دست دادن چهار پیام است.

ارتباطات پیام‌های فوری معمولاً کوتاه‌مدت و برخط هستند، درحالی‌که مکالمه پیام کوتاه ممکن است برای مدت‌زمان طولانی طول بکشد و شرکت‌کنندگان ممکن است به‌طور موقت آفلاین باشند. علاوه بر این، پیام‌های متنی ممکن است ناهم‌زمان باشند، به‌این‌ترتیب که یک فرستنده قبل از دریافت پاسخ، چندین پیام ارسال می‌کند. اولین تطبیقی که برای استخراج پروتکل پیام‌رسانی ایمن از OTR موردنیاز است، ایجاد OTR در سناریوهای آفلاین است. ایده اصلی برای انجام این کار با استفاده از روش الجمال انجام‌شده است؛ بنابراین OTR می‌تواند برای یک سناریو آفلاین با استفاده از روش ذخیره‌سازی تعدادی از سهم‌های دفی‌هلمن موقت[۱۸] از هر شرکت‌کننده و بر روی یک سرور، تطبیق داده شود.

تطبیق دوم مربوط به ثبت کلید است. در OTR یک سهم دفی‌هلمن موقت باید با استفاده از یک MAC که توسط کلید قبلی محاسبه‌شده، محافظت شود و نکته مهم اینکه این سهم باید قبل از استفاده توسط فرستنده A توسط گیرنده B تائید گردد. فرایند زنجیره نموده امن کلیدها از طریق MAC ها نیاز به ثبت‌های زیاد و همچنین تائید نیز نیاز دارد. پروتکل TEXTSECURE با جایگزین نمودن زنجیره MAC با یک مقدار مخفی که از کلید بلندمدت (g^a, g^b) و سهم‌های دفی‌هلمن موقت (g^{x_a}, g^{x_b}) به‌دست‌آمده و در مرحله تولید کلید نیز تغذیه‌شده، با سناریو سازگار می‌شود.

۲-۲-۱- شرح مختصری درباره ساختار پروتکل سیگنال

اگرچه پروتکل‌های متنوعی در حوزه پیام‌رسان‌های فوری با ویژگی رمزگذاری سرتاسری وجود دارند ولی برجسته‌ترین پروتکل در این حوزه پروتکل پیام‌رسان سیگنال می‌باشد. سیگنال یک پروتکل ضامن‌دار با ویژگی محرمانگی روبه‌جلو می‌باشد که برای تبادل پیام هم‌زمان و غیرهمزمان قابل‌استفاده است. پروتکل سیگنال ویژگی رمزگذاری سرتاسری و ویژگی‌های امنیتی پیشرفته مانند محرمانگی روبه‌جلو کامل و محرمانگی پیش‌رو را فراهم می‌کند. این پروتکل را می‌توان به مراحل زیر تقسیم نمود:

پروتکل تبادل کلید آغازین یا X3DH: این پروتکل کلیدهای دفی‌هلمن موقّت، میان‌مدت و بلندمدت را باهم ترکیب می‌کند و یک مقدار محرمانه تحت عنوان کلید ریشه تولید می‌کند.

مرحله نامتقارن ضامن‌دار[۱۹]: در این مرحله کاربران کلیدهای دفی‌هلمن موقّت جدیدی را تولید و با روش پینگ‌پنگی (پرسش و پاسخ) به یکدیگر ارسال می‌کنند. سپس با استفاده از کلید ریشه قبلی، کلیدهای زنجیره جدید با ویژگی محرمانگی روبه‌جلو تولید می‌کنند.

مرحله متقارن ضامن‌دار[۲۰]: در این مرحله کاربران کلیدهای دفی‌هلمن جدیدی تولید نمی‌کنند بلکه با استفاده از توابع تولید کلید، کلیدهای زنجیره جدید تولید نموده و سپس با استفاده از آن‌ها، کلیدهای پیام جدیدی برای رمزگذاری و رمزگشایی پیام‌ها تولید می‌کنند.

در پروتکل سیگنال هر پیام ارسال‌شده توسط کاربر با استفاده از یک کلید پیام جدید رمزگذاری می‌شود و این سبب می‌شود که پروتکل ویژگی محرمانگی روبه‌جلو را در سطح بالایی فراهم کند. روش پرسش و پاسخ استفاده‌شده در تولید کلیدهای دفی‌هلمن موقّت باعث افزایش آنتروپی کلیدهای ریشه تولیدشده، می‌شود و این باعث می‌شود که پروتکل به‌صورت پیوسته ویژگی محرمانگی روبه‌جلو کامل و امنیت پسامصالحه[۲۱] را فراهم نماید. پروتکل سیگنال، به‌ویژه ساختار ضامن‌دار استفاده‌شده در آن، تاریخچه نسبتاً پیچیده‌ای دارد. پروتکل رمزنگاری سیگنال امروزه در ارتباطات شخصی بسیاری جهت رمزگذاری پیام‌ها مورداستفاده قرار می‌گیرد. برای مثال در نرم‌افزار واتساپ،

وایبر، پیام‌رسان فیس‌بوک و همچنین در مجموعه‌ای از نرم‌افزارهای پیام‌رسان امن مانند Silent Circle، پوند، Conversations و ChatSecure از پروتکل سیگنال استفاده می‌شود.

۳-۱- سابقه پژوهش‌های انجام‌شده

در مورد دو مؤلفه امنیت و کاربردپذیری در برنامه‌های کاربردی پیام‌رسان ایمن، تحقیقات زیادی انجام‌نشده است. در این چند سال اخیر، یکی از موضوعاتی که برای محققان از اهمیت زیادی برخوردار شده، اهمیت کاربردپذیری پیام‌رسان‌های امن و نه صرفاً مسائل فنی پیرامون پیام‌رسان‌ها است. اولین مقاله تحقیقاتی که به بررسی مباحث مربوط به کاربردپذیری پیام‌رسان‌های رمزگذاری شده سرتاسری پرداخته، مقاله انجام‌شده توسط شرودر[۲۲] [۱۳] است. در این تحقیق، یک مطالعه جامعی در مورد کاربردپذیری ویژگی‌های امنیتی سیگنال انجام‌شده است. همچنین در این تحقیق، راه‌حل‌هایی در مورد مشکلات احراز هویت کاربران و همچنین برخی از حملات مانند مردی در میان[۲۳]، آورده شده است. در مقاله [۱۱]، یک پژوهش نسبتاً کاملی بر روی پیام‌رسان‌های امن انجام‌شده است. این پژوهش با توجه به برخی مؤلفه‌ها شامل ایجاد اعتماد بین موجودیت‌ها، امنیت در مکالمه و همچنین مسئله حریم خصوصی، صورت گرفته است. بررسی نویسندگان در [۱۱] نشان داده که پروتکل‌های تخصصی در رمزگذاری قادر به تأمین امنیت و حریم خصوصی نیستند.

مجموعه‌ای از تحقیقات و مقالات درباره پروتکل سیگنال انجام‌شده است که در اینجا توضیح مختصری از آن‌ها ارائه می‌شود. در ابتدا، کُبیسی، بارگاوان و بلنچت[۲۴] با استفاده از ProVerif و CryptoVerif یک نمونه ساده از پروتکل سیگنال را تحت عنوان پروتکل ProScript در جاوا اسکریپت تحلیل و بررسی کرده‌اند. تمرکز آن‌ها بیشتر بر روی ارائه روشی برای تائید خودکار، تبادل پیام امن و پیاده‌سازی بوده است. همچنین آن‌ها نمونه ساده پروتکل سیگنال را در نظر گرفته‌اند [۱۴].

ادعاشده است که ضامن نامتقارن پروتکل سیگنال که ایده اصلی آن از طراحی پروتکل OTR گرفته‌شده است ویژگی‌های امنیتی ازجمله محرمانگی پیش‌رو را دارد. محرمانگی پیش‌رو پروتکل‌هایی مانند پروتکل سیگنال توسط گوردون، کرمرز و گارات[۲۵] مطالعه شده است. مشاهده اصلی آن‌ها این است که محرمانگی پیش‌رو پروتکل سیگنال نسبت به یک دشمن غیرفعال مشخص می‌شود و درنتیجه در صورت برقراری محرمانگی روبه‌جلو، ویژگی گفته‌شده برای پروتکل سیگنال برقرار خواهد بود. آن‌ها مشاهده کرده‌اند که از روش‌هایی مانند ضامن نامتقارن می‌توان جهت تأمین یک ویژگی امنیتی قوی در برابر یک دشمن فعال استفاده کرد. آن‌ها به‌صورت رسمی این ویژگی را امنیت پسامصالحه تعریف کرده‌اند و نشان داده‌اند چگونه این ویژگی احتمال موفقیت یک دشمن را که قصد حمله به یک جلسه را دارد کاهش می‌دهد. همچنین تحلیل آن‌ها نشان می‌دهد که امنیت پسامصالحه پروتکل سیگنال امکان دارد به جزئیات دیگری که مرتبط با تنظیم مجدد حالت دستگاه و اجرای چندین دستگاه به‌صورت هم‌زمان است بستگی داشته باشد [۱۵].

گرین و میرس[۲۶] با استفاده از رمزگذاری قابل‌تشخیص روشی برای به دست آوردن امنیت روبه‌جلو دقیق بدون تغییر دادن کلیدهای عمومی پیشنهاد داده‌اند. در روش آن‌ها به‌جای حذف کردن کلید خصوصی یک کاربر می‌توان آن را به نحوی تصحیح کرد که با استفاده از آن نمی‌توان پیام‌های خاصی را رمزگشایی نمود [۱۶].

بلیر[۲۷] و همکارانش تعاریف امنیتی کلی برای تبادل کلید ضامن‌دار در یک مفهوم متفاوت و نیز بر اساس یک مدل محاسباتی با تمایز ناپذیری کلید، ارائه کرده‌اند. آن‌ها یک پروتکل مبتنی بر دفی‌هلمن پیشنهاد داده‌اند که به دلیل استفاده از روش ضامن‌دار تا حدودی مشابه پروتکل سیگنال است. آن‌ها اثبات کرده‌اند که پروتکل پیشنهادشده در مدل امنیتی آن‌ها و تحت فرضیه دفی‌هلمن پیش‌گو، امن می‌باشد. همچنین نحوه ترکیب طرح‌های رمزگذاری متقارن با طرح‌های تبادل کلید ضامن‌دار را نشان داده‌اند. مدل آن‌ها محرمانگی روبه‌جلو و پس‌رو را تأمین می‌کند ولی فقط تبادل پیام یک‌طرفه بین آلیس و باب را پوشش می‌دهد بنابراین مفاهیم امنیتی ذکرشده فقط یک‌طرفه هستند: اگر کلید بلندمدت دریافت‌کننده فاش شود در این صورت امنیت پروتکل از بین خواهد رفت. علاوه بر این در پروتکل آن‌ها فقط نامتقارن ضامن‌دار را پوشش داده‌شده و متقارن ضامن‌دار در نظر گرفته نشده است [۱۷].

پوترینگ و روسلر[۲۸] ساختار ارائه‌شده توسط بلیر را توسعه داده‌اند و مدلی را ارائه کرده‌اند که به‌روزرسانی‌های دوطرفه را پوشش می‌دهد. آن‌ها یک مفهوم قوی از مصالحه را ارائه کرده‌اند و ساختارهایی را بیان کرده‌اند که در تعریف رمزگذاری مبتنی بر هویت سلسله‌مراتبی صدق می‌کند [۱۸].

سایر قسمت‌های مقاله به شرح زیر است. در بخش ۲، پیش‌نیازها و تعاریف امنیتی موردنیاز در طراحی پروتکل‌های امنیتی، شرح داده‌شده است. در فصل ۳، جزئیات پروتکل سیگنال، موردبررسی قرار می‌گیرد. همچنین در این فصل، اولین الگوریتمی که الگوریتم ضامن‌دار دابل

نامیده شده و ترکیبی از دفی‌هلمن و کلید متقارن ضامن‌دار است توصیف می‌شود. دومین الگوریتمی که X3DH نامیده می‌شود و برای توافق کلید بین موجودیت‌ها جهت رمز نمودن پیام‌های ارسالی مابین اعضای گفتگو استفاده می‌شود در این فصل بررسی می‌گردد. همچنین در فصل ۳، نقش حملات کوانتومی در امنیت پروتکل توافق کلید X3DH بررسی‌شده و اهمیت استفاده از رمزنگاری پساکوانتومی در بخش توافق کلید سیگنال شرح داده می‌شود. در پایان، نتیجه‌گیری مقاله در بخش ۴، آورده شده است.

۲- تعاریف امنیتی موردنیاز

ازآنجایی‌که عملیات رمزنگاری، داده‌ها را به یک سری اطلاعات نامفهوم تبدیل می‌کند، می‌توان از آن برای محرمانگی داده‌ها در حین عبور از یک کانال عمومی نظیر اینترنت بهره برد. اگرچه این روش از استراق سمع جلوگیری نمی‌کند ولی بااین‌حال استراق سمع کننده نمی‌تواند اطلاعاتی از محتوای پیام‌های ردوبدل شده به دست آورد. فرض کنید دو کاربر بخواهند اطلاعاتی را از طریق اینترنت به‌صورت امن ردوبدل نمایند. یکی از روش‌های مرسوم این است که با استفاده از پروتکل TLS، کاربر اول اطلاعات را رمزنگاری کرده و آن را به سرور ارسال نماید. در این حالت سرور پس از دریافت اطلاعات رمزنگاری‌شده، آن‌ها را ذخیره می‌نماید و پس از رمزگشایی آن‌ها و پردازش‌های لازم دوباره آن‌ها رمزنگاری کرده و برای کاربر مقصد ارسال می‌نماید. این روش اگرچه روشی امن برای ارسال داده‌ها محسوب می‌شود ولی اگر سرور موردحمله قرار گیرد اطلاعات محرمانه بین این دو کاربر افشا می‌گردد؛ و یا حالتی را در نظر بگیرید که این سرور خواسته و یا ناخواسته اطلاعات ردوبدل شده را در اختیار شخص ثالث دیگری قرار دهد. روش دیگری که برای ایجاد یک ارتباط محرمانه بین دو کاربر اتخاذ می‌گردد، استفاده از رمزنگاری سرتاسری است. در این حالت برنامه‌های کاربردی در طرفین ارتباط (دو کاربر نهایی) پیام‌ها را رمزنگاری و رمزگشایی می‌نمایند و سرور مابین آن‌ها فقط وظیفه انتقال پیام‌ها رمزنگاری‌شده را بر عهده‌دارند و هیچ‌گونه عملیات رمزگشایی در این سرور انجام نمی‌گیرد؛ بنابراین عملیات‌های رمزنگاری و رمزگشایی در سمت کاربرهای نهایی انجام می‌پذیرد و با این کار هیچ حمله‌کننده‌ای و یا سرور به مفهوم اطلاعات دست نمی‌یابد. در ادامه برخی اصطلاحات امنیتی مورد نیاز تعریف می‌شوند.

۲-۱- احراز اصالت[۲۹]

احراز اصالت را می‌توان در دو بخش بیان نمود. تشخیص اصالت افراد و تشخیص اصالت پیام. احراز اصالت افراد، درواقع تائید می‌کند که آیا طرفین ارتباط همان‌هایی هستند که ادعا می‌کنند. احراز اصالت پیام نیز این اطمینان را به طرفین ارتباط می‌دهد که پیام ردوبدل شده در حین حرکت از کانال عمومی دچار تغییر نشده است و همان پیام اصلی است که توسط فرستنده در مبدأ ارسال‌شده است. این کار توسط کدهای احراز اصالت پیام تضمین می‌گردد. کد احراز اصالت پیام در مبدأ و با استفاده پیام اصلی و یک کلید محرمانه توافق شده بین طرفین ارتباط، محاسبه می‌شود و این کد مبنای اطمینان از تمامیت پیام دریافتی در مقصد خواهد بود.

۲-۲- محرمانگی کامل پیشرو[۳۰]

ایده محرمانگی پیشرو این است که وقتی یک کلید طولانی‌مدت به خطر افتاد، کلیدهای جلساتی که قبلاً با استفاده از این کلید بلندمدت ایجادشده بودند، به خطر نیفتند. مثالی از پروتکل‌های که امنیت پیشرو را ارائه می‌دهد؛ پروتکل‌های توافق کلید هستند که کلید طولانی‌مدت را فقط برای احراز اصالت کردن در تبادل استفاده می‌نمایند. پروتکل‌های انتقال کلید که در آن از کلید طولانی‌مدت برای رمزگذاری کلید جلسه استفاده می‌کنند نمی‌توانند امنیت پیشرو را ارائه دهند؛ بنابراین یک پروتکل برقراری کلید، محرمانگی پیشرو را ارائه می‌دهد اگر کلیدهای طولانی‌مدت به خطر افتاده باعث به خطر افتادن کلیدهای برقرارشده قبلی در پروتکل نگردد.

۲-۳- انکارناپذیری[۳۱]

انکارناپذیری خاصیتی است که در پیام‌رسان‌های جدید مشترک است و بدین‌صورت است که دیگران قادر به تائید این‌که اطلاعات از یک شخص خاص است نیستند. به‌عبارت‌دیگر، اگر باب پیامی از آلیس دریافت کرد، می‌تواند مطمئن باشد که آلیس آن را ارسال کرده است، اما نمی‌تواند به شخص دیگری ثابت کند این آلیس است که آن را ارسال کرده است. پروتکل‌های پیام‌رسان امنی که از خاصیت انکارناپذیری پشتیبانی می‌کنند به کاربر خود این اطمینان را می‌دهند که در حین مکالمه، شرکت‌کنندگان کلماتی را که مشاهده می‌کنند

معتبر است و هیچ‌کس دیگری در آن اصلاحاتی را انجام نداده است و این در حالی است که بعد از اتمام مکالمه هرکسی می‌تواند پیام‌ها را طوری جعل نماید که این پیام‌ها از طرف او به نظر برسند.

۲-۴- هم‌زمانی[۳۲]

دو نوع ارتباط هم‌زمان و ناهم‌زمان وجود دارد و پروتکل‌های چت می‌تواند دارای یکی از این دو ارتباط باشند. پروتکل‌های همگام این شرط را دارند که همه شرکت‌کنندگان برای دریافت یا ارسال پیام باید برخط باشند. اگر یک پروتکل چت ناهم‌زمان باشد، به این معنی است که شرکت‌کنندگان برای دریافت پیام، ازجمله پیام کوتاه متنی یا ایمیل، نیازی به برخط بودن ندارند، زیرا در این حالت شخص ثالثی وجود دارد که اطلاعات را تا زمانی که گیرنده دوباره برخط شود ذخیره می‌کند. وقتی صحبت از پروتکل‌های چت امروزی می‌شود، استفاده از پروتکل‌های هم‌زمان توصیه نمی‌شود. دلیل این امر این است که محدودیت‌های فنی و اجتماعی مانند باتری دستگاه و محدود بودن افراد در برخط بودن دائمی برای دریافت پیام همیشه وجود دارد. به همین دلیل است که اکثر پیام‌رسان‌های فوری با در اختیار داشتن یک شخص ثالث پیام‌ها را ذخیره می‌کنند تا بعدازاینکه افراد برخط شدند بتواند پیام‌های یک گفتگو را دریافت نمایند و در حقیقت یک ارتباط ناهم‌زمان را ایجاد می‌نمایند.

۲-۵- محرمانگی[۳۳]

محرمانگی، این اطمینان را می‌دهد که در هر محلی که پردازش داده‌ها اعمال شود، سطح لازم برای رازداری وجود دارد و از افشای غیرمجاز اطلاعات در حین عبور از کانال عمومی جلوگیری می‌گردد. این مفهوم معمولاً با رمزنگاری داده‌های در سمت فرستنده و رمزگشایی آن در سمت گیرنده به دست می‌آید. در پروتکل‌های رمزنگاری، محرمانگی در مورد کلیدها و سایر اطلاعات جانبی ضروری است. حمله‌کنندگان، این فرصت را دارند که با سرقت پرونده‌های رمز عبور، شکستن برنامه‌های رمزگذاری یا مهندسی اجتماعی، مکانیسم محرمانگی را خراب کنند. از طرف دیگر، کاربران می‌توانند به‌صورت عمدی یا تصادفی اطلاعات حساس را با رمزگذاری نکردن آن قبل از ارسال آن به شخص دیگر و یا گرفتار شدن در تله‌های حمله مهندسی اجتماعی، افشا کنند؛ بنابراین، محرمانگی را می‌توان از طریق رمز نمودن داده‌ها در هنگام ذخیره‌سازی و انتقال، اعمال کنترل دقیق دسترسی‌ها و نیز با آموزش افراد در مورد روش‌های محافظت از داده‌ها ایجاد نمود.

۳- پروتکل سیگنال

هدف از طراحی پروتکل سیگنال، معرفی یک جایگزین مناسب بجای پروتکل OTR در برنامه‌های پیام‌رسان بوده است. پروتکل OTR یکی از اولین پروتکل‌های پیام‌رسانی فوری بود که برای رمزگذاری سرتاسری استفاده‌شده است. یکی از ویژگی‌های پروتکل OTR این بود که غالباً کلیدها را به‌روز می‌نمود. درواقع برای هر دور از ارسال و دریافت پیام، کاربران با استفاده از پروتکل دفی‌هلمن یک راز مشترک ایجاد می‌کردند. با این روش هر کاربر برای هر بار ارسال و دریافت پیام، یک راز مشترک جدید دریافت می‌کند و این عمل باعث می‌شود که رمزگشایی پیام‌های قبلی برای دیگران غیرممکن شود [۱۹].

پروتکل سیگنال توسط دو محقق[۳۴] Open Whisper Systems طراحی‌شده است. گروه Open Whisper Systems قصد داشت که یک استاندارد رمزنگاری سرتاسری جدید معرفی نموده به‌طوری‌که در هر دو محیط پیام‌رسانی هم‌زمان و غیر هم‌زمان کارایی داشته باشد [۲۰-۲۱]. سه هدف مهم پروتکل سیگنال شامل رمزگذاری سرتاسری و همچنین خصوصیات امنیتی پیشرفته‌ای مانند محرمانگی پیشرو[۳۵] و محرمانگی پس رو[۳۶] است [۱۹]. در ابتدا، سیگنال به دو برنامه TextSecure و برنامه RedPhone تقسیم‌شده بود. برنامه اول مربوط به پیام کوتاه و پیام‌رسانی فوری بود، درحالی‌که از برنامه دوم به‌عنوان یک برنامه VoIP رمزگذاری شده، استفاده می‌گردید. در ادامه، با ترکیب دو برنامه TextSecure و RedPhone پروتکل جدیدی به نام سیگنال تشکیل شد.

در سال‌های اخیر، پروتکل سیگنال توسط شرکت‌های بزرگ و مهمی مورداستفاده قرارگرفته است. برای مثال، فیس‌بوک از این پروتکل در پیام‌رسان واتس‌آپ و یا گوگل در طراحی پیام‌رسان Allo استفاده نموده است. در این بخش، اطلاعات بیشتری در مورد روش‌های مختلفی که سیگنال برای فراهم آوردن مشخصه رمزگذاری سرتاسری استفاده می‌کند، ارائه می‌شود. در بخش اول، الگوریتم ضامن‌دار دابل[۳۷] را شرح داده [۲۳-۲۲] و به‌طور خلاصه نحوه کار آن بیان می‌شود. در بخش دوم، روشی که سیگنال برای پیاده‌سازی توافق کلید

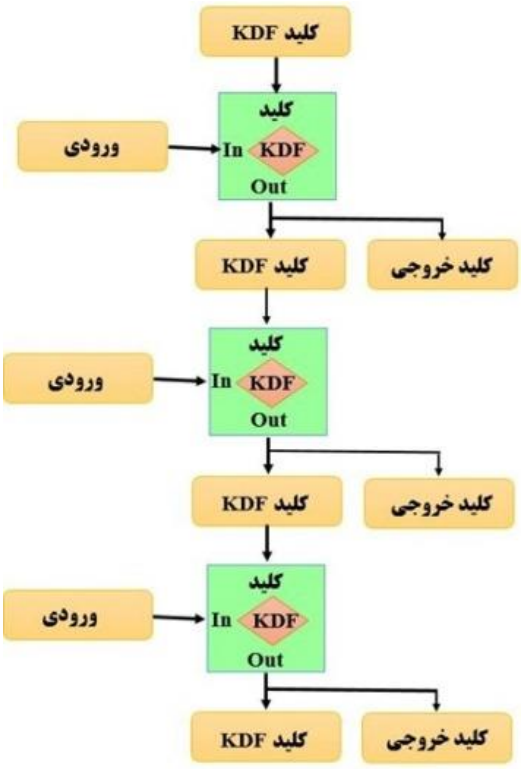
دفی‌هلمن[۳۸] استفاده می‌کند آورده شده که به آن دفی‌هلمن سه‌گانه توسعه‌یافته[۳۹] می‌گویند. در بخش سوم، درباره نقش حملات کوانتومی در امنیت پروتکل سیگنال بحث می‌شود.

۱-۳- الگوریتم ضامن‌دار دابل

در این بخش الگوریتم ضامن‌دار دابل با دقت شرح داده می‌شود. پروتکل سیگنال از الگوریتم ضامن‌دار دابل برای تبادل پیام‌های رمزگذاری شده استفاده می‌کند که در عملیات تبادل از یک کلید مخفی مشترک استفاده می‌شود که طرفین آن را توافق نموده‌اند. برای توافق بر روی کلید مخفی مشترک نیز، از برخی پروتکل‌های توافق کلید متداول، استفاده‌شده است. پروتکل سیگنال از پروتکل توافق کلید X3DH [۲۴] استفاده می‌کند که در قسمت بعدی، شرح داده می‌شود. الگوریتم ضامن‌دار دابل از مراحل مختلفی تشکیل‌شده است. اولین گام، زنجیره‌های تابع اشتقاق کلید[۴۰] [۲۲] است. دو مرحله بعدی متفاوت بوده که اولی کلیدمتقارن ضامن‌دار[۴۱] می‌باشد و دومی دفی‌هلمن ضامن‌دار[۴۲] است. از ترکیب این سه مرحله، الگوریتم ضامن‌دار دابل تشکیل می‌شود.

۱-۱-۳- زنجیره KDF

یکی از مفاهیم مهم و اصلی در الگوریتم ضامن‌دار دابل، مفهوم زنجیره KDF است [۲۲]. در این زنجیره، یک کلید KDF تصادفی و مخفی به همراه برخی داده‌های ورودی گرفته‌شده و سپس یک کلید به‌عنوان یک کلید KDF جدید برای زنجیره بعدی و همچنین یک کلید خروجی برای پیام‌ها، به‌عنوان خروجی به دست می‌آید. قابل‌توجه است که اگر کلید مشخص نباشد آنگاه داده‌های خروجی از رشته‌های تصادفی قابل‌تشخیص[۴۳] نیستند که این مسئله یکی از ویژگی‌های مربوط به اولیه‌های رمزنگاری بوده که داده رمز شده نباید از یک‌رشته تصادفی قابل‌تشخیص باشد. زنجیره KDF دارای خصوصیات مهم تاب‌آوری[۴۴]، امنیت پیشرو[۴۵] و امنیت پس‌رو[۴۶] است [۲۲]. وظیفه زنجیره KDF در طول نشست ضامن‌دار دابل[۴۷]، ذخیره کلیدهای KDF برای هر یک از شرکت‌کنندگان است که برای سه زنجیره ریشه[۴۸]، زنجیره ارسال[۴۹] و زنجیره دریافت[۵۰] کاربرد دارد. قابل‌توجه است که زنجیره ارسال آلیس با زنجیره دریافت باب مطابقت دارد و بالعکس که این مسئله در بخش ۳-۱-۳ بیشتر توضیح داده می‌شود. قابل‌ذکر است که در این زیر بخش، KDF با الگوریتم دفی‌هلمن ادغام‌شده است.



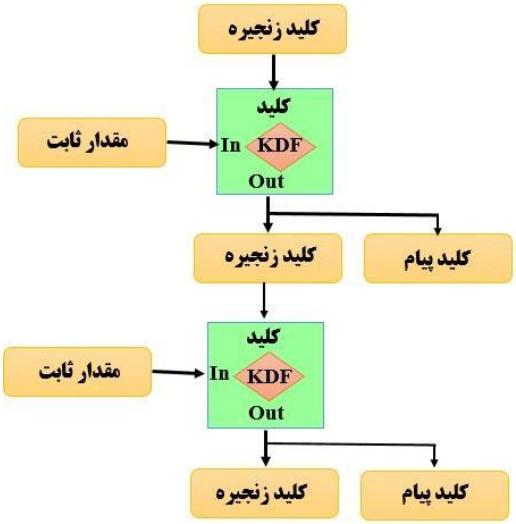
شکل (۱): زنجیره KDF بر روی سه ورودی پردازش انجام داده و سه خروجی تولید می‌کند.

زنجیره‌های KDF در هر دو بخش از مرحله دفی‌هلمن ضامن‌دار و مرحله کلیدمتقارن ضامن‌دار نقش دارد. درحالی‌که طرفین پیام‌های خود را ردوبدل می‌کنند آن‌ها باید کلیدهای عمومی دفی‌هلمن جدید را نیز ردوبدل نمایند. رازهایی که از خروجی دفی‌هلمن به دست می‌آیند به ورودی‌های زنجیره ریشه برای زنجیره KDF تبدیل‌شده و سپس کلیدهای خروجی از زنجیره ریشه به کلیدهای KDF جدید برای زنجیره‌های ارسال و دریافت تبدیل می‌شوند. به این فرایند، دفی‌هلمن ضامن‌دار گفته می‌شود [۲۲].

با استفاده از زنجیره‌ها به‌عنوان ورودی در KDF و همچنین کلیدهای خروجی برای رمزگذاری و رمزگشایی پیام‌ها، خروجی‌های دفی‌هلمن ضامن‌دار به‌دست‌آمده و زنجیره‌های ارسال و دریافت برای هر ارسال و دریافت پیام تولید می‌گردد. فرایند گفته‌شده در بالا، مرحله کلید متقارن ضامن‌دار نامیده می‌شود [۲۲].

۲-۱-۳- کلیدمتقارن ضامن‌دار

کلیدمتقارن ضامن‌دار از زنجیره‌های KDF برای زنجیره‌های ارسال و دریافت استفاده می‌کند. کلیدهای خروجی، آن دسته از کلیدهای پیام منحصربه‌فردی هستند که برای رمزگذاری یا رمزگشایی پیام‌ها استفاده می‌شوند. در ادامه شرح فرایند ضامن‌دار دابل، کلیدهای KDF برای زنجیره‌های کلیدمتقارن ضامن‌دار، کلیدهای زنجیره نامیده می‌شود [۲۲].



شکل (۲): فرایند انجام‌شده در دو گام کلیدمتقارن ضامن‌دار

زنجیره‌های KDF مورداستفاده برای زنجیره‌های ارسال و دریافت، ثابت هستند. آن‌ها نیازی به تصادفی یا مخفی بودن ندارند زیرا کلید زنجیره از زنجیره KDF دفی‌هلمن گرفته‌شده که ازلحاظ رمزنگاری ایمن است. در [۲۲] پیشنهادشده که مؤلفه ثابت برای کلید پیام می‌تواند 0x01 باشد و برای کلید زنجیره‌ای 0x02 در نظر گرفته شود. زنجیره‌های ارسال و دریافت اطمینان می‌دهند که هر پیام با یک کلید منحصربه‌فرد رمزگذاری یا رمزگشایی‌شده و پس از استفاده می‌تواند حذف شوند. برای محاسبه یک پیام جدید و کلید زنجیره‌ای از یک کلید زنجیره‌ای که قبلاً داده‌شده، فقط یک مرحله کلیدمتقارن ضامن‌دار وجود دارد. شکل (۲) دو مرحله از این فرایند را نشان می‌دهد. اولین KDF یک کلید زنجیره‌ای از زنجیره KDF دفی‌هلمن دریافت می‌کند و یک کلید زنجیره‌ای جدید برای KDF بعدی و یک کلید پیام برای رمزگذاری یا رمزگشایی پیام ارسال می‌نماید.

کلید پیامی که از زنجیره KDF مشتق شده است در ادامه برای استخراج کلیدهای پیام جدید یا کلیدهای زنجیره‌ای دیگری استفاده نمی‌شود. به همین دلیل، این امکان وجود دارد که ذخیره کلید پیام بدون نگرانی از تأثیر بر امنیت کلیدهای دیگر انجام شود. تنها استثنا مربوط به پیام‌هایی هستند که به کلیدهای پیام خاصی تعلق دارند. این‌یک مزیت به شمار می‌رود که پروتکل‌ها بتوانند پیام‌های خارج از نوبت یا سفارش[۵۱] را مدیریت کنند زیرا یک شرکت‌کننده می‌تواند کلید پیام را بدون نگرانی ذخیره نموده و در ادامه زمانی که پیام صحیحی برای آن کلید پیام دریافت می‌کند آن را رمزگشایی نماید. در مورد مبحث پیام‌های خارج از نوبت در بخش ۳-۱-۵ بیشتر توضیح داده می‌شود.

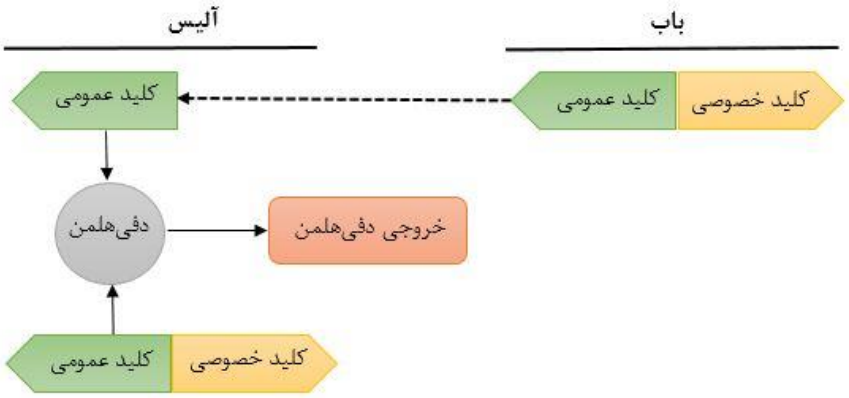
۳-۱-۳- دفی‌هلمن ضامن‌دار

ضامن‌دار دابل از ترکیب کلیدمتقارن ضامن‌دار و دفی‌هلمن ضامن‌دار تشکیل‌شده است. اگر در ضامن‌دار دابل از دفی‌هلمن ضامن‌دار برای محاسبه کلیدهای زنجیره‌ای جدید، برای ارسال و دریافت کلیدهای زنجیره‌ای، استفاده نشود آنگاه یک مهاجم می‌تواند با به دست آوردن یکی از کلیدهای زنجیره‌ای، قادر به محاسبه همه کلیدهای پیام در آینده باشد و بنابراین تمام پیام‌ها را در آینده رمزگشایی نماید [۲۲]. برای این کار هریک از طرفین یک جفت کلید دفی‌هلمن و یک کلید عمومی و یک کلید خصوصی را تولید نموده که اولین جفت کلید ضامن‌دار آن‌ها خواهد بود. هنگام ارسال پیام، هدر[۵۲] باید حاوی کلید عمومی فعلی باشد. گیرنده در هنگام دریافت پیام، کلیدهای عمومی که با آن پیام فرستاده‌شده است را بررسی نموده و یک مرحله دفی‌هلمن ضامن‌دار را انجام می‌دهد تا بتواند جفت کلید ضامن‌دار فعلی گیرنده را با یک کلید جدید جایگزین نماید [۲۲]. نتیجه این فرایند چیزی شبیه به بازی پینگ-پونگ[۵۳] است که دو طرف به‌نوبت در حال جایگزین نمودن جفت کلیدهای خود هستند. مهاجم برای دریافت هرگونه اطلاعات باارزش از طرفین، کار سختی را در پیش دارد. به عبارت دقیق‌تر، اگر یکی از پیام‌ها به خطر بیفتد[۵۴] و مهاجم از مقدار کلید خصوصی فعلی مطلع شود مشکلی ازنظر امنیت، برای پیام‌ها به وجود نمی‌آید زیرا کلید خصوصی به‌زودی با یک کلید جدید و سازش‌ناپذیر[۵۵] جایگزین خواهد شد [۲۲].

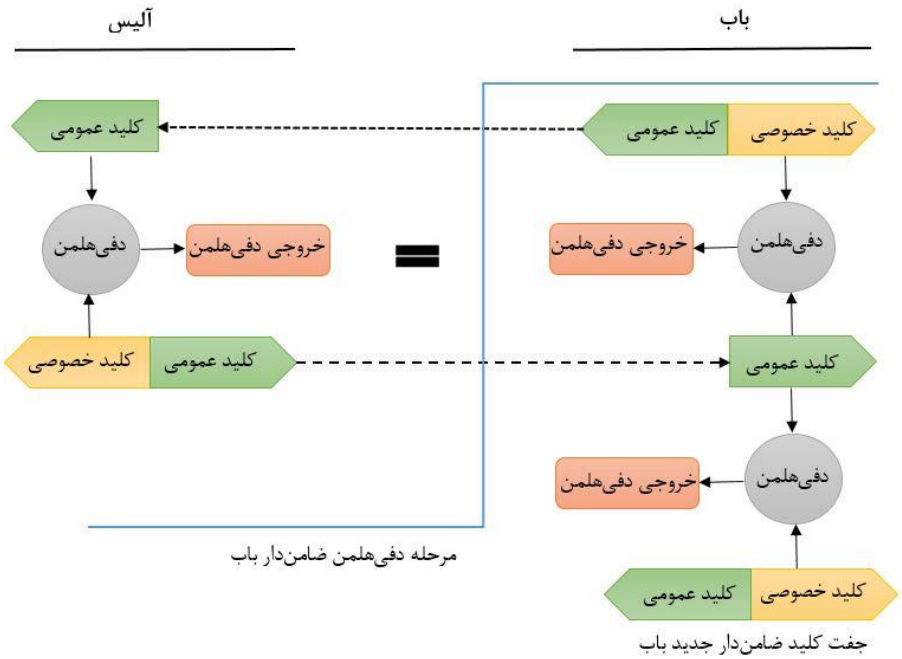
در ادامه یک نمونه از نحوه انجام دفی‌هلمن ضامن‌دار برای به دست آوردن یک دنباله مشترک از خروجی‌های دفی‌هلمن شرح داده می‌شود. برای شروع این فرایند، باب با ارسال کلید عمومی ضامن‌دار خود به آلیس، مقدمات اولیه را فراهم نموده و این در حالی است که باب کلید عمومی ضامن‌دار آلیس را نمی‌داند. اکنون آلیس مرحله آغازین این فرایند را با انجام محاسبه دفی‌هلمن بین کلید عمومی ضامن‌دار خودش و کلید عمومی ضامن‌دار باب به شکل زیر انجام می‌دهد.

شکل (۴) نشان می‌دهد که آلیس پس از پایان محاسبات دفی‌هلمن، کلید عمومی ضامن‌دار خود را برای اطلاع باب انتشار[۵۶] می‌دهد. وقتی باب پیام ابتدایی آلیس را دریافت می‌کند، با محاسبه خروجی دفی‌هلمن جدید بین کلید عمومی ضامن‌دار آلیس و کلید خصوصی ضامن‌دار خود که برابر با خروجی دفی‌هلمن آلیس است، یک مرحله ضامن‌دار دفی‌هلمن را انجام می‌دهد. خروجی‌های دفی‌هلمن برابر هستند زیرا این اعداد[۵۷] یک ساده‌سازی[۵۸] از دفی‌هلمن ضامن‌دار هستند. حال یک زنجیره KDF وجود دارد که از کلید ریشه (راز مشترک[۵۹] بین آلیس و باب) برای تولید کلیدهای مشابه استفاده نموده و در ادامه باب جفت کلید ضامن‌دار خود را جایگزین کرده و یک خروجی دفی‌هلمن جدید محاسبه می‌کند.

باب پیام بعدی خود را با کلید عمومی ضامن‌دار جدید ارسال می‌کند. سرانجام، آلیس پیام جدید باب را با کلید عمومی ضامن‌دار جدید خود دریافت می‌کند. آلیس با استفاده از کلید خصوصی ضامن‌دارش و همچنین کلید عمومی جدید باب یک خروجی دفی‌هلمن جدید تولید نموده تا با این عمل خروجی دفی‌هلمن همانند باب را به دست آورد و از آن برای رمزگشایی پیام استفاده نماید. در ادامه آلیس یک جفت کلید ضامن‌دار دفی‌هلمن جدید جهت جایگزین نمودن با جفت کلید قدیمی‌اش تولید می‌کند. حال با داشتن جفت کلید دفی‌هلمن ضامن‌دار جدید، آلیس با استفاده از کلید خصوصی ضامن‌دار جدیدش و همچنین آن کلید عمومی ضامن‌دار از باب که در تبادل پیام بعدی استفاده می‌شود، خروجی دفی‌هلمن دیگری به دست می‌آورد. این تبادلات برای هر پیام ارسال‌شده با استفاده از کلید عمومی ضامن‌دار و خروجی دفی‌هلمن جدید، ادامه می‌یابد.

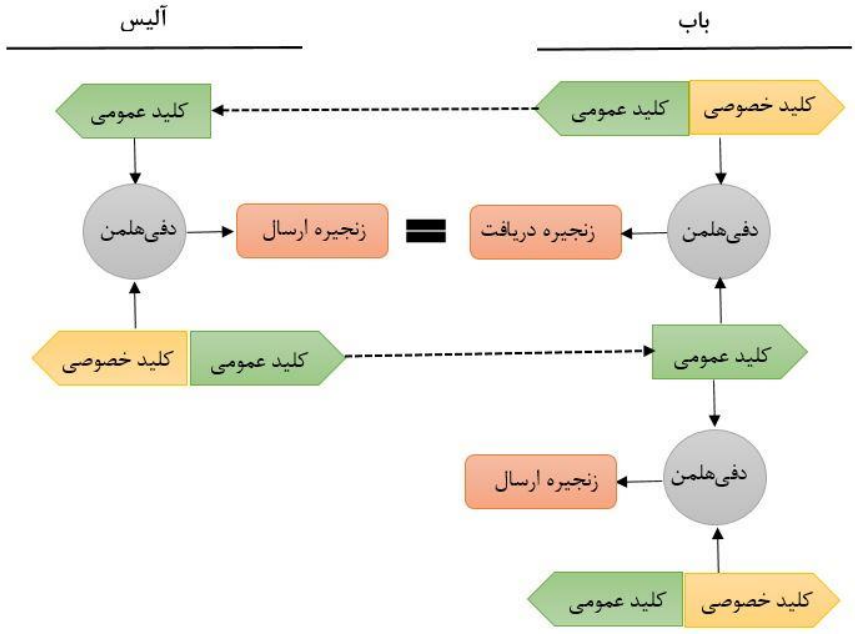


شکل (۳): مقداردهی اولیه[۶۰] از فرایند دفی‌هلمن ضامن‌دار توسط آلیس

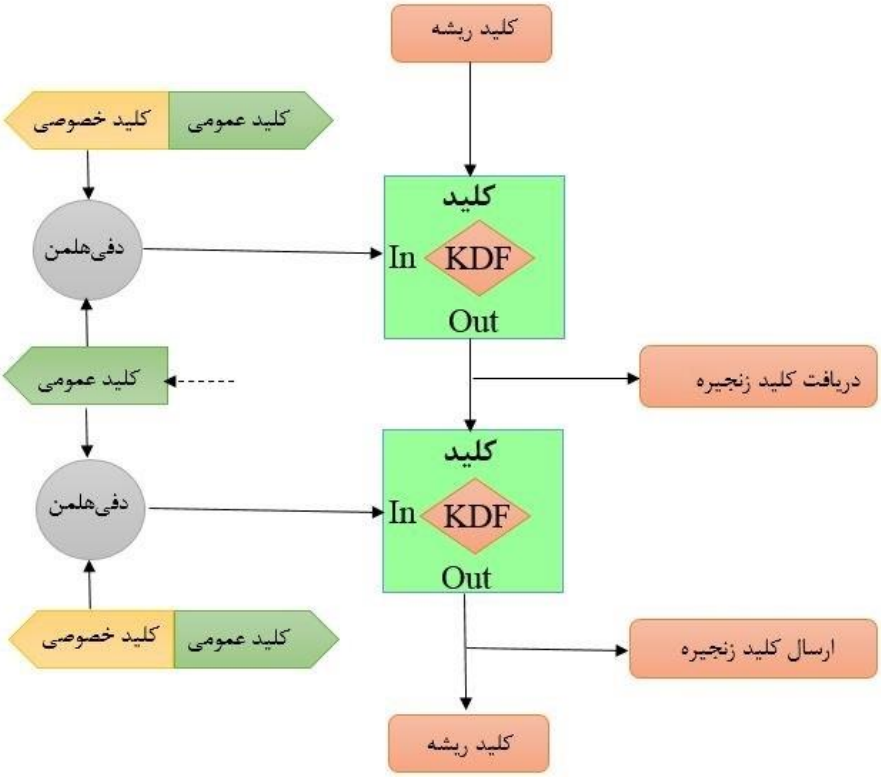


شکل (۴): مقداردهی اولیه از دفی‌هلمن ضامن‌دار که توسط باب انجام می‌شود.

تا اینجای کار، خروجی‌های دفی‌هلمن جهت ساده‌سازی تشریح فرایند دفی‌هلمن ضامن‌دار، فقط خروجی‌ها نامیده شده بود؛ اما خروجی‌های دفی‌هلمن در KDF جهت به دست آوردن کلیدهای زنجیره‌ای فرستنده و گیرنده برای فرایند کلیدمتقارن ضامن‌دار استفاده می‌شود. شکل (۵) این نکته را مشخص می‌کند که خروجی دفی‌هلمن با ارسال یا دریافت زنجیره تغییر می‌کند. در مرحله اول که آلیس قصد دارد پیام خود را با کلید عمومی ضامن‌دارش و خروجی دفی‌هلمن ارسال نماید یک زنجیره ارسال از خروجی دفی‌هلمن نتیجه گرفته می‌شود که این زنجیره از طریق زنجیره KDF به دست می‌آید. در ادامه، باب در سمت خودش، با استفاده از کلید عمومی آلیس و کلید خصوصی‌اش یک کلید زنجیره دریافت را از طریق خروجی دفی‌هلمن به دست می‌آورد. سپس باب کلید زنجیره ارسال جدید را از طریق خروجی دفی‌هلمن دومش نتیجه می‌گیرد [۲۲].



شکل (۵): زنجیره‌های ارسال و دریافت



شکل (۶): نمایی از فرایند کامل مرحله دفی‌هلمن ضامن‌دار

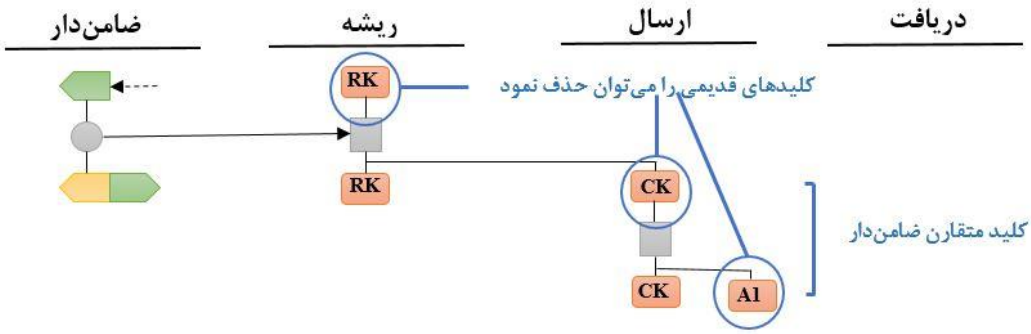
شکل‌هایی که تاکنون نمایش داده شدند یک توضیح ساده از فرایند دفی‌هلمن ضامن‌دار بود. دفی‌هلمن ضامن‌دار، کلیدهای خروجی را می‌گیرد و از آن‌ها به‌عنوان ورودی‌های KDF جهت به دست آوردن زنجیره ریشه استفاده می‌کند. در ادامه خروجی‌های KDF به‌عنوان کلید ارسال یا دریافت استفاده می‌شود. در اینجا، استفاده از زنجیره KDF باعث بهبود تاب‌آوری و امنیت پس‌رو می‌شود. قابل‌ذکر است که در علوم مربوط به سامانه‌های پیچیده، تاب‌آوری به ظرفیت یک اکوسیستم در پاسخ دادن به اختلالات یا نابسامانی‌ها گفته می‌شود؛ به‌گونه‌ای که بتواند در برابر خسارت‌های واردشده از خود مقاومت نشان دهد و به‌سرعت بهبود یابد. شکل (۶) نشان می‌دهد که دفی‌هلمن ضامن‌دار دو بار زنجیره ریشه KDF را به‌روز می‌کند و از کلیدهای خروجی KDF به‌عنوان کلیدهای زنجیره ارسال و دریافت جدید استفاده می‌نماید [۲۲].

۴-۱-۳- ضامن‌دار دابل

ضامن‌دار دابل دسته‌ای از الگوریتم‌ها است که از ترکیب کلیدمتقارن و دفی‌هلمن ضامن‌دار به شرح زیر به دست می‌آید:

- هنگام ارسال یا دریافت پیام، یک مرحله کلیدمتقارن ضامن‌دار بر روی زنجیره ارسال یا دریافت برای استخراج کلید پیام اعمال می‌شود [۲۲].
- هنگامی‌که کلید عمومی ضامن‌دار جدید دریافت می‌شود، قبل از فرایند کلیدمتقارن ضامن‌دار، مرحله دفی‌هلمن ضامن‌دار انجام‌شده تا کلیدهای زنجیره‌ای جایگزین شوند [۲۲].

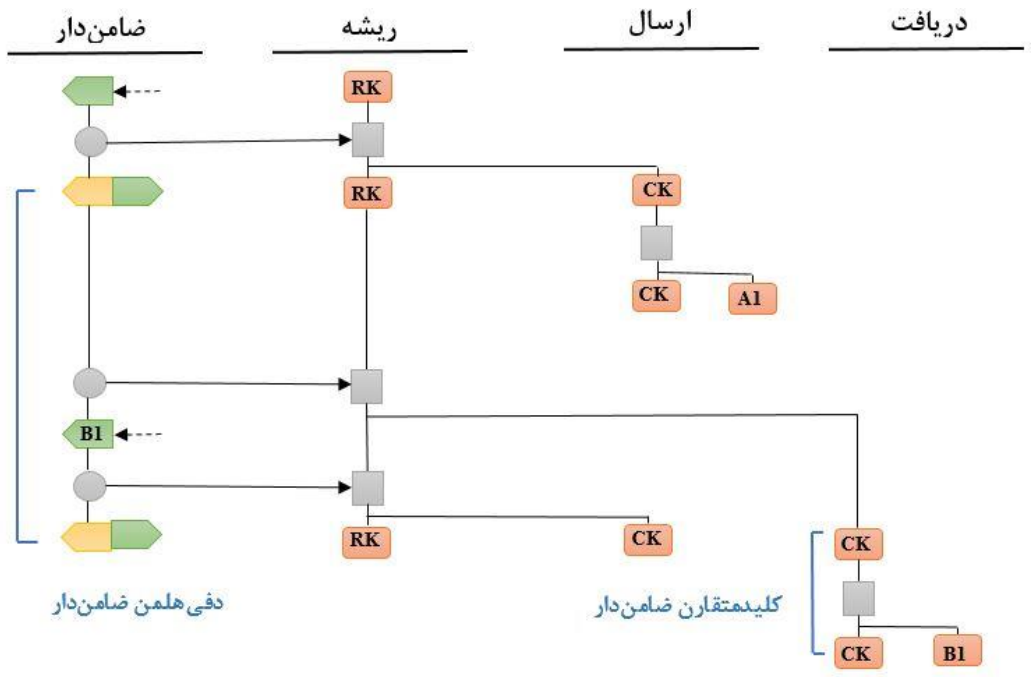
شکل (۷): مرحله ضامن‌دار دابل آغازین که توسط آلیس انجام می‌شود.



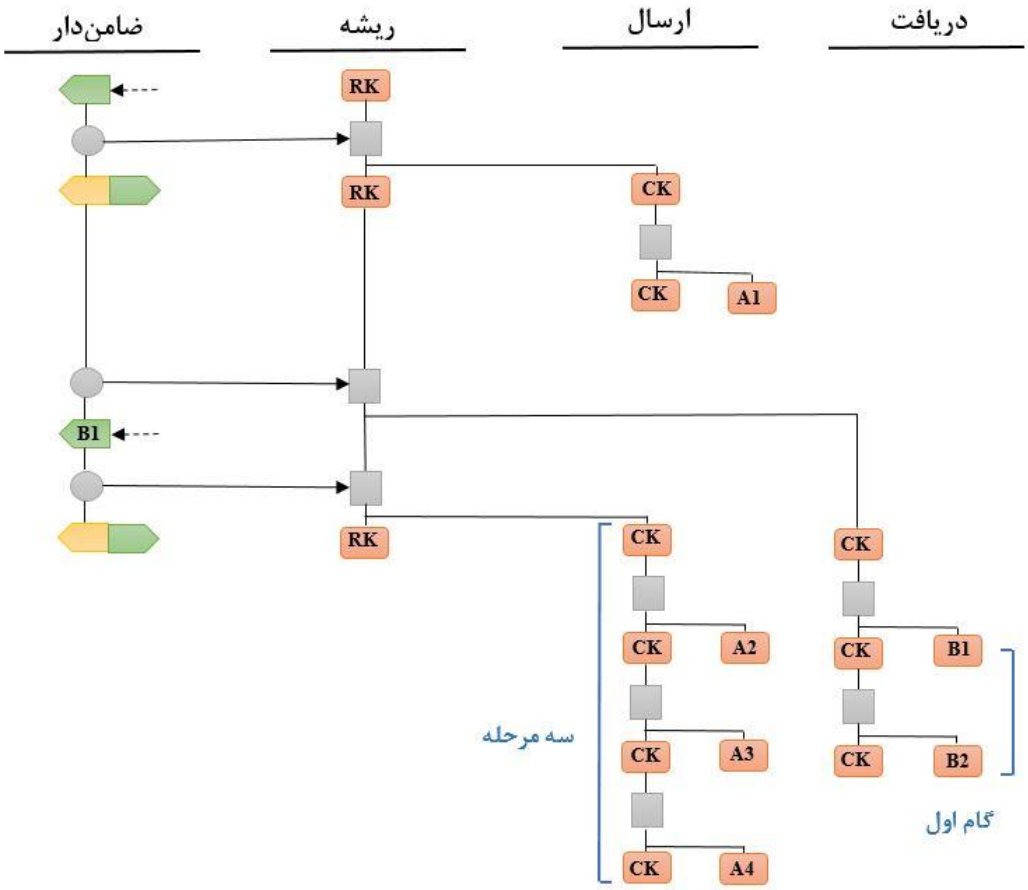
شکل (۸): اولین پیام ضامن‌دار دابل که با A1 نشان داده‌شده است.

این بخش، در مورد ارتباط بین الگوریتم‌های معرفی‌شده برای تشکیل ضامن‌دار دابل بوده که به این موضوع از دیدگاه آلیس پرداخته می‌شود. در شکل (۷) نشان داده‌شده که چگونه آلیس با استفاده از کلید عمومی ضامن‌دار باب، مقداردهی اولیه خودش را انجام می‌دهد به‌طوری‌که کلید ریشه (RK) راز مشترکی بوده که به‌عنوان کلید اصلی ریشه برای زنجیره KDF استفاده می‌شود. آلیس جفت کلید ضامن‌دار خود را تولید نموده و سپس خروجی دفی‌هلمن را به زنجیره KDF ریشه می‌فرستد تا یک کلید ریشه جدید و یک کلید زنجیره ارسال (CK) محاسبه نماید [۲۲]. شکل گفته‌شده به چهار قسمت مختلف تقسیم‌شده است. فرایند ضامن‌دار جایی رخ می‌دهد که جفت کلید ضامن‌دار تغییر می‌کند و کلید خصوصی ضامن‌دار آلیس و کلید عمومی ضامن‌دار باب ارسال‌شده تا یک خروجی دفی‌هلمن برای ورودی زنجیره KDF ریشه تولید شود. قسمت ستون در شکل (۷) مکانی از الگوریتم است که کلید پیام برای رمزگذاری از طریق زنجیره KDF کلیدمتقارن، تولید می‌شود. همچنین ستون آخر در الگوریتم جایی است که کلید پیام برای رمزگشایی پیام دریافت شده با استفاده از زنجیره KDF کلیدمتقارن، به دست می‌آید. برای اطمینان از حفظ محرمانگی در سراسر فرایند ضامن‌دار دابل، RK قدیمی پس از استفاده برای استخراج RK جدید، حذف می‌شود.

شکل (۸) نشان می‌دهد که آلیس اولین پیام خود را برای باب می‌فرستند که A1 نامیده می‌شود. مؤلفه CK ارسالی در یک مرحله کلیدمتقارن ضامن‌دار برای استخراج یک CK جدید و یک کلید پیام (A1) استفاده می‌گردد تا اینکه آلیس بتواند پیامش را رمزگشایی نماید. در ادامه CK جدید برای استفاده بعدی ذخیره می‌گردد و این در حالی است که CK قدیمی و کلید پیام را می‌توان حذف نمود زیرا دیگر هیچ استفاده‌ای برای آلیس ندارد.



شکل (۹): اولین پیام ضامن‌دار دابل دریافت شده که با B1 نشان داده‌شده است.



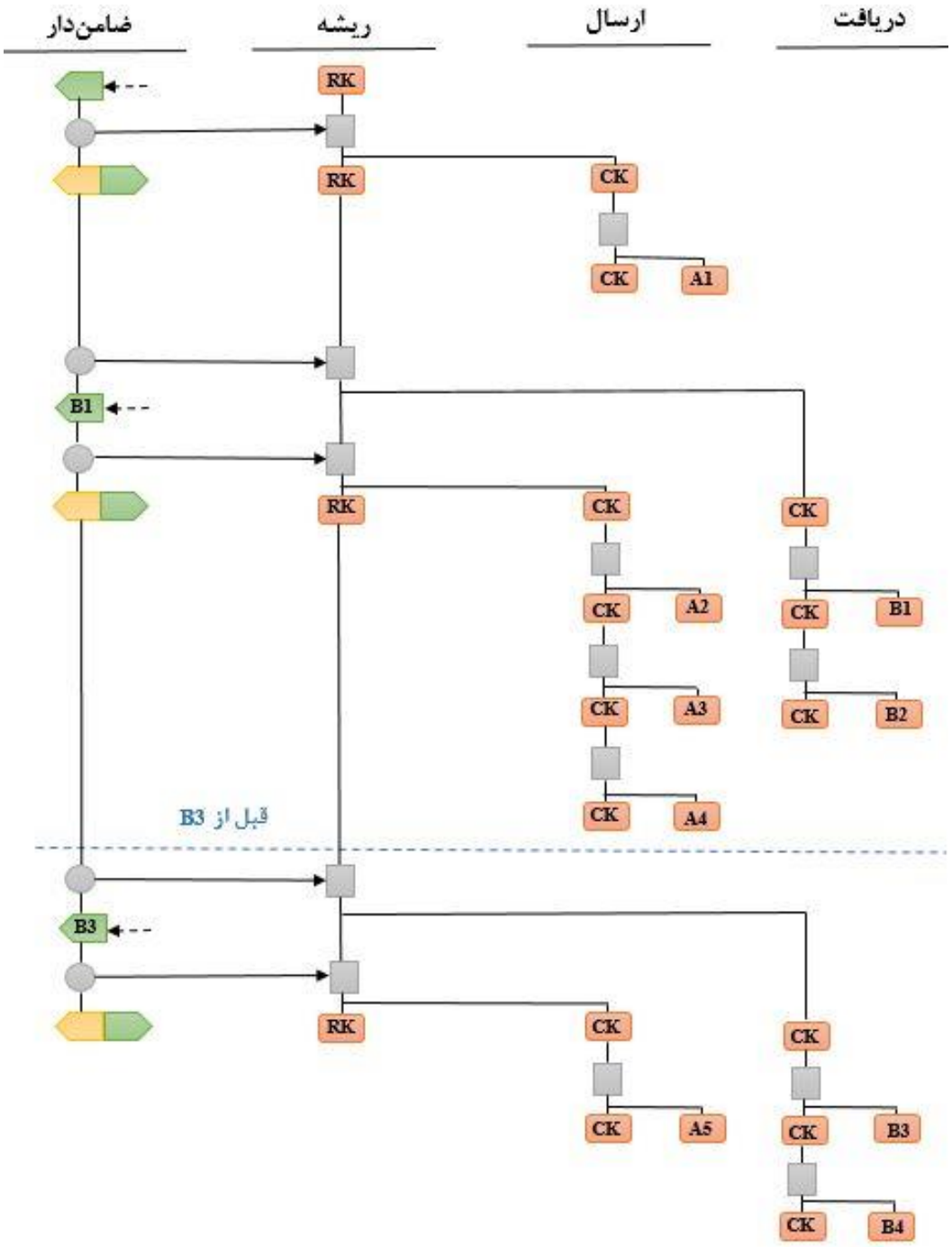
شکل (۱۰): مرحله ضامن‌دار دابل برای پیام‌های ارسالی A2، A3 و A4 و پیام دریافتی B2

شکل (۹) نشان می‌دهد که آلیس اولین پاسخ خود را از باب دریافت می‌کند که با B1 نشان داده‌شده و باب کلید عمومی ضامن‌دار جدید خود را ارسال نموده است. این بدان معناست که آلیس نیاز به محاسبه یک جفت کلید ضامن‌دار جدید دارد. آلیس برای به دست آوردن کلیدهای دریافت و ارسال زنجیره‌ای جدید، یک مرحله دفی‌هلمن ضامن‌دار جدید به کار می‌برد. آلیس برای به دست آوردن RK و CK جدید برای زنجیره KDF دریافتی، از کلید خصوصی ضامن‌دار قدیمی‌اش و کلید عمومی جدید باب استفاده می‌کند. کلید زنجیره دریافتی، برای استخراج کلید زنجیره دریافتی جدید استفاده‌شده و کلید پیام، برای رمزگشایی پیام باب بکار می‌رود. در ادامه آلیس با استفاده از کلید خصوصی ضامن‌دار جدیدش یک خروجی دفی‌هلمن جدید برای ریشه بعدی از زنجیره KDF به دست می‌آورد تا اینکه بتواند یک RK جدید تهیه نموده و با این عمل CK را بفرستد.

شکل (۱۰) نشان می‌دهد که آلیس برای ارسال پیام A2، دریافت پیام B2 با کلید عمومی ضامن‌دار قدیمی باب و همچنین فرستادن دو پیام جدید A3 و A4 برای باب، چند مرحله ضامن‌دار را باید انجام دهد. آلیس پیام B2 را با استفاده از کلیدهای ضامن‌دار قدیمی باب دریافت می‌کند، این بدان معناست که آلیس فقط نیاز به انجام یک مرحله ضامن‌دار با کلیدمتقارن دارد تا یک CK دریافتی جدید و یک کلید پیام برای رمزگشایی پیام B2 به دست آورد. قبل از اینکه آلیس بخواهد پیام دوم خود را که با A2 نشان داده‌شده بفرستد، باید یک مرحله ضامن‌دار با استفاده از کلیدمتقارن را انجام داده تا یک CK ارسالی جدید و یک کلید پیام برای رمزگذاری پیام A2 خودش به دست آورد. آلیس برای به دست آوردن کلیدهای درست پیام باید همین عملیات کلیدمتقارن ضامن‌دار را برای پیام‌های A3 و A4 نیز انجام دهد.

شکل (۱۱) وضعیتی را نشان می‌دهد که آلیس پیام‌های B3 و B4 را با استفاده از کلید عمومی ضامن‌دار جدید باب دریافت نموده و همچنین آخرین پیام فرستاده‌شده از طرف آلیس را (A5) نشان می‌دهد. آلیس پیام‌های جدیدی را از باب با استفاده از کلید عمومی جدیدش دریافت می‌کند و این در حالی است که آلیس ابتدا یک خروجی دفی‌هلمن جدید برای ضامن‌دار کردن ریشه زنجیره KDF به دست آورده تا اینکه بتواند یک RK جدید و یک CK دریافتی جدید محاسبه نموده و از آن‌ها برای رمزگشایی پیام‌های باب استفاده

نماید. مؤلفه CK دریافتی برای اجرای مرحله کلیدمتقارن ضامن‌دار دومرتبه استفاده می‌شود. در مرتبه اول برای به دست آوردن یک CK جدید و یک کلید پیام جدید برای رمزگشایی پیام B3 استفاده می‌شود و در مرتبه دوم برای مرحله ضامن‌دار جهت استخراجCK دوم و کلید پیام برای پیام B4، استفاده می‌گردد. در ادامه آلیس یک جفت کلید ضامن‌دار جدید تولید نموده و با بکار بردن کلید خصوصی ضامن‌دار جدیدش، یک RK جدید و یک CK ارسالی جدید با استفاده از کلید عمومی ضامن‌دار جدید باب، استخراج می‌نماید. مؤلفه CK ارسالی به این منظور استفاده می‌شود تا یک مرحله کلیدمتقارن ضامن‌دار انجام شود که این عمل باعث تولید یک CK جدید و همچنین استخراج یک کلید پیام شده و آلیس با استفاده از آن‌ها پیام A5 را رمزگذاری می‌نماید.

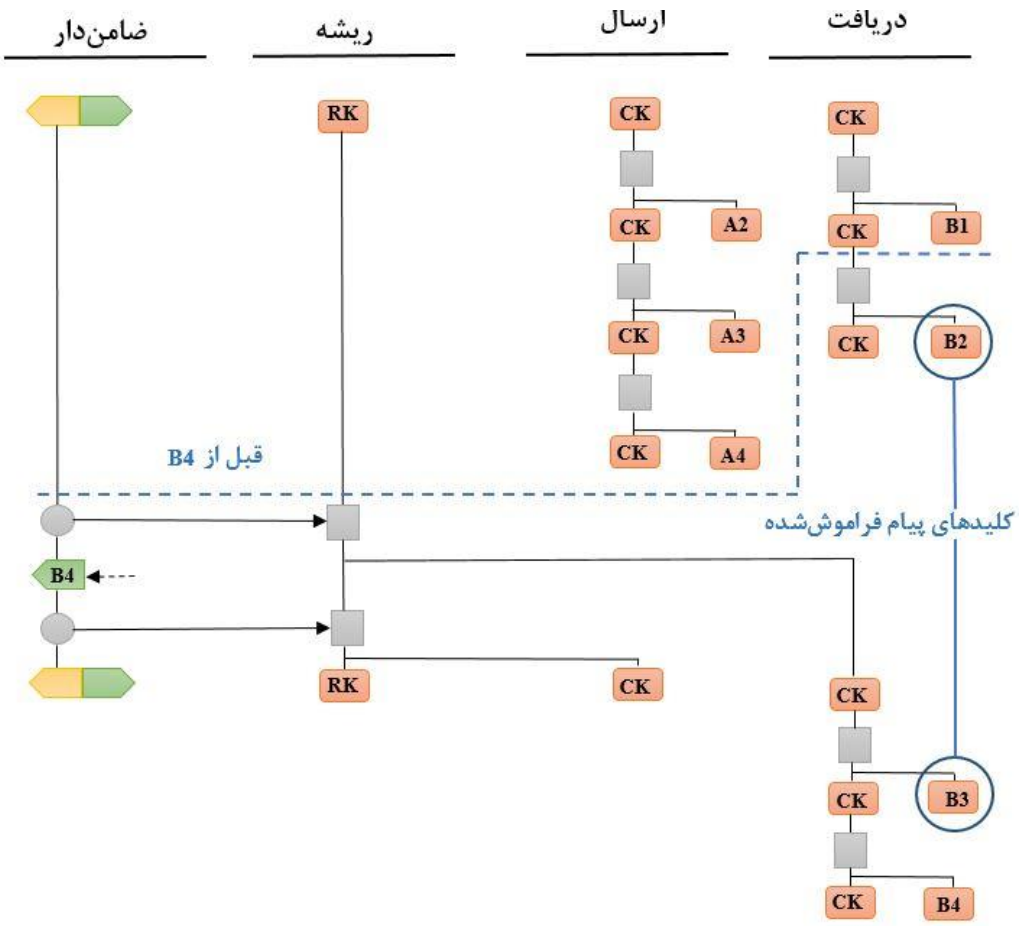


شکل (۱۱): مرحله ضامن‌دار دابل پیام A5 به همراه فرایند دریافت پیام‌های B3 و B4

۵-۱-۳- پیام‌های خارج از نوبت

فرایند ضامن‌دار در هر هدر پیام، با واردکردن شماره پیام در زنجیره ارسال $(N = 0,1,2,\cdots)$ و همچنین طول (تعداد کلیدهای پیام) در زنجیره ارسال قبلی (PN)، پیام‌های ازدست‌رفته یا خارج از نوبت را مدیریت می‌نماید [۲۲]. دلیل این موضوع این است که دریافت‌کننده، کلیدهای مربوط به کلید پیام را در اختیار داشته باشد درحالی‌که هنوز کلیدهای پیام فراموش‌شده[۶۱] را ذخیره دارد و همچنین گیرنده پیام را بعداً دریافت می‌نماید. قابل‌ذکر است که هنگام دریافت یک پیام، یک دفی‌هلمن ضامن‌دار راه انداخته[۶۲] می‌شود. همچنین با کم نمودن PN دریافتی از طول زنجیره دریافت‌کننده فعلی، تعداد پیام‌های رد شده[۶۳] در آن زنجیره دریافتی به دست می‌آید. پارامتر N دریافتی برابر با تعداد پیام‌هایی است که پس از مرحله دفی‌هلمن ضامن‌دار در زنجیره دریافت‌کننده جدید رد می‌شوند. نکته قابل‌توجه در این فرایند این است که اگر یک پیام دریافت شده نتواند یک مرحله دفی‌هلمن ضامن‌دار را راه اندازد[۶۴] آنگاه دریافت‌کننده باید مقدار N دریافتی را از طول زنجیره دریافتی خودش کم[۶۵] نماید.

برای توضیح این موضوع با یک‌شکل، می‌توانیم از دنباله پیام موجود از بخش قبل، استفاده کنیم، اما باید توجه داشته باشیم که در اینجا پیام B2 و B3 حذف می‌شوند. در ادامه زمانی که آلیس پیام B4 را از باب دریافت می‌کند مقادیر پارامترها به‌صورت $PN = 2$ و $N = 1$ می‌شود. حال آلیس متوجه می‌شود که نیاز به انجام یک مرحله دفی‌هلمن ضامن‌دار دارد اما در ابتدا، آلیس باید این محاسبه را انجام دهد که چند کلید پیام را برای ذخیره از زنجیره دریافتی فعلی خود (زنجیره ارسال قبلی باب) نیاز دارد. ازآنجاکه $PN = 2$ و طول زنجیره دریافت‌کننده فعلی او یک است درنتیجه تعداد کلیدهای ذخیره‌شده از زنجیره دریافت‌کننده فعلی آن یک کلید پیام (B2) می‌شود. در ادامه آلیس یک مرحله دفی‌هلمن ضامن‌دار انجام داده که به‌واسطه این فرایند، یک زنجیره دریافت جدید ایجاد می‌گردد. ازآنجاکه طول زنجیره دریافتی جدید آلیس صفر است او باید یک کلید پیام با استفاده از زنجیره دریافت جدید خودش (B3) ذخیره نماید. پس‌ازاینکه آلیس پیام‌های B2 و B3 را ذخیره نمود می‌تواند آخرین کلید پیام را برای رمزگشایی پیام B4 استخراج نماید.



شکل (۱۲): مدیریت پیام‌های خارج از نوبت

۲-۳- پروتکل توافق کلید X3DH

الگوریتم ضامن‌دار دابل به یک پروتکل توافق کلید بین دو شرکت‌کننده نیاز دارد. در بخش ۳-۱ در مورداستفاده از پروتکل توافق کلید توسعه‌یافته سه‌گانه دفی‌هلمن (X3DH) بحث شد. الگوریتم X3DH برای ایجاد یک راز مشترک بین دو طرف استفاده می‌گردد که متقابلاً یکدیگر را بر اساس کلیدهای عمومی احراز هویت می‌کنند [۲۴]. دو ویژگی مهم این الگوریتم، امنیت پیشرو و همچنین بحث انکارپذیری است.

روش معرفی‌شده، جهت توافق کلید برای تنظیمات غیر هم‌زمان[۶۶] طراحی‌شده که در آن یک کاربر که باب نامیده می‌شود آفلاین در نظر گرفته‌شده اما اطلاعات را در یک سرور منتشر نموده است. کاربر دیگری که آلیس می‌نامیم می‌خواهد از این اطلاعات برای ارسال داده‌های رمزگذاری شده به باب استفاده نماید و همچنین یک راز مشترک برای ارتباطات بعدی ایجاد کند [۲۴].

۲-۳-۱- مقدمات پیاده‌سازی

برای پیاده‌سازی پروتکل X3DH یک سری خصوصیات وجود دارد [۲۴] که برای راحتی پیاده‌سازی از قبل انتخاب و تعیین‌شده است. دو پارامتر کلیدی این پروتکل، خم بیضوی و تابع چکیده ساز بوده و همچنین یک سری از اطلاعات در مورد آن‌ها که در کل این بخش استفاده می‌شود. خم بیضوی مورداستفاده بر پایه یکی از دو منحنی X25519[۶۷] یا X44810[۶۸] است. دلیل استفاده از این دو خم نیز سرعت پیاده‌سازی طرح‌های توافق کلید مبتنی بر این دو منحنی است. تابع چکیده ساز[۶۹] بکار رفته نیز می‌تواند هر تابع چکیده ساز امن ۲۵۶ یا ۵۱۲ بیتی باشد و همچنین از یک پارامتر به نام پارامتر اطلاعات استفاده می‌شود که یک‌رشته کد اسکی است که برای شناسایی برنامه بکار می‌رود.

در کل این بخش، مجموعه‌ای از کلیدها همراه با پروتکل X3DH استفاده می‌شوند. این کلیدها به این دلیل انتخاب می‌شوند که وقتی آلیس می‌خواهد با استفاده از رمزگذاری، برخی از داده‌های ابتدایی را برای باب ارسال نموده و به‌عنوان راز مشترک استفاده نماید، از سرور کلیدهای باب را که از قبل روی سرور بارگذاری نموده است درخواست می‌کند. درواقع این کار باعث می‌شود تا طرف‌های دیگر این اجازه را داشته باشند که یک راز مشترک با باب ایجاد نمایند. از یک سرور برای ذخیره پیام‌های آلیس و باب استفاده می‌شود که بعداً باب می‌تواند آن‌ها را بازیابی کند. به عبارت بهتر، سرور این مجموعه کلیدها را برای آلیس و باب نگه می‌دارد تا در صورت لزوم بازیابی شوند [۲۴]. این کلیدها، کلیدهای عمومی از خم بیضوی انتخاب‌شده هستند که به‌صورت زیر تعریف‌شده و نمایش داده می‌شوند:

- کلید IK_A: کلید شناسایی[۷۰] آلیس
- کلید EK_A: کلید موقتی[۷۱] آلیس
- کلید IK_B: کلید شناسایی باب
- کلید SPK_B: پیش کلید امضاشده[۷۲] باب
- کلید OPK_B: پیش کلید یک‌بارمصرف[۷۳] باب

کلیدهای عمومی که در اجرای پروتکل X3DH استفاده می‌شوند باید همه به فرم X25519 یا X44810 باشند [۲۴]. هر موجودیت در این پروتکل به‌عنوان یک کلید عمومی شناسایی طولانی‌مدت[۷۴] در نظر گرفته می‌شود؛ اما باید توجه داشت که باب دارای پیش کلیدهای امضاشده‌ای است که به‌صورت دوره‌ای تغییر می‌کند و همچنین یک مجموعه از کلیدهای یک‌بارمصرف نیز وجود دارد. پیش کلیدهای یک‌بارمصرف، در یک اجرای تکی از پروتکل X3DH[۷۵] استفاده می‌گردند.

۲-۳-۲- پروتکل X3DH

پروتکل X3DH از سه مرحله مختلف تشکیل‌شده است که این مراحل عبارت‌اند از:

۱. باب کلید شناسایی خود را به همراه پیش کلیدهایش در یک سرور منتشر می‌کند.
۲. آلیس بسته پیش کلید[۷۶] را از سرور دریافت نموده و از آن برای ارسال پیام اولیه به باب استفاده می‌کند.
۳. باب پیام اولیه آلیس را دریافت و پردازش می‌نماید.

مرحله اول: انتشار کلیدها

مرحله اول مربوط به کارهایی است که باب قبل از اینکه آلیس بتواند از سرور درباره باب اطلاعاتی به دست آورد، باید انجام دهد. باب باید مجموعه‌ای از کلیدهای عمومی مربوط به خم بیضوی انتخاب‌شده را به سرور ارسال نموده تا ذخیره شوند که این کلیدها شامل موارد زیر هستند:

- کلید شناسایی باب IK_B
- پیش کلید امضاشده باب SPK_B
- امضا پیش کلید باب $Sig(IK_B, Encode(SPK_B))$
- یک مجموعه از پیش کلیدهای یک‌بارمصرف باب $(OBK_B^1, OBK_B^2, OBK_B^3, \cdots)$

کلیدهای شناسایی باید یک‌بار در سرور بارگذاری شوند، درحالی‌که کلیدهای دیگر مانند پیش کلیدهای یک‌بارمصرف جدید را می‌توان بعداً در صورت کم شدن تعداد سرورها، با اطلاع دادن به باب برای بارگذاری بیشتر، بار دیگر بارگذاری نمود. از طرف دیگر، امضاهای جدید پیش کلیدهای امضاشده، باید به‌طور دوره‌ای بارگذاری شوند و این به خود باب بستگی دارد که چه زمانی بخواهد آن‌ها را بارگذاری نماید به‌طوری‌که این بارگذاری می‌تواند هرروز، یک‌بار در هفته یا یک‌بار در ماه انجام شود.

اگر دیگر کاربران به دلیل تأخیر در شبکه ارتباطات، موفق به به‌روزرسانی پیش کلیدهای امضاشده خود نشوند و آن‌ها قبل از دریافت پیش کلیدهای جدید، به باب پیام بفرستند این برای باب بسیار ضرورت دارد که کلیدهای خصوصی قبلی مربوط به پیش کلید قدیمی امضاشده را، حتی پس از بارگذاری یک پیش کلید امضاشده جدید، ذخیره نماید [۲۴]. همچنین برای حفظ امنیت پیشرو، حذف کلید خصوصی مهم است.

مرحله دوم: ارسال پیام اولیه

آلیس با سرور ارتباط برقرار نموده و بسته پیش کلیدها را که حاوی کلیدهای باب است را از سرور گرفته و می‌آورد[۷۷]. حال آلیس کلیدهای مشابهی که باب در مرحله اول بر روی سرور قرار داده است[۷۸] را دریافت می‌کند. اکنون آلیس، دارای کلید شناسایی باب، پیش کلید امضاشده، امضای پیش کلید و به‌صورت اختیاری یک پیش کلید یک‌بارمصرف انفرادی[۷۹] است.

اگر سرور تعداد بیشتری از پیش کلید یک‌بارمصرف باب را داشته باشد، آلیس آن‌ها را دریافت می‌کند، زیرا سرور هر بار که پیش کلید یک‌بارمصرف را به کاربر دیگری ارسال می‌کند یکی از آن‌ها حذف می‌شود. اگر سرور تعداد بیشتری از آن‌ها را ذخیره نکرده باشد، بسته شامل پیش کلید نخواهد بود [۲۴].

آلیس تلاش می‌کند که امضای پیش کلید را تائید نماید اما اگر به‌درستی امضا تائید نشود، آلیس باید پروتکل را ادامه ندهد[۸۰]. برای اطلاعات بیشتر در مورد روند احراز هویت در پروتکل سیگنال، به مرجع [۲۵] مراجعه شود. هنگامی‌که فرایند احراز هویت با موفقیت انجام گردید، آلیس یک جفت کلید موقت با استفاده از کلید عمومی EK_A تولید می‌کند [۲۴]. حال اگر بسته حاوی یک پیش کلید یک‌بارمصرف نباشد آنگاه آلیس محاسبات زیر را انجام می‌دهد:

$$\begin{aligned} DH۱ &= DH(IK_A, SPK_B), \\ DH۲ &= DH(EK_A, IK_B), \\ DH۳ &= DH(EK_A, SPK_B), \\ SK &= KDF(DH۱ \,||\, DH۲ \,||\, DH۳). \end{aligned}$$

اگر بسته نرم‌افزاری حاوی یک پیش کلید یک‌بارمصرف باشد، محاسبه دفی‌هلمن دیگری به‌صورت زیر اضافه می‌شود:

$$\begin{aligned} DH۴ &= DH(EK_A, OPK_B), \\ SK &= KDF(DH۱ \,||\, DH۲ \,||\, DH۳ \,||\, DH۴). \end{aligned}$$

این‌یک نکته مهمی است که آلیس پس از انجام محاسبه SK، کلید خصوصی موقت و خروجی دفی‌هلمن خود را باید برای حفظ محرمانه بودن پاک نماید. آلیس داده‌های مرتبط به دنباله بایت[۸۱] AD را محاسبه می‌کند که حاوی اطلاعاتی برای هر دو طرف است.

$$AD = Encode(IK_A) \,||\, Encode(IK_B).$$

آلیس می‌تواند اطلاعات بیشتری را به ترتیب الحاق نماید[۸۲]، مانند نام‌های کاربری، گواهینامه‌ها یا سایر اطلاعاتی که ممکن است مهم باشد. سپس آلیس پیام اولیه خود را به باب ارسال می‌کند که حاوی اطلاعات زیر است:

- کلید شناسایی آلیس IK_A
- کلید موقتی آلیس EK_A
- شناسه‌هایی که نشان می‌دهد آلیس از کدام یک از پیش کلیدهای باب استفاده نموده است.
- یک متن رمزنگاری همراه با برخی از طرح‌های رمزگذاری مانند AEAD [۲۶-۲۷] و استفاده از AD به‌عنوان داده‌های مرتبط و استفاده از یک کلید رمزگذاری که یا SK بوده یا خروجی برخی توابع شبه تصادفی رمزنگاری‌شده توسط SK است.

متن رمز شده آغازین آلیس معمولاً به‌عنوان پیام ابتدایی در یک پروتکلی ارتباطی postX3DH، مانند پروتکل ضامن‌دار دابل، استفاده می‌شود. متن رمز شده دو نقش مهم دارد که اولین نقش را به‌عنوان اولین پیام در برخی از پروتکل‌های postX3DH دارد و دومین نقش آن، به‌عنوان بخشی از پیام ابتدایی X3DH آلیس به باب است [۲۴].

مرحله سوم: دریافت پیام ابتدایی

مرحله سوم از پروتکل X3DH همانند دو مرحله قبل است. باب پیام اولیه آلیس را که شامل کلید شناسایی آلیس و کلید موقت می‌باشد را از پیام بازیابی می‌کند. سپس باب کلید خصوصی مربوط به هویت فرد و همچنین کلیدهای خصوصی مربوط به پیش کلید امضاشده و پیش کلید یک‌بارمصرفی که آلیس از آن استفاده نموده را بارگیری می‌نماید [۲۴].

باب برای استخراج SK خود، همان مراحل گفته‌شده در بالا را به همراه محاسبات دفی‌هلمن و تابع KDF تکرار می‌کند و سپس مقادیر دفی‌هلمن را همانند آلیس حذف می‌نماید. در مرحله بعدی، باب دنباله‌ای از بایت AD را می‌سازد و در پایان تلاش می‌کند متن رمز شده اولیه را با استفاده از SK و AD رمزگشایی نماید. تنها تفاوت باب با آلیس در این قسمت از پروتکل، نحوه رمزگشایی است. در صورت عدم موفقیت در رمزگشایی، باب SK را حذف نموده و پروتکل را لغو می‌کند و شرکت‌کنندگان باید پروتکل را از ابتدا انجام دهند [۲۴]. اگر رمزگشایی موفقیت‌آمیز باشد، باب اطلاعاتی را به دست می‌آورد که آلیس رمزگذاری نموده و پروتکل برای باب کامل در نظر گرفته می‌شود. برای حفظ محرمانگی پیشرو و عدم به خطر انداختن آن، باب باید هر کلید خصوصی پیشرو یک‌بارمصرف[۸۳] را که در طول پروتکل استفاده‌شده است حذف نماید.

۳-۳- به‌کارگیری رمزنگاری پساکوانتومی در امنیت پروتکل سیگنال

یکی از مسائل مهم و چالش‌برانگیز در حوزه رمزنگاری، نقش و تأثیر قدرت محاسباتی کامپیوترهای کوانتومی (حملات کوانتومی) بر روی سامانه‌های رمزنگاری متداول است. تأثیر حملات کوانتومی در سامانه‌های رمزنگاری متقارن باعث کاهش امنیت این سامانه‌ها به نصف ادعاهای امنیتی این سامانه‌ها می‌شود اما در حوزه رمزنگاری نامتقارن (کلید عمومی) این نقش و تأثیر بسیار جدی، قابل‌تأمل و پراهمیت است. به‌بیان‌دیگر، اگر در حوزه رمزنگاری نامتقارن از سامانه‌های کلاسیک به سامانه‌های پساکوانتوم مهاجرتی صورت نگیرد آنگاه در حداقل پنج سال آینده، خطرات بالقوه‌ای برای امنیت سامانه‌های مورداستفاده مردم مانند بانک‌ها، حوزه دولت الکترونیک و موارد بسیار دیگر، رخ می‌دهد. یکی از راه‌های حل‌های پیشنهادشده، رمزنگاری پساکوانتوم[۸۴] است که مؤسسه ملی فناوری و استاندارد[۸۵] از سال ۲۰۱۷ متولی یک مسابقه رمزنگاری در این حوزه شده است و امیدوار است که تا سال ۲۰۲۵، حداقل سامانه‌های رمزنگاری پساکوانتومی را در بخش‌های کلید عمومی، برقراری کلید و امضای دیجیتال برای استفاده عموم پیاده‌سازی و استانداردسازی نماید.

راه‌حل قطعی مقابله با حملات کوانتومی، رمزنگاری کوانتومی بوده که مبتنی بر مکانیک کوانتوم است اما به دلیل هزینه و در دسترس نبودن برای عموم، قابل‌استفاده در حال حاضر نیست. اگرچه که بخش‌های نظامی ممکن است این فناوری را در حال حاضر استفاده نمایند اما در بخش غیرنظامی این بستر هنوز فراهم نشده است؛ بنابراین، استفاده از بسترهای موجود کلاسیک و تغییر نرم‌افزاری سامانه‌های رمزنگاری نامتقارن کلاسیک مورداستفاده، یک پوشش برای رسیدن به تجاری‌سازی و در دسترس قرار گرفتن فناوری رمزنگاری کوانتومی است. به بیان بهتر، رمزنگاری پساکوانتوم یک راه‌حل قطعی برای دفع خطرات احتمالی حملات کوانتومی نیست و فقط یک پوشش بین مهاجرت از دنیای رمزنگاری کلاسیک به دنیای رمزنگاری کوانتومی است.

سامانه‌های رمزنگاری کلید عمومی، تبادل کلید و امضای دیجیتال مورداستفاده در حال حاضر، بر مبنای مسائل ریاضی تجزیه اعداد بزرگ و لگاریتم گسسته هستند. این مسائل ریاضی تا حداقل چند سال پیش به نظر می‌رسیدند که مسائل سختی در برابر قدرت محاسباتی کامپیوترهای کلاسیک باشند اما با ظهور فناوری و الگوریتم‌های کوانتومی مانند الگوریتم شور جهت تجزیه اعداد بزرگ به عامل‌های اول، موضوع استفاده از مسائل سخت ریاضی مقاوم در برابر الگوریتم‌های کوانتومی به یک بحث مهم و چالش‌برانگیز در دنیای رمزنگاری تبدیل‌شده است.

تاکنون سه موضوع ریاضی شامل مشبکه، کدهای تصحیح خطا و سامانه‌های چند متغیره، ادعاشده که مسائلی سخت در برابر الگوریتم‌های کوانتومی هستند؛ اما باید به این نکته مهم توجه داشت که فقط ادعاشده که سامانه‌های رمزنگاری مشبکه‌مبنا، کدمبنا و چند متغیره در برابر الگوریتم‌های کوانتومی موجود امن هست و هیچ تضمین امنیتی وجود ندارد که الگوریتم کوانتومی برای به دست آوردن مسائل سخت مشبکه مانند مسئله کوچک‌ترین بردار، وجود نداشته باشد. شاید به نظر برسد که یک ایده، طراحی یک مسئله سخت جدید به جز این سه مسئله گفته‌شده باشد اما باید توجه داشت که مسئله‌ای را سخت در نظر می‌گیریم که حداقل چند دهه، جامعه ریاضی، سخت بودن آن را به چالش کشیده باشد و یک اطمینان نسبی حاصل شود به‌طوری‌که بتوان آن را مسئله سخت در نظر گرفت. با توجه نکات گفته‌شده، انتخاب و استفاده از سامانه‌های رمزنگاری پساکوانتوم مشبکه‌مبنا، کدمبنا و چند متغیره، یکی از راه‌های مهاجرت از دنیای رمزنگاری کلاسیک به دنیای رمزنگاری کوانتوم بوده اما لازم است که در انتخاب پارامترهای امنیتی آن دقت و توجه لازم را داشته باشیم.

به جز اینکه، فناوری الگوریتم‌های کوانتومی در آینده می‌توانند سامانه‌های رمزنگاری کلاسیک موجود را تهدید نمایند یکی از خطرات مهم دیگر، ذخیره ارتباطات محرمانه فعلی توسط دشمن بوده[۸۶] که در آینده نزدیک بتواند با استفاده از قدرت محاسباتی کامپیوترهای کوانتومی، این ارتباطات محرمانه ذخیره‌شده را بازیابی نمایند و از اطلاعات استخراج‌شده، امنیت را به خطر بیندازد؛ بنابراین، نه‌فقط در پنج سال آینده بلکه در همین زمان حاضر نیز، فناوری کوانتومی تهدیدی بسیار جدی باید تلقی شود و سامانه‌های رمزنگاری کلاسیک الزاماً تا یک سال آینده باید با سامانه‌های رمزنگاری پساکوانتومی جایگزین شوند. مباحث گفته‌شده در بالا به این دلیل بیان شد که پروتکل سیگنال نیز از این تهدید مستثنا نیست. به بیان بهتر، در پروتکل سیگنال یک پروتکل توافق کلید مبتنی بر خم بیضوی استفاده می‌شود که مسئله سخت آن مربوط به لگاریتم گسسته است؛ بنابراین، طراحان سیگنال به‌تازگی به این نتیجه رسیده‌اند که بجای استفاده از پروتکل توافق کلید کلاسیک از یک پروتکل توافق کلید مقاوم در برابر حملات کوانتومی استفاده نمایند که در ادامه مقاله، شرح داده می‌شود. درواقع، طراحان سیگنال از این مسئله نگران هستند که ذخیره اطلاعات محرمانه فرستاده‌شده، بتواند در آینده خطر بالقوه‌ای را برای کاربران ایجاد نماید [۲۸].

پروتکل توافق کلید X3DH مبتنی بر خم بیضوی بوده که همان‌طور که گفته شد مسئله سخت آن مرتبط با مسئله لگاریتم گسسته است که این مسئله در برابر الگوریتم‌های کوانتومی آسیب‌پذیر هست. طراحان سیگنال پیشنهاد ترکیب پروتکل توافق کلید X3DH و سامانه پساکوانتومی کپسوله‌سازی کلید[۸۷] کریستال کای‌بر[۸۸] را جهت امنیت در برابر حملات کوانتومی داده‌اند. سامانه کریستال کای‌بر، یک سامانه رمزنگاری پساکوانتومی مبتنی بر مسائل یادگیری همراه با خطا[۸۹] بوده که سختی مسئله یادگیری همراه با خطا نیز مرتبط با مسئله یافتن کوچک‌ترین بردار در مشبکه است. سامانه کریستال کای‌بر از نظر پیاده‌سازی نرم‌افزاری و اندازه کلیدهای عمومی و خصوصی استفاده‌شده در آن و همچنین پارامترهای امنیتی، کاندید نهایی انتخاب‌شده توسط NIST برای جایگزینی با سامانه‌های رمز کلید عمومی و تبادل کلید کلاسیک است. ایده‌های ساخت سامانه‌های رمزنگاری پساکوانتوم را می‌توان به دو بخش خالص[۹۰] و ترکیبی[۹۱] تقسیم نمود. مقاله [۲۹]، این تقسیم‌بندی را در حوزه‌های مختلف توضیح داده است. منظور از ایده خالص این است که سامانه رمزنگاری پساکوانتومی بر اساس یک مسئله شفاف مانند مشبکه یا کد، طراحی‌شده باشد. سامانه‌هایی که در مسابقه رمزنگاری پساکوانتوم NIST در حال رقابت هستند مبتنی بر ایده خالص هستند.

در ایده ترکیبی، سامانه پساکوانتومی ساخته‌شده مبتنی بر دو حالت است. حالت اول ایده ترکیبی این است که چند سامانه پساکوانتومی موجود را با یکدیگر الحاق[۹۲] نموده و یک سامانه جدید پساکوانتومی معرفی گردد. برای مثال سرویس وب آمازون از این ایده بهره گرفته و با الحاق چند سامانه کپسوله‌سازی کلید، ادعا نموده به یک سامانه امن برقراری کلید پساکوانتومی دست‌یافته است [۳۰]. حالت دوم ایده ترکیبی این است که یک سامانه رمزنگاری نامتقارن کلاسیک را با یک سامانه رمزنگاری پساکوانتومی الحاق نماییم. برای مثال در مقاله [۳۱] ادعاشده که از الحاق سامانه توافق کلید مبتنی بر خم بیضوی X25519 و همچنین یک سامانه کپسوله‌سازی کلید، یک

سامانه کپسوله‌سازی کلید به‌دست‌آمده که از لحاظ امنیت و پیاده‌سازی، نسبت به سایر سامانه‌های ترکیبی پساکوانتومی کارایی بهتری دارد.

واقعیت این است که در ساخت سامانه‌های پساکوانتومی خالص مانند سامانه‌های موجود در مسابقه NIST، امنیت این سامانه‌ها، نزدیک به یک دهه است که مطالعه شده و بنابراین یک اطمینان خاطر نسبی از امنیت این سامانه‌ها را می‌توان قبول داشت اما روش‌های ساخت سامانه‌های پساکوانتومی ترکیبی به‌تازگی مطرح‌شده و نیاز به زمان و تحقیقات بیشتری در حوزه امنیت این سامانه‌ها هست. برای مثال، این مسئله که اگر چند سامانه کپسوله‌سازی را ترکیب نماییم و بررسی این ادعا که با درست بودن یک تعداد مشخص از این سامانه‌ها، سامانه الحاق شده امن بوده، مسئله‌ای دشوار بوده و همچنین این سؤال که دشمن با استفاده از آن سامانه‌هایی که در سامانه الحاق شده امن نیستند آیا می‌تواند به اطلاعات بیشتری دست پیدا نماید نیز مسئله مهم دیگری است که باید به‌دقت پاسخ داده شود. به‌بیان‌دیگر، هیچ زمان امنیت را نباید فدای کارایی نمود و به همین علت است که NIST با این‌که سامانه‌های کدمبنا از نظر اندازه کلید، قابل‌رقابت با سامانه‌های مشبکه مبنا نیستند اما به دلیل قدمت مسئله سخت سامانه‌های کدمبنا، این سامانه‌ها را در بخش جایگزین دور آخر این مسابقه حفظ نموده است. صرف‌نظر از ایده ترکیبی که طراحان سیگنال ادعا نمودند و نام آن را PQXDH[۴۲] نامیده‌اند اما بررسی ادعای طراحان به دلیل نبود پیاده‌سازی مطرح‌شده، امکان‌پذیر نیست؛ اما اگر ادعاهای امنیتی مطرح‌شده در مقاله [۳۱] درست باشد آنگاه می‌توان سامانه توافق کلید پساکوانتومی هیبریدی پیشنهادشده در [۳۱] را در جهت مقاوم‌سازی پروتکل سیگنال در برابر حملات کوانتومی استفاده نمود.

۴- نتیجه‌گیری

این مقاله مربوط به تشریح و تحلیل پروتکل سیگنال بوده که زیربنای برنامه‌های کاربردی پیام‌رسانی مانند واتس‌آپ است. نرم‌افزار واتس‌آپ منبع باز نیست و بنابراین تعیین اینکه آیا واقعاً پروتکل سیگنال را پیاده‌سازی می‌کند یا خیر دشوار است. بااین‌وجود، کد پروتکل سیگنال در دسترس بوده و این امر باعث شده که بتوان امنیت پیام‌رسان واتس‌آپ را (با شرط پیاده‌سازی پروتکل سیگنال) تحلیل و بررسی نمود. بر اساس تجزیه‌وتحلیل امنیتی انجام‌شده بر روی پروتکل سیگنال، این نتیجه به دست آمد که مؤلفه اصلی پروتکل سیگنال یک اولیه رمزنگاری بنام تبادل کلید ضامن‌دار بوده که دلیل مفهومی بنام رمزنگاری ضامن‌دار شده است. پروتکل‌های ضامن‌دار تبادل کلید (مانند دفی‌هلمن ضامن‌دار) دارای دو ویژگی بسیار مهم محرمانگی پیشرو و پس‌رو هستند که این خصوصیات باعث می‌شود اگر تعدادی از کلیدهای رمزگذاری یکی از کاربران فاش شوند در این صورت نمی‌توان با استفاده از آن‌ها کلیدهای قبلی را به دست آورد و پیام‌های قبلی تبادل یافته را رمزگشایی نمود. به‌عبارت‌دیگر، روش ضامن‌دار نمودن باعث می‌شود که بعد از هر مرتبه ارسال پیام، کلیدهای جلسه به‌روزرسانی شوند. به دلیل این‌که پروتکل سیگنال یک طراحی جدید دارد که قبلاً موردمطالعه قرار نگرفته، تحلیل امنیتی این پروتکل یک مسئله چالشی و سخت است. در پروتکل سیگنال بیشتر از ده کلید مختلف استفاده می‌شود و نیز فرآیند به‌روزرسانی کلیدها در آن پیچیده است؛ بنابراین مدل‌های تحلیلی رایج که برای پروتکل‌ها ارائه‌شده‌اند برای سیگنال به‌راحتی صدق نمی‌کند. با این وجود، در جمع‌بندی این مقاله این نتیجه به دست آمد که نقص امنیتی قابل‌توجهی در طراحی پروتکل سیگنال پیدا نشده اما باید توجه داشت اگرچه که پروتکل سیگنال را می‌توان در برابر حملات کلاسیک امن دانست اما به دلیل پیشرفتی که در حوزه ساخت کامپیوترهای کوانتومی به وجود آمده، نیاز است که در بخش توافق کلید این پروتکل، اصلاح و یا تغییر پساکوانتومی صورت بگیرد. به بیان دقیق‌تر، استفاده از سامانه‌های کپسوله‌سازی کلید پساکوانتومی یکی از مهم‌ترین اقدامات در جهت دفع خطر حملات کوانتومی به بخش توافق کلید پروتکل سیگنال است.

مراجع

[1] K. Siau and Z. Shen, "Mobile communications and mobile services," *International Journal of Mobile Communications*, vol. 1, no. 2, pp. 3-14, Jan. 2003, doi: 10.1504/ijmc.2003.002457.

[2] M. Mannan and P.C. Oorschot, "A Protocol for Secure Public Instant Messaging", in *International Conference on Financial Cryptography and Data Security*, 2006, pp. 20-35, doi: 10.1007/11889663_2.

[3] R. Alkhulaiwi, A. Sabur, K. Aldughayem and O. Almanna, "Survey of secure anonymous peer to peer Instant Messaging protocols," in *14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 294-300, doi: 10.1109/PST.2016.7906977.

[4] C. Gloor and A. Perrig, "Trusted Introductions for Secure Messaging," in *Cambridge International Workshop on Security Protocols*, 2023, pp. 123-135, doi: 10.1007/978-3-031-43033-6_13.

[5] M.H. Eldefrawy, K. Alghathbar, M.K. Khan and H. Elkamchouchi, "Secure Instant Messaging Protocol for Centralized Communication Group," in *4th IFIP International Conference on New Technologies, Mobility and Security*, 2011, pp. 1-4, doi: 10.1109/ntms.2011.5720590.

[6] P. Bug, "Privacy hole in Windows/MSN Messenger," *Computer Fraud and Security*, vol. 2002, no. 3, pp. 1-3, Mar. 2002, doi: 10.1016/s1361-3723(02)00304-4.

[7] W. Goucher, "Shooting the messenger," *Computer Fraud and Security*, vol. 2008, no. 7, pp. 19-20, Jul. 2008, doi: 10.1016/s1361-3723(08)70115-5.

[8] D.C. Ranasinghe, "Lightweight Cryptography for Low Cost RFID," in *Networked RFID Systems and Lightweight Cryptography*, Springer, 2008, pp. 311-346, doi: 10.1007/978-3-540-71641-9_18.

[9] T.Durden, "Wikileaks Unveils Vault 7" in *The Largest Ever Publication of Confidential CIA Documents, Another Snowden Emerges*, Zerohedge, 2017.

[10] S. Osullivan, "Instant Messaging vs. instant compromise," *Network Security*, vol. 2006, no. 7, pp. 4-6, Jul. 2006, doi: 10.1016/s1353-4858(06)70408-1.

[11] N. Unger et al., "SoK: Secure Messaging," in *IEEE Symposium on Security and Privacy*, 2015, pp. 232-249, doi: 10.1109/SP.2015.22.

[12] T. Frosch et al., "How Secure is TextSecure," in *IEEE European Symposium on Security and Privacy*, 2016, pp. 457-472, doi: 10.1109/EuroSP.2016.41.

[13] S. Schr, M. Huber, D. Wind and C. Rottermanner, "When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging," in *Proceedings 1st European Workshop on Usable Security*, 2016, pp. 1-7, doi: 10.14722/eurousec.2016.23012.

[14] N. Kobeissi, K. Bhargavan and B. Blanchet, "Automated Verification for Secure Messaging Protocols and Their Implementations: A Symbolic and Computational Approach," in *IEEE European Symposium on Security and Privacy*, 2017, pp. 435-450, doi: 10.1109/EuroSP.2017.38.

[15] K. Cohn-Gordon, C. Cremers and L. Garratt, "On Post-compromise Security," in *IEEE 29th Computer Security Foundations Symposium*, 2016, pp. 164-178, doi: 10.1109/csf.2016.19.

[16] M.D. Green and I. Miers, "Forward Secure Asynchronous Messaging from Puncturable Encryption," in *IEEE Symposium on Security and Privacy*, 2015, pp. 305-320, doi: 10.1109/sp.2015.26.

[17] M. Bellare, A.C. Singh, J. Jaeger, M. Nyayapati and I. Stepanovs, "Ratcheted Encryption and Key Exchange: The Security of Messaging," in *Annual International Cryptology Conference*, 2017, pp. 619-650, doi: 10.1007/978-3-319-63697-9_21.

[18] B. Poettering and P. Rösler, "Towards Bidirectional Ratcheted Key Exchange," in *Annual International Cryptology Conference*, 2018, pp. 3-32, doi: 10.1007/978-3-319-96884-1_1.

[19] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt and D. Stebila, "A formal security analysis of the signal messaging protocol," *Journal of Cryptology*, vol. 33, pp. 1914-1983, Sep. 2020, doi: doi.org/10.1007/s00145-020-09360-1.

[20] P. Rosler, C. Mainka and J. Schwenk, "More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema," in *IEEE European Symposium on Security and Privacy*, 2018, pp. 415-429, doi: 10.1109/eurosp.2018.00036.

[21] R. Endeley, "End-to-End Encryption in Messaging Services and National Security Case of WhatsApp Messenger," *Journal of Information Security*, vol. 09, no. 1, pp. 95-99, Jan. 2018, doi: 10.4236/jis.2018.91008.

[22] T. Perrin and M. Marlinspike, "The Double Ratchet Algorithm", 2016, [online] Available: https://signal.org/docs/specifications/doubleratchet/.

[23] J. Jiang, Y. Zhu, X. Yang, J. Xu and Y. Xie, "The Research on Secure Communication Scheme Based on Double Ratchet Algorithm with Forward Secrecy for IoT Perception Layer Device," in *7th International Conference on Computer and Communication Systems*, 2022, pp. 660-664, doi: 10.1109/ICCCS55155.2022.9846271.

[24] M. Marlinspike and T. Perrin, "The X3DH key agreement protocol," 2016, [online] Available: https://whispersystems.org/docs/specifications/x3dh/.

[25] T. Perrin, “The xeddsa and vxeddsa signature schemes,” 2016, [online] Available: whispersystems.org/docs/specifications/xeddsa.
[26] P. Rogaway, “Authenticated encryption with associated data,” in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 98-107, doi: 10.1145/586110.586125.
[27] J. Chan and P. Rogaway, “On Committing Authenticated Encryption,” in *European Symposium on Research in Computer Security*, 2022, pp. 275-294, doi: 10.1007/978-3-031-17146-8_14.
[28] B.Toulas, “Signal adds quantum-resistant encryption to its E2EE messaging protocol,” 2023, [online] Available: signal.org/blog/pqxdh.
[29] N. Alnahawi et al., “SoK: Post-Quantum TLS Handshake,” 2023, [online] Available: eprint.iacr.org/2023/1873.
[30] A. Petcher and M. Campagna,, “Security of Hybrid Key Establishment using Concatenation,” 2023, [online] Available: eprint.iacr.org/2023/972.
[31] M. Barbosa et al, “X-Wing: The Hybrid KEM You've Been Looking For,” 2024, [online] Available: eprint.iacr.org/ 2024/039.

زیرنویس‌ها

[1] End-to-End Encryption
[2] Edward Snowden
[3] Mass Surveillance
[4] Instant Messaging
[5] Asynchronous
[6] End-users
[7] Impersonators
[8] Layman
[9] WikiLeaks
[10] Central Intelligence Agency (CIA)
[11] Leak
[12] Fair Share of Mass Surveillance
[13] Bleeding-Edge Applications
[14] Silent Circle Instant Messaging Protocol
[15] Malleable encryption
[16] Four message handshake
[17] SIGMA protocol paradigm
[18] Ephemeral DH shares
[19] Asymmetric ratcheting
[20] Symmetric ratcheting stage
[21] Post-compromise security
[22] Svenja Schröder
[23] Man-in-the-middle attack
[24] Kobeissi, Bhragavan and Blanchet
[25] Cohn-Gordon, Cremers and Garratt
[26] Green and Miers
[27] Bellare
[28] Poettering and Rosler
[29] Authentication
[30] Perfect forward secrecy
[31] Undeniable
[32] Synchronization
[33] Confidentiality
[34] Moxie Marlinspike and Trevor Perrin
[35] Forward secrecy or Perfect forward secrecy
[36] Backward secrecy or Future secrecy
[37] Double Ratchet Algorithm
[38] DiffieHellman key agreement

[39] Extended Triple Diffie-Hellman
[40] Key Derivation Function Chains (KDF Chains)
[41] Symmetric-key Ratchet
[42] Diffie-Hellman Ratchet
[43] Indistinguishable
[44] Resilience
[45] Forward security
[46] Break-in recovery
[47] Double Ratchet session
[48] Root chain
[49] Sending chain
[50] Receiving chain
[51] Out-of-Order
[52] Header
[53] Ping-Pong
[54] Compromised
[55] Uncompromised
[56] Advertise
[57] Figures
[58] Simplification
[59] Shared secret
[60] Initialization
[61] Skipped message keys
[62] Triggered
[63] Skipped messages
[64] Trigger
[65] Minus
[66] Asynchronous settings
[67] https://tools.ietf.org/html/rfc7748
[68] https://tools.ietf.org/html/rfc7748
[69] https://www.wikiwand.com/en/Cryptographic_hash_function
[70] Identity key
[71] Ephemeral key
[72] Signed prekey
[73] One-time prekey
[74] Long-term identity public key
[75] Single X3DH protocol run
[76] Prekey bundle
[77] Fetch
[78] Pushed
[79] Single one-time prekey
[80] Abort
[81] Byte sequence
[82] Concatenate
[83] Onetime prekey private key
[84]Post-quantum cryptography
[85]NIST
[86]Harvest now, decrypt later
[87] Key encapsulation mechanism
[88] CRYSTALS-Kyber
[89] Learning with errors
[90] Pure
[91] Hybrid
[92] Concatenation
[93] Post-Quantum Extended Diffie-Hellman