Designing Anonymous Communication System by Lattice-Based Cryptography

A. Hasani Karbasi[1], M. Alidoost Nia[2], R. Ebrahimi Atani[3*]

1- PhD Student, Mathematical Department of Guilan University
2- Master Student, Computer Department of Guilan University
3- Assistant Professor, Computer Department of Guilan University

(Reccive: 2014/04/08, Accept: 2014/11/16)

Abstract

Anonymous networks provide data confidentiality and anonymity as two important factors through the Internet. In recent years, with growing of quantum computing and also newly performed attacks, it's necessary to reform classic anonymous networks like Tor. So we need a new architecture which is quantum-resistant. In the other side, this is important to block attacks like user identity detection so we need to revise classic structures. In this paper, we propose a lattice-based architecture which includes NTRU cryptographic system and NSS digital signature. Finally, the structure of the anonymous networks has been revised according to the performance requirements and security issues. The proposed architecture should be quantum-resistant that is investigated within highly practical security analysis

Keywords:

Anonymous Networks, Performance Evaluation, NTRU Cryptography System, NSS Digital Signature

*** Corresponding Author Email:** rebrahimi@guilan.ac.ir

مجله علمی- پژوهشی «پدافند الکترونیکی و سایبری»
سال دوم، شماره ۳، پاییز ۱۳۹۳؛ ص ۲۲-۱۳

طراحی یک سامانه ارتباطات گمنام با استفاده از رمزنگاری مبتنی بر مشبکه‌ها

امیر حسنی‌کرباسی[۱]، مهران علیدوست‌نیا[۲]، رضا ابراهیمی آتانی[۳*]

۱- دانشجوی دکتری، دانشکده ریاضیات دانشگاه گیلان
۲- دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر دانشگاه گیلان
۳- استادیار، گروه مهندسی کامپیوتر دانشگاه گیلان

(دریافت: ۹۳/۰۱/۱۹، پذیرش: ۹۳/۰۷/۲۵)

چکیده

شبکه‌های گمنام برای تحقق دو عامل مهم محرمانگی داده‌ها و گمنامی کاربران در بستر شبکه اینترنت فعالیت می‌کند. در سال‌های اخیر با رشد و توسعه پردازش‌های کوانتومی و همچنین وقوع حملات جدید نیاز به اصلاح در ساختار شبکه‌های گمنام کلاسیک از جمله *TOR*، به‌وجود آمده است. از این رو نیاز به ارائه یک معماری مقاوم در برابر حملات عصر پردازش‌های کوانتومی و همچنین لزوم مقاوم‌سازی این شبکه‌ها در برابر حملات تشخیص هویت کاربران و عدم انکار، باعث شده تا معماری کلاسیک بازبینی و اصلاح شود. ما در این مقاله به ارائه معماری مبتنی بر *Lattice* و سیستم رمزنگار *NTRU* و امضای دیجیتال *NSS* پرداخته‌ایم که در نتیجه ساختار معماری شبکه‌های گمنام کلاسیک با توجه به نیازمندی‌های کارایی و آسیب‌پذیری‌های امنیتی پیش رو اصلاح شده‌اند. معماری پیشنهادی در مقابل حملات کوانتومی مقاوم بوده که به‌طور تئوری اثبات و طی یک تحلیل امنیتی جامع کاملاً عملی، بررسی شده است.

واژه‌های کلیدی: گمنامی در شبکه، ارزیابی کارایی، سیستم رمزنگار *NTRU*، امضای دیجیتال *NSS*

۱. مقدمه

با توسعه بستر اینترنت، لزوم بهره‌گیری از تکنیک‌های امنیت داده بسیار با اهمیت جلوه می‌کند. از جمله مسائل پیش‌رو در امنیت ارتباطات، بحث گمنامی است. رأی‌گیری الکترونیکی، تراکنش‌های بانکی، زیرساخت‌های رایانش ابری، تجارت الکترونیک، کنترل‌های از راه دور و استریم‌های چندرسانه‌ای تنها بخشی از کاربردهایی است که نیازمندی‌های گمنامی در بستر شبکه را ایجاب می‌کند [۱]. در فراهم کردن بسترهای گمنام، نیاز به‌وجود یک معماری امن و مطمئن الزامی بوده که یکی از پیش نیازهای ورود به حوزه گمنامی محسوب می‌شود. امنیت و صحت داده‌های مورد تبادل از آنجا اهمیت دارد که تمامی سرویس‌های نیازمند گمنامی می‌بایست از سرویس گمنام‌ساز مورد نظر استفاده کنند. وجود نقص در چنین سیستمی باعث تزلزل امنیت اطلاعات در ارتباطات همه سرویس‌های زیرمجموعه خواهد شد. طبق آخرین آمارها تا اوایل سال ۲۰۱۴ بیش از 1Gb/s از پهنای باند مصرفی برای سرویس گمنامی، به علت مشکلات امنیتی در خروجی‌های سرویس گمنام ساز تلف می‌شود [۲]. بجز معماری انتخابی برای پیاده‌سازی سرویس‌های گمنام، انتخاب و طراحی یک پروتکل امن نیز مهم به نظر می‌رسد. آنالیزهای امنیتی، در سرویس‌های گمنامی کلاسیک، بر روی حملات جدید و راهکارهای مقابله با آثار مخرب آنها متمرکز شده است [۳]. همه پارامترهای بیان شده نیازمند دید آگاهانه و امنیت محور نسبت به حوزه گمنامی در ارتباطات است.

یکی از بسترهای فراهم‌کننده گمنامی، شبکه‌های گمنام *TOR* هستند. این شبکه‌ها از یکسری گره‌های داوطلب به‌عنوان مسیریاب استفاده می‌کنند. این گره‌های داوطلب وظیفه ارسال و به اصطلاح رله داده‌ها را از یک گره به گره دیگر بر عهده دارند و فقط از ارتباطات رو به جلو بهره می‌برند. این دیدگاه رو به جلو به‌دلیل معماری خاص در طراحی شبکه‌های گمنام *TOR* است. این شبکه‌ها به‌خودی‌خود از سیستم‌های کلاسیک در رمزنگاری استفاده می‌کنند. هر چند تاکنون امنیت سطوح گمنامی در این شبکه‌ها بسیار بالا بوده و حملات موفق زیادی روی آن گزارش نشده است، اما باید گفت این معماری برای کاربردهای آینده می‌بایست بهینه‌سازی شود.

با ظهور محاسبات کوانتومی و پایه‌های متفاوت این‌گونه پردازش‌ها نسبت به سیستم‌های محاسبات کلاسیک، اولین تأثیر آن در رمزنگاری کلاسیک، شکسته شدن سیستم‌های رمزنگار مبتنی بر کلید عمومی است. این سیستم‌ها که بر اساس نظریه اطلاعات و مسائل ریاضی تجزیه اعداد ارزیابی می‌شوند، امروزه در معماری‌های پردازش کوانتومی با طول کلید تا سقف ۵۱۲ کیلوبیت به راحتی شکسته می‌شوند[۴]. این امر که آینده رمزنگاری با روش‌های کلاسیک کلید عمومی را در بستر پردازش‌های کوانتومی به خطر می‌اندازد، ما را بر آن داشته تا در معماری‌های کلاسیک کاربردی مانند *TOR* بازنگری جدی داشته باشیم و اگر بخواهیم باز هم از

* رایانامه نویسنده مسئول: rebrahimi@guilan.ac.ir

همان روش‌های کلاسیک برای تشکیل کلید در معماری *TOR* استفاده کنیم، نیاز است تا سیستم رمزنگار کلید عمومی را سنگین وزن‌تر از گذشته انتخاب نماییم. این موضوع خود مشکلات عدیده‌ای در بر دارد از جمله مهم‌ترین این مشکلات، موضوع ارتباطات بلادرنگ و ارتباطات گمنام است. برای داشتن ارتباطات بلادرنگ و انتقال اطلاعات امن و گمنام تحت شبکه لازم است که از الگوریتم‌های سبک وزن استفاده نماییم. اما امن کردن کلید عمومی فقط با سنگین‌تر کردن محاسبات آن امکان‌پذیر است.

NTRU یک سیستم رمزنگار کلید عمومی است که توسط *Hoffstein*، *Pipher* و *Silverman* در سال ۱۹۹۸ [۵] ارائه شد. *NTRU* از حلقه چندجمله‌ای‌ها با ضرایب در اعداد صحیح $\mathbb{Z}$ استفاده می‌کند. *NTRU* یک سیستم رمزنگار مبتنی بر *Lattice* بوده و امنیت آن مبتنی بر مسائل سخت ریاضی *Lattice* از جمله یافتن کوتاه‌ترین بردار (*SVP*) و یافتن نزدیکترین بردار (*CVP*) در فضای *Lattice* است.

یکی از چالش‌های *NTRU* اینست که گاهی عملیات رمزگشایی با موفقیت انجام نمی‌شود که با انتخاب صحیح پارامترها و تنظیمات اولیه مناسب می‌توان احتمال عدم موفقیت در رمزگشایی (*Decryption Failure*) را خیلی کاهش داد و به صفر رساند. از سوی دیگر *NTRU* مزایای بسیار زیادی دارد، *NTRU* برای یک پیام با طول *N*، عملیات رمزنگاری و رمزگشایی را با $O(N^2)$ عمل انجام می‌دهد که در سیستم رمزنگار *RSA* در بهترین حالت $O(N^3)$ عملیات لازم است[۵]. در جدول ۱ مقایسه کارایی و سرعت بین *NTRU*، *RSA* و *Elliptic Curve Cryptography(ECC)* در یک سیستم کامپیوتری ۸۰۰ مگاهرتز پنتیوم III نشان داده شده است.

جدول ۱. مقایسه کارایی بین *NTRU*، *RSA* و *ECC* [۱۷]

		***NTRU*-251**	***RSA*-1024**	***ECC*-163**
کلید عمومی	بیت	۲۰۰۸	۱۰۲۴	۱۶۴
کلید خصوصی	بیت	۲۵۱	۱۰۲۴	۱۶۳
بلوک متن ساده	بیت	۱۶۰	۷۰۲	۱۶۳
بلوک متن رمزشده	بیت	۲۰۰۸	۱۰۲۴	۱۶۳
سرعت رمزنگاری	بلوک بر ثانیه	۲۲۷۲۷	۱۲۸۰	۴۵۸
	مگابیت بر ثانیه	۳۶	۰.۹۰	۰.۰۷۵
سرعت رمزگشایی	بلوک بر ثانیه	۱۰۸۶۹	۱۱۰	۷۰۲
	مگابیت بر ثانیه	۱.۷	۰.۰۷۷	۰.۱۱

همچنین *NTRU* برخلاف *RSA* و *ECC* در برابر حملات محاسبات کوانتومی بسیار مقاوم است[۶]. در این مقاله به جای سیستم رمزنگار *RSA* در شبکه‌های گمنام *TOR*، سیستم رمزنگار سبک وزن و امن *NTRU* به‌کار گرفته شده است و امنیت فوق العاده آن در بخش ۳ اثبات می‌شود. *NTRU* هم اکنون در *JAVA*، *C* و *OMAP* پیاده‌سازی شده است و طول کوتاه کلیدها در آن، *NTRU* را به کاراترین سیستم رمزنگار عملی تبدیل کرده است.

امضای دیجیتال و احراز هویت کلید عمومی امن برای ارتباطات الکترونیکی، تجارت الکترونیکی و امنیت اطلاعات بسیار ارزشمند است. امضای دیجیتال فقط برای سیستم‌های کامپیوتری با محاسبات سنگین نبوده بلکه در تجهیزات سبک وزن مانند کارت‌های هوشمند، شبکه‌های بی‌سیم و ابزارهایی با محدودیت در حافظه و پردازش نیز به‌کار می‌روند. امضای دیجیتال، جامعیت داده، احراز هویت و عدم انکار را فراهم می‌کند و به همین دلیل اهمیت بسیاری دارد و تحقیقات زیادی روی آن انجام شده است، به‌عنوان مثال [۷-۱۶].

در این مقاله یک طرح امضای دیجیتال و احراز هویت سریع و امن که یک مکمل برای سیستم رمزنگار *NTRU* است و از کلیدهای عمومی و خصوصی *NTRU* استفاده می‌کند، معرفی شده است و از آن بجای توابع چکیده ساز به‌کار برده شده در *TOR* بهره گرفته می‌شود که *The NTRU Signature Scheme(NSS)* نامیده می‌شود. در جدول ۲ مقایسه کارایی الگوریتم امضاء و الگوریتم تأیید اعتبار امضاء بین *NSS*، امضای دیجیتال *RSA* و امضای دیجیتال *ECC (ECDSA)* به تصویر کشیده شده است و اثبات امنیتی آن در بخش ۴ ارائه شده است.

جدول ۲. مقایسه کارایی و سرعت بین *NSS*، امضای دیجیتال *RSA* و *ECDSA* [۱۸]

	پنتیوم	**تجهیزات سبک وزن**
الگوریتم امضای *NSS*	۰٫۳۵ میلی ثانیه	۰٫۳۳ میلی ثانیه
الگوریتم امضای *RSA*	۶۶٫۵۵ میلی ثانیه	۳۶٫۱۳ میلی ثانیه
الگوریتم امضای *ECDSA*	۱٫۱۸ میلی ثانیه	۱٫۷۹ میلی ثانیه
الگوریتم تأیید اعتبار امضای *NSS*	۰٫۲۹میلی ثانیه	۰٫۲۵ میلی ثانیه
الگوریتم تأیید اعتبار امضای *RSA*	۱٫۲۳ میلی ثانیه	۰٫۷۹ میلی ثانیه
الگوریتم تأیید اعتبار امضای *ECDSA*	۱٫۷۰ میلی ثانیه	۳٫۲۶ میلی ثانیه

ساختار این مقاله به شرح زیر است، در بخش دوم شبکه‌های کلاسیک *TOR* و روند شکل‌گیری مدار مورد مطالعه قرار گرفته است، در بخش سوم، سیستم رمزنگار *NTRU* تشریح شده و انتخاب پارامترها و تعدادی از حملات رایج بروی *NTRU* مانند حملات *Lattice* بحث شده و امنیت آن تحلیل شده است. در بخش چهارم، امضای دیجیتال *NSS* بحث شده و انتخاب پارامترها و امنیت آن تحلیل شده است. در بخش پنجم طراحی و پیاده‌سازی سیستم رمزنگار *NTRU* و امضای دیجیتال *NSS* در شبکه‌های گمنام *TOR* پیشنهاد شده است، در بخش ششم تحلیل امنیتی معماری پیشنهادی *Lattice TOR* مورد بحث و بررسی قرار گرفته است و در نهایت در بخش هفتم، جمع بندی و نتیجه‌گیری ارائه شده است.

۲. شبکه‌های کلاسیک *TOR*

در تبادل اطلاعات و ساخت مدارهای *TOR* از سه الگوریتم *RSA*، *AES* و *Diffie-Hellman* و یک الگوریتم چکیده‌ساز استفاده شده است که به‌طور خلاصه در مورد هر کدام توضیح داده می‌شود.

۲. ۱. سیستم رمزنگار *RSA*

اولین مرحله از کار توافق کلید بین گره‌هاست که بدین ترتیب جهت توزیع کلیدهای توافقی، شبکه *TOR* باید سازوکاری داشته باشد تا امنیت تبادل کلیدها در مرحله تبادل کلید حفظ شود. در تبادل کلید از الگوریتم *Diffie-Hellman* استفاده می‌شود که نصف کلید مبدأ برای توافق به مقصد ارسال می‌گردد. این نصف کلیدها با نماد g^{xi} و g^{yi} نمایش داده می‌شوند که توسط الگوریتم *RSA* رمز شده و به مقصد یعنی *OR* ارسال می‌شود. در تبادل اطلاعات به علت محدود بودن سلول‌ها نمی‌توان چکیده پیام را نیز ارسال کرد به همین علت فقط این نصف کلید به‌وسیله کلید عمومی مقصد با عنوان KP_{Kor} رمز می‌شود و در تبادل نصف کلید اول برای شروع عملیات ساخت مدار، عبارت g^x فقط به صورت $EP_{Kor}(g^x)$ رمز گردیده و ارسال می‌شود که در آن E نماینده سیستم رمزنگار *RSA* است.

۲. ۲. الگوریتم توافق کلید *Diffie-Hellman*

این الگوریتم فقط برای توافق روی کلیدهای جلسه بوده و برای اتصال هر *OP* (کاربر) با *OR*ها، می‌بایست یک کلید توافقی بین کاربر و هر مسیریاب ایجاد شود. این فرآیند این‌گونه انجام می‌گیرد که کاربر g^e یا نصف کلید را به مسیریاب ارسال کرده و پس از رمزگشایی به‌وسیله الگوریتم *RSA* قسمت دوم کلید یا g^y را به کاربر می‌فرستد و در نتیجه کلید جلسه بین کاربر و آن گره خاص ایجاد می‌گردد که $K=g^{xy}$ خواهد بود و طول عمر این کلیدها با طول عمر یک مدار برابر است. از این پس برای انتقال از هر گره به گره دیگر برای آن کاربر وجود کلیدهای جلسات الزامی است.

۲. ۳. سیستم رمزنگار *AES*

این الگوریتم به‌وسیله کلید جلسه K که توضیح داده شد، در هر لایه (یعنی در انتقال از هر مسیریاب) عملیات رمزنگاری را انجام می‌دهد. در رمزنگاری *AES* کل بسته یعنی شامل *Payload* و *Header* رمز می‌شوند و با گذر از هر لایه با داشتن کلید جلسه می‌توان رمزگشایی کرده و اصطلاحاً مسیریاب را *Pass* کرد. نکته مهم اینجاست که پس از *Pass* کردن و انتقال از هر لایه به لایه دیگر یک *circID* جدید به سلول تعلق گرفته و می‌توان ارسال را به‌طور گمنام و بدون دانستن منبع اصلی انجام داد. این نکته حائز اهمیت است که به جز ساخت مسیر اولیه، از این پس نیز با داشتن کلید جلسات گره‌های موجود، می‌توان تمام بسته‌های پیام ارسالی حاوی هر نوع داده‌ای را با این مجموعه کلید رمز نمود.

۲. ۴. روند شکل‌گیری مدار *TOR*

فرض کنید گره‌های A، B، C و D مجموعه گره‌های انتقال بوده و گره A فرستنده و گره D گیرنده نهایی باشند. برای انتقال اطلاعات می‌بایست کلیدهای جلسه $K1$ تا $K3$ بین گره A و سه گره دیگر توافق شود. در این فرآیند، هر یک از گره‌های میانی، خود یک مسیریاب محسوب می‌شوند.

کاربر (*OP*) مسیر جدید را از فهرست دریافت کرده و قسمت اول کلید را به‌وسیله کلید عمومی گره اول رمز کرده (*OR*1) و می‌فرستد. سپس *OR*1 در پاسخ، چکیده کلید جلسه $H(K1)$ و همچنین قسمت دوم کلید را می‌فرستد. تا اینجا کلید اول ($K1$) تشکیل شده است. در ادامه برای اتصال به *OR*2 باید از *OR*1 نیز عبور کند. تمام مراحلی که در قسمت قبل توضیح داده شد را باید برای *OR*2 نیز تکرار کند با این تفاوت که می‌بایست کلید $K1$ را داشته و اطلاعات ارسالی را با آن کلید، رمز کند تا بسته ارسالی به اصطلاح از *OR*1، *Pass* شده و به *OR*2 برسد. *OR*2 نیز دقیقاً عملیات مرحله قبلی را تکرار می‌کند با این تفاوت که بسته ارسالی را به جای اینکه به *OP* بفرستد به *OR*1 ارسال می‌کند و به همین صورت این بسط قابل گسترش است. لازم به ذکر است که گسترش مدارها به‌وسیله دستور *Extend* انجام می‌گیرد. پس از اینکه تمام مراحل شکل‌گیری مدار انجام گرفت، ارسال بسته‌های اطلاعاتی با پروتکل *TCP* اجرا می‌شود. نکته مهم این است که پس از تشکیل مدار و ایجاد کلیدهای K دیگر نیازی به الگوریتم‌های رمزنگاری *RSA* و *Diffie-Hellman* نیست و فقط برای تبادل اطلاعات از کلیدهای نشست K استفاده می‌شود. در شکل ۱ مراحل ایجاد یک مدار به‌طور کامل و با حداقل سه *OR* (برای ارضای شرط گمنامی در شبکه‌های میکس) بین گره‌های A و D که به اصطلاح *گره خروجی* نامیده می‌شود، نشان داده شده است. حال برای تبادل اطلاعات، مسیرها به‌وسیله *circID*های C_{AB}، C_{BC} و C_{CD} مشخص می‌گردند که به‌ترتیب هر کدام مسئول مسیریابی رو به جلو بین زوج گره‌های (A, B)، (B, C) و (C, D) هستند. برای تبادل اطلاعات از گره A به مقصد نهایی که به‌عنوان مثال می‌تواند یک وب سرور باشد دستورات زیر به ترتیب رمز شده و به مقصد ارسال می‌گردند:

Relay C_{AB} $AES_{K1}(AES_{K2}(AES_{K3}$(*Data or commands*)))
Relay C_{BC} $AES_{K2}(AES_{K3}$(*Data or commands*))
Relay C_{CD} AES_{K3}(*Data or commands*)
Decrypt and run Data or commands on last OR

داده‌ها و یا دستورات رمزگشایی شده در *OR*3 یا گره D اجرا شده و در نهایت نتایج حاصل از اجرا به شکل زیر به مبدا یا *OP* باز گردانده می‌شود:

Relay CCD AESK3(results)
Relay CBC AESK2(AESK3(results))
Relay CAB AESK1(AESK2(AESK3(results)))
Decrypt and show results on OP

۳. سیستم رمزنگار *NTRU*

در این بخش سیستم رمزنگار *NTRU* با تحلیل امنیتی آن، ارائه شده است. *NTRU* از *Convolution* حلقه چندجمله‌ای‌ها استفاده می‌کند و امنیت آن مبتنی بر مسائل سخت ریاضی است. این سیستم رمزنگار یک نمونه از سیستم‌های رمزنگاری احتمالاتی است.

۳. ۱. پارامترها

NTRU به ۴ پارامتر $(\mathcal{N}, \mathcal{P}, \mathcal{Q}, \mathcal{D})$ که اعداد صحیح هستند بستگی دارد به‌طوری که $\mathcal{N} > 1$ و عدد اول است و $(\mathcal{N},\mathcal{Q}) = (\mathcal{P},\mathcal{Q}) = 1$ و $\mathcal{Q}$ خیلی بزرگ‌تر از $\mathcal{P}$ انتخاب می‌شود ($\mathcal{Q} >> \mathcal{P}$) و $\mathcal{D}$ یک مقدار ثابت و کوچک‌تر از $\mathcal{N}$ است ($\mathcal{D} \approx \mathcal{N}/3$).

به حلقه خارج قسمتی $\mathcal{R} = \mathcal{Z}[x] / \langle x^{\mathcal{N}} - 1 \rangle$، مجموعه چندجمله‌ای‌های *Convolution* از درجه $\mathcal{N}-1$ گویند و می‌توان چندجمله‌ای‌های $\mathcal{R}$ را با بردار ضرایب آنها در $\mathcal{Z}^{\mathcal{N}}$ نشان داد. به‌عنوان مثال چندجمله‌ای $f = f_0+f_1x+\ldots+f_{\mathcal{N}-1}x^{\mathcal{N}-1} \in \mathcal{R}$ را می‌توان به شکل برداری $f = (f_0 , f_1 , \ldots , f_{\mathcal{N}-1}) \in \mathcal{Z}^{\mathcal{N}}$ نوشت. عمل جمع حلقه چندجمله‌ای‌ها جمع مؤلفه به مؤلفه بوده و مانند جمع چندجمله‌ای‌های معمولی است و عمل ضرب *Convolution* چندجمله‌ای‌های حلقه را با نماد * در حلقه $\mathcal{R}$ نشان می‌دهند که در رابطه (۱) تعریف شده است.

$$
\begin{aligned}
f(x) &:= \sum_{i=0}^{N-1} f_i x^i = [f_0, f_1, \ldots, f_{N-1}]_{1\times N} \quad , f_i \in Z \\
g(x) &:= \sum_{i=0}^{N-1} g_i x^i = [g_0, g_1, \ldots, g_{N-1}]_{1\times N} \quad , g_i \in Z \\
h(x) &:= \sum_{i=0}^{N-1} h_i x^i = [h_0, h_1, \ldots, h_{N-1}]_{1\times N} \quad , h_i \in Z \\
h_K &:= \sum_{i=0}^{K} f_i . g_{K-i} + \sum_{i=K+1}^{N-1} f_i . g_{N+K-i} = \sum_{i+j\equiv K (\mathrm{mod}\, N)} f_i . g_j
\end{aligned}
\qquad (۱)
$$

فرض کنید $\mathcal{L}_m$، $\mathcal{L}_f$، $\mathcal{L}_g$ و $\mathcal{L}_\Phi$ زیرمجموعه‌های $\mathcal{R}$ باشند که در جدول ۳ تعریف شده‌اند. همچنین فرض کنید پارامتر $\mathcal{P}$ تعریف شده باشد در این صورت اگر همه ضرایب $f \in \mathcal{R}$ به پیمانه $\mathcal{P}$ کاهش یابند گوییم چندجمله‌ای f با پیمانه $\mathcal{P}$ کاهش یافته است یعنی $f \in \mathcal{R}_\mathcal{P}$، که در آن $\mathcal{R}_\mathcal{P} = (\mathcal{Z}/\mathcal{P}\mathcal{Z})[x] / \langle x^{\mathcal{N}}-1 \rangle$. با روش مشابه $\mathcal{R}_\mathcal{Q}$ نیز به‌دست می‌آید که عمل ضرب * در $\mathcal{R}_\mathcal{P}$ و $\mathcal{R}_\mathcal{Q}$ تعریف شده است. به‌علاوه، اگر همه ضرایب f در بازه $[-\mathcal{P}/2 , \mathcal{P}/2]$ ظاهر شوند گوییم $f \in \mathcal{R}_\mathcal{P}$، *Centered lift* شده است یعنی f به حالت $f \in \mathcal{R}$ در آمده است.

۳. ۲. ساخت کلید

برای تولید کلیدهای *NTRU* ابتدا دو چندجمله‌ای $f \in \mathcal{L}_f$ و $g \in \mathcal{L}_g$ انتخاب می‌شوند. وارون چندجمله‌ای‌های $f \in \mathcal{R}_\mathcal{P}$ و $f \in \mathcal{R}_\mathcal{Q}$ با $\mathcal{F}_\mathcal{P}$ و $\mathcal{F}_\mathcal{Q}$ نشان داده می‌شوند در این صورت $\mathcal{F}_\mathcal{Q} , \mathcal{F}_\mathcal{P} \in \mathcal{R}$ با شرایط رابطه (۲) محاسبه می‌شوند.

جدول ۳. تعریف پارامترهای عمومی *NTRU*

نماد	تعریف
$\mathcal{L}_f$	$f \in \mathcal{R} \mid f$ که به تعداد $\mathcal{D}+1$ تا ضریب 1+ و $\mathcal{D}$ تا ضریب 1- دارد و بقیه ضرایب 0 هستند.
$\mathcal{L}_g$	$g \in \mathcal{R} \mid g$ که به تعداد $\mathcal{D}$ تا ضریب 1+ و $\mathcal{D}$ تا ضریب 1- دارد و بقیه ضرایب 0 هستند.
$\mathcal{L}_\Phi$	$\Phi \in \mathcal{R} \mid \Phi$ که به تعداد $\mathcal{D}$ تا ضریب 1+ و $\mathcal{D}$ تا ضریب 1- دارد و بقیه ضرایب 0 هستند.
$\mathcal{L}_m$	$m \in \mathcal{R} \mid m$ که ضرایب m به پیمانه $\mathcal{P}$ و بین $-\mathcal{P}/2$ و $\mathcal{P}/2$ انتخاب می‌شوند.

$$\mathcal{F}_\mathcal{P} * f \equiv 1 \ (mod\ \mathcal{P})$$

$$\mathcal{F}_\mathcal{Q} * f \equiv 1 \ (mod\ \mathcal{Q}) \qquad (۲)$$

لازم بذکر است که چندجمله‌ای $f \in \mathcal{L}_f$ طوری انتخاب می‌شود که وارون‌پذیر باشد، واضح است که درصورتی که وارون‌پذیر نباشد می‌توان چندجمله‌ای دیگری را که وارون‌پذیر است انتخاب کرد.

قرار می‌دهیم $\mathcal{H} = \mathcal{F}_\mathcal{Q} * g \ (mod\ \mathcal{Q})$ که کلید عمومی *NTRU* بوده و ثابت می‌شود که هم ارز عبارت $f * \mathcal{H} \equiv g \ (mod\ \mathcal{Q})$ است. همچنین پارامترهای $\mathcal{N}$، $\mathcal{P}$ و $\mathcal{Q}$ نیز عمومی هستند و کلید خصوصی *NTRU* را زوج $(f, \mathcal{F}_\mathcal{P})$ تشکیل می‌دهند.

۳. ۳. رمزنگاری

فرض کنید آلیس می‌خواهد پیام $m \in \mathcal{L}_m$ که ضرایب آن به پیمانه $\mathcal{P}$ کاهش یافته است را رمز کند. ابتدا $\Phi \in \mathcal{L}_\Phi$ را انتخاب می‌کند که یک چندجمله‌ای تصادفی بوده و نقش یک کلید یکبار مصرف را بازی می‌کند. متن رمز شده در رابطه (۳) نشان داده شده است.

$$\mathcal{E} = \mathcal{P} . \Phi * \mathcal{H} + m \ (mod\ \mathcal{Q}) \qquad (۳)$$

۳. ۴. رمزگشایی

باب در اولین مرحله رمزگشایی با ضرب *Convolution* چندجمله‌ای $\mathcal{E}$ در کلید خصوصی f محاسبات خود را شروع می‌کند که در رابطه (۴) نشان داده شده است.

$$
\begin{aligned}
\mathcal{A} &= f * \mathcal{E} \ (mod\ \mathcal{Q}) = f * (\mathcal{P} . \mathcal{H} * \Phi + m) \ (mod\ \mathcal{Q}) \\
&= \mathcal{P} . f * \mathcal{H} * \Phi + f * m \ (mod\ \mathcal{Q}) \\
&= \mathcal{P} . f * \mathcal{F}_\mathcal{Q} * g * \Phi + f * m \ (mod\ \mathcal{Q}) \\
&= \mathcal{P} . g * \Phi + f * m \ (mod\ \mathcal{Q})
\end{aligned}
\qquad (۴)
$$

در مرحله دوم، ضرایب چندجمله‌ای $\mathcal{A} \in \mathcal{R}_\mathcal{Q}$، *Centered lift* می‌شوند پس داریم $\mathcal{P} . g * \Phi + f * m \in \mathcal{R}$، حال ضرایب این چندجمله‌ای به پیمانه $\mathcal{P}$ کاهش می‌یابد که در نتیجه جمله $\mathcal{P} . g * \Phi$ حذف شده و $f * m \ (mod\ \mathcal{P})$ باقی می‌ماند. در نهایت $\mathcal{F}_\mathcal{P}$ از سمت چپ به چندجمله‌ای $f * m \ (mod\ \mathcal{P})$ ضرب شده و چند جمله ای حاصل شده *Centered lift* می‌شود که همان پیام ساده است.

نکته قابل توجه اینست که اگر $\mathcal{Q} > (6\mathcal{D}+1).\mathcal{P}$ انتخاب شود، مرحله رمزگشایی با موفقیت انجام می‌شود[۱۹]. رمزگشایی موفق بستگی به برقراری رابطه نرم $|\mathcal{P}\,.\,g * \Phi + f * m|_\infty < \mathcal{Q}$ دارد. در [۲۰] نشان داده شده است که احتمال رمزگشایی موفق با پارامترهای مختلف از رابطه (۵) به‌دست می‌آید.

$$Pr(\text{رمزگشایی موفق}) = (2\Psi(\mathcal{Q}\text{-}1/2\sigma)\text{-}1)^{\cdot} \qquad (۵)$$

که $\Psi(.)$ توزیع نرمال استاندارد است و $\cdot\sigma \approx \sqrt{\frac{36D^2}{N}+\frac{8D}{6}}$

۳. ۵. تحلیل امنیتی *NTRU*

در این بخش به حملات اصلی *NTRU* و تحلیل رمز آن می‌پردازیم. یکی از روش‌های حمله به سیستم رمزنگار *NTRU*، یافتن کلید خصوصی f و یا کلید جعلی نزدیک به f است.

۳. ۵. ۱. حمله جستجوی جامع

یکی از راه‌های یافتن کلید خصوصی یا کلید جعلی مشابه با آن، جستجوی جامع همه چندجمله‌ای‌های $f' \in \mathcal{L}_f$ است. در بخش ۳-۲ بیان شد که رابطه $f * \mathcal{H} \equiv g \pmod{\mathcal{Q}}$ برقرار است پس در یک جستجوی جامع بررسی می‌شود که $f' * \mathcal{H} \pmod{\mathcal{Q}}$ ضرایب کوچکی داشته باشد در این صورت کلید خصوصی یا یک بردار نزدیک به آن به‌دست می‌آید. به‌طور مشابه حمله گر می‌تواند همه $g' \in \mathcal{L}_g$ ممکن را آزمایش کند که $g' * \mathcal{H}^{-1} \pmod{\mathcal{Q}}$ ضرایب کوچکی داشته باشند تا کلید خصوصی یا یک بردار نزدیک به آن به‌دست آید. در نتیجه امنیت کلید بستگی به تعداد عناصر $\mathcal{L}_f$ یا $\mathcal{L}_g$ دارد.

در حالتی که چندجمله‌ای‌ها دودویی باشند ($\mathcal{P}=2$)، اندازه فضای کلید $\mathcal{L}_g$ از رابطه (۶) به‌دست می‌آید.

$$|L_g| = \binom{N}{D} = \frac{N!}{(N-D)!D!} \qquad (۶)$$

و در حالتی که چندجمله‌ای‌ها سه تایی باشند ($\mathcal{P}=3$)، اندازه فضای کلید $\mathcal{L}_g$ از رابطه (۷) به‌دست می‌آید.

$$|L_g| = \binom{N}{D}\binom{N-D}{D} = \frac{N!}{(N-2D)!(D!)^2} \qquad (۷)$$

پس انتخاب $\mathcal{P}=3$ یک انتخاب بسیار مناسب است.

۳. ۵. ۲. حملات *Lattice*

Coppersmith و *Shamir* در [۲۱] یک حمله *Lattice* بر روی کلید خصوصی *NTRU* مبتنی بر *SVP* را پیشنهاد دادند. *NTRU Lattice* استاندارد یک *Lattice* با بعد $2\mathcal{N}$ است که با نماد L^{NT} نشان داده می‌شود و توسط ماتریس پایه B^{NT} تولید می‌شود.

$$B^{NT} = \begin{bmatrix} \lambda & 0 & \dots & 0 & h_0 & h_1 & \dots & h_{N-1} \\ 0 & \lambda & \dots & 0 & h_{N-1} & h_0 & \dots & h_{N-2} \\ \dots & & & & \dots & & & \\ 0 & 0 & \dots & \lambda & h_1 & h_2 & \dots & h_0 \\ 0 & 0 & \dots & 0 & Q & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & Q & \dots & 0 \\ \dots & & & & \dots & & & \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & Q \end{bmatrix}_{2N\times 2N}$$

که در ماتریس B^{NT}، $H = \sum h_i x^i$ کلید عمومی *NTRU* بوده و λ یک ثابت غیر صفر است. روش ساده نویسی ماتریس B^{NT} به شکل زیر است:

$$B^{NT} = \begin{bmatrix} \lambda I & H \\ 0 & QI \end{bmatrix}$$

در [۱۹] اثبات شده است که بردار $(\lambda f,\ g)$ در L^{NT} قرار دارد و به احتمال زیاد کوتاه‌ترین بردارهای غیرصفر L^{NT}، $(f,\ g)$ و چرخش‌های آن هستند. در نتیجه حل مسئله *SVP* یا *apprSVP* و یافتن کوتاه‌ترین بردارها در ماتریس B^{NT} که به‌عنوان کلید رمزگشایی استفاده می‌شوند، امنیت *NTRU* را تهدید می‌کند. الگوریتم *LLL* [۱۹] می‌تواند در زمان چندجمله‌ای مسئله *apprSVP* را حل کرده و کوتاهترین بردارها را بیابد ولی برای $\mathcal{N}$ بزرگ، زمان اجرایی آن نمایی خواهد بود. همچنین الگوریتم دیگری که *BKZ-LLL* [۱۹] نام دارد، بردارهای خیلی کوتاه *Lattice* را محاسبه می‌کند ولی چون به یک پارامتر β بستگی دارد و با عامل $\beta^{2.\beta}$ مسئله *apprSVP* را حل می‌کند درنتیجه برای $\mathcal{N}$ بزرگ، زمان اجرایی آن نمایی خواهد بود.

آزمایشات متعددی ثابت کرده است که انتخاب $\mathcal{N}$ بین ۲۵۱ تا ۱۰۰۰ امنیتی معادل با امنیت پیاده‌سازی *RSA* و *ElGamal* و *ECC* دارد[۲۲] و بنابه جدول ۱ کارایی *NTRU* بهینه‌تر از *RSA* و *ECC* است. بنابراین با انتخاب صحیح پارامترها *NTRU* سبک وزن بوده و امنیت فوق‌العاده‌ای دارد در نتیجه بکارگیری *NTRU* بجای سیستم رمزنگار *RSA* در شبکه‌های گمنام بسیار بهینه‌تر و امن‌تر خواهد بود.

۴. امضای دیجیتال *NSS*

در این بخش به تشریح امضای دیجیتال مبتنی بر *NTRU* یا *The NTRU Signature Scheme(NSS)* می‌پردازیم و در نهایت نشان خواهیم داد که به‌کار بردن *NSS* بجای توابع چکیده‌ساز در روند شکل‌گیری مدار شبکه‌های گمنام *TOR* بسیار بهینه‌تر و امن‌تر است[۱۹].

در مرحله اول، آلیس پارامترهای $(\mathcal{N},\ \mathcal{Q},\ \mathcal{D})$ را مطابق بخش ۳، بطور صحیح انتخاب می‌کند تا مسائل سخت ریاضی *apprSVP* و *apprCVP* در یک *Lattice* با بعد $2\mathcal{N}$ به پیمانه $\mathcal{Q}$، برقرار شوند.

آلیس چندجمله‌ای‌های $f, g \in \mathcal{R}$ را تشکیل داده و کلید عمومی تأیید اعتبار امضاء را که در رابطه (۸) آمده است، محاسبه می‌کند.

$$\mathcal{H} \equiv \mathcal{F}_{\circ} * g \ (mod\ \mathcal{Q}) \qquad (۸)$$

لازم بذکر است که این محاسبات مشابه *NTRU* است.

۴. ۱. الگوریتم امضاء و تأیید اعتبار سند

برای امضای یک سند $D = (D_1, D_2)$، آلیس به جفت‌های (f, g) و (F, G) نیاز دارد که F و G از رابطه (۹) به‌دست می‌آیند.

$$f * G - g * F = \mathcal{Q} \qquad (۹)$$

آلیس دو چندجمله‌ای رابطه (۱۰) را محاسبه می‌کند که در این روابط منظور از $\lfloor p \rceil$ یعنی ضرایب چندجمله‌ای p به نزدیک‌ترین عدد صحیح گرد می‌شود.

$$V_1 = \lfloor (D_1 * G - D_2 * F) / \mathcal{Q} \rceil$$
$$V_2 = \lfloor (-D_1 * g + D_2 * f) / \mathcal{Q} \rceil \qquad (۱۰)$$

در نهایت آلیس امضای خود را که در رابطه (۱۱) محاسبه شده است به همراه سند D منتشر می‌کند.

$$S = V_1 * f + V_2 * F \qquad (۱۱)$$

در سمت گیرنده، باب امضای آلیس (S) و سند (D) را دریافت کرده و توسط کلید عمومی $\mathcal{H}$ رابطه (۱۲) را محاسبه می‌کند.

$$t \equiv \mathcal{H} * S \ (mod\ \mathcal{Q}) \qquad (۱۲)$$

حال باید بردار ضرایب چندجمله‌ای t به پیمانه $\mathcal{Q}$ تا جایی که امکان دارد به بردار ضرایب D_2 نزدیک باشد تا باب بتواند بررسی کند که بردار (S, t) به‌طور مناسب به بردار سند $D = (D_1, D_2)$ در فضای *Lattice* نزدیک است، در این صورت امضای آلیس تأیید اعتبار می‌شود. به این نکته نیز اشاره می‌شود که در تشکیل مشبکه، تعیین دو پارامتر p و q از اهمیت بالایی برخوردار است که در آن q یک عدد بزرگتر و p عددی کوچک‌تر خواهد بود. تفاوت NTRU و ETRU نیز در همین تعیین پارامترها است.

۴. ۲. تحلیل امنیتی *NSS*

در این بخش اثبات می‌شود که چرا *NSS* به *NTRU Lattice* وابسته است. L^{NT} دو پایه دارد، پایه خوب و خوش فرم $\begin{pmatrix} f & g \\ F & G \end{pmatrix}$ و پایه بد فرم $\begin{pmatrix} 1 & H \\ 0 & Q \end{pmatrix}$. منظور از پایه بد فرم اینست که بردارهای آن، بردارهای کوتاه در *Lattice* نیستند. آلیس می‌تواند بردارهای (D_1, D_2) را برحسب پایه خوب بنویسد که در رابطه (۱۳) این موضوع نشان داده شده است.

$$(D_1, D_2) = (u_1, u_2)\begin{pmatrix} f & g \\ F & G \end{pmatrix} \qquad (۱۳)$$

و در رابطه (۱۴) معادله رابطه (۱۳) را برای (u_1, u_2) محاسبه می‌کند.

$$(u_1,u_2) = (D_1,D_2)\begin{pmatrix} f & g \\ F & G \end{pmatrix}^{-1} = (D_1,D_2)\begin{pmatrix} G/Q & -g/Q \\ -F/Q & f/Q \end{pmatrix} \qquad (۱۴)$$

لازم بذکر است که معکوس ماتریس $\begin{pmatrix} f & g \\ F & G \end{pmatrix}$ همیشه وجود دارد زیرا بنابه رابطه (۹)، $det\begin{pmatrix} f & g \\ F & G \end{pmatrix} = \mathcal{Q}$ است.

با توجه به اینکه مختصات u_1 و u_2 اعداد صحیح نیستند، حاصلضرب $(u_1,u_2)\begin{pmatrix} f & g \\ F & G \end{pmatrix}$ در L^{NT} نیست. پس آلیس u_1 و u_2 را مانند رابطه (۱۵) به نزدیکترین عدد صحیح گرد می‌کند.

$$V_1 = \lfloor u_1 \rceil \ , \ V_2 = \lfloor u_2 \rceil \qquad (۱۵)$$

بنابراین منطقی است که بردار $(S,t) = (V_1,V_2)\begin{pmatrix} f & g \\ F & G \end{pmatrix}$ به D نزدیک باشد. در نتیجه چون $(S, t) \in L^{NT}$ است پس آلیس نیاز ندارد که جفت S و t را منتشر کند و باب می‌تواند t را به‌وسیله S و کلید عمومی $\mathcal{H}$ محاسبه کند. یعنی $\mathcal{H} * S \pmod{\mathcal{Q}}$ برابر با t است. با توجه به اینکه *NSS* نیز مشابه *NTRU* وابسته به ماتریس L^{NT} است بنابراین امنیت *NTRU* و *NSS* بستگی به محاسبه مسائل سخت ریاضی *CVP* و *SVP* دارد. در نتیجه *NSS* امنیت بسیار بالایی را فراهم می‌کند. همچنین با توجه به جدول ۲، *NSS* بسیار کاراتر و بهینه‌تر از سایر طرح‌های امضای دیجیتال است و چون هم در سیستم رمزنگار *NTRU* و هم در امضای دیجیتال *NSS* از یک کلید عمومی یکسان استفاده می‌شود و *NSS* با تابع چکیده ساز جایگزین می‌شود، حجم محاسبات در ارتباطات گمنام *TOR* به‌طور چشمگیری کاهش می‌یابد.

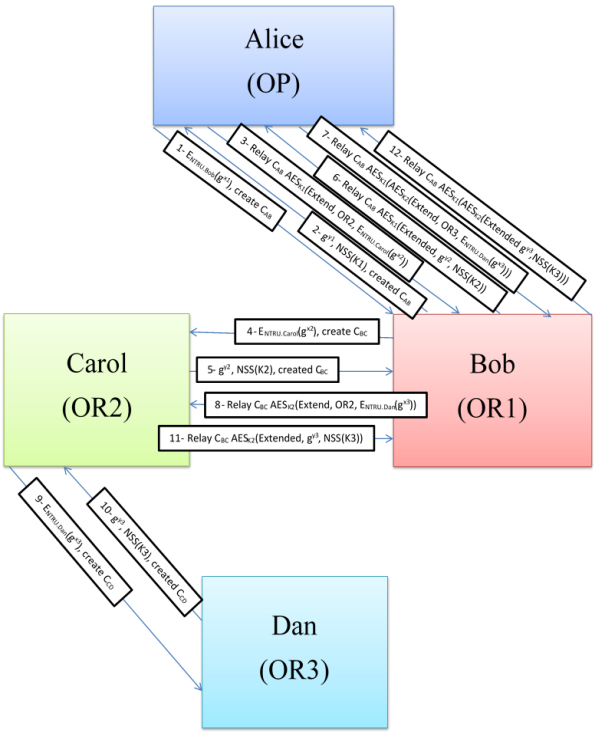
۵. پیاده‌سازی *NTRU* و *NSS* در شبکه‌های گمنام *TOR*

همان‌طور که پیش از این گفته شد، در عصر محاسبات کوانتومی، بازبینی در ساختار شبکه‌های گمنام یکی از الزامات مهم به‌شمار می‌رود. لذا برای ارتقای اصول امنیتی در شبکه‌های گمنام لازم است تا قسمت‌های آسیب‌پذیر پروتکل توزیع کلید با روش‌های نوین جایگزین گردد. در این قسمت معماری *TOR* با استفاده از پیاده‌سازی *NTRU* و امضای دیجیتال *NSS* بیان مجدد می‌شود. توزیع کلید و ارتباطات گمنام در معماری اصلاح شده طبق شکل ۱ انجام می‌پذیرد.

Alice به‌عنوان گره آغازین و ارسال‌کننده داده است که در ابتدا لازم است تا برای شروع ارتباط، کلیدهای عمومی گره‌های میانی را در دست داشته باشد تا بتواند به‌صورت لایه‌ای اطلاعات را رمز کرده و به مقصد برساند. همان‌طور که می‌دانیم سیستم رمزنگار در شبکه‌های مختلط به صورت پیازی است که معماری ابتدایی *TOR* نیز به همین شکل عمل می‌کند. لذا در این طرح بر روی لایه‌ای بودن

این معماری تأکید شده تا اصلاحات انجام گرفته، مشکلی در معماری مبنای شبکه‌های گمنام ایجاد نکند. کلیدهای *NTRU*، کلیدهای عمومی گره‌های میانی هستند و برای انتقال امن اطلاعات، شبکه حداقل باید دارای ۳ گره میانی باشد و فرض شده است که *Dan* نقطه خروج و یا *Exit Node* است. آنچه که واضح است این است که اطلاعات می‌بایست به‌صورت مرحله به مرحله ارسال شود و این ترتیب اصل مبنایی در شبکه‌های مختلط محسوب می‌شود. پس از آنکه اطلاعات مجموعه کلیدهای مسیر در اختیار *Alice* قرار گرفت، مرحله تولید کلید جلسه آغاز می‌شود. کلید جلسه برای رمزنگاری اطلاعات در همان جلسه یا نشست به‌کار می‌رود. در معماری جدید برای انتقال نیمه کلید مورد نظر در پروتکل توافق کلید *Diffie-Hellman*، لازم است تا نیمه کلید رمز شود. در این ساختار نیمه کلید اولیه توسط *NTRU* رمز شده و نیمه کلید بعدی و همچنین کلید نهایی (که در نهایت در سمت گره مقصد ایجاد می‌شود) با روش *NSS* امضا شده و به مبدا باز گردانده می‌شود. در نهایت پس از انتقال درست اطلاعات طبق مراحل دوازده گانه شکل ۱، کلیدهای $K1$ تا $K3$ تشکیل می‌شوند که همان کلیدهای جلسه گره‌های میانی به‌شمار می‌روند. با توجه به اینکه ساختار توزیع کلید *Deffie-Hellman* از سیستم هشینگ قوی برای تبادل کلید استفاده می‌کند و همچنین توافقی اتخاذ می‌گردد، در سیستم پیشنهادی تغییری نخواهد کرد. در این معماری، روش *NSS* جایگزین بسیار مناسبی برای تابع چکیده‌ساز بوده که می‌تواند با امنیت بالاتری، درستی تشکیل کلید جلسه و همچنین انتقال امن کلید را انجام دهد و به جز محرمانگی کلید، هویت دارنده کلید، هویت پیام، یکپارچگی پیام و عدم انکار در ارتباطات نیز در طرح پیشنهادی ما مشخص و قابل تمایز خواهد بود. نکته مهمی که لازم است در اینجا به آن اشاره کنیم، دلیل تمرکز ما بر روی انتقال کلید و تشکیل مجموعه کلید جلسه است. چرا که امنیت در شبکه‌های گمنام تا حد زیادی وابسته به توزیع امن کلیدهای جلسه است. پس از توزیع درست کلید، اطلاعات با پروتکل قوی رمزنگاری *AES* رمز می‌شوند و لایه‌های بیشتر در شبکه می‌تواند ضریب امنیت را به‌صورت نمایی بالا ببرد. در نتیجه تمرکز بر روی توزیع امن کلید بسیار مهم به نظر می‌رسد. در معماری پیشنهادی اشاره شد که سیستم رمزنگار *NTRU* جایگزین *RSA* شده است، بنابراین شبکه گمنام در مقابل حملات کامپیوترهای کوانتومی مقاوم می‌شود. پس با اصلاح معماری شبکه‌های گمنام در این دو مرحله، امنیت سیستم توزیع کلید ارتقا می‌یابد و همچنین امنیت انتقال اطلاعات نیز تضمین می‌شود.

حال به‌طور خلاصه مراحل دوازده گانه معماری اصلاح شده شبکه‌های گمنام را بررسی می‌کنیم. ابتدا *Alice* درخواست خود را مبنی بر ساخت کلید جلسه با *Bob* به او ارسال می‌کند. این درخواست شامل یک نیمه کلید است که توسط کلید عمومی *Bob* و با پروتکل *NTRU* رمز شده است. انتقال اطلاعات در نهایت صورت گرفته و در گره *Bob* رمزگشایی می‌شود. *Bob* در پاسخ و در مرحله ۲ کلید نهایی را تولید کرده و با روش *NSS* امضا نموده و به *Alice* ارسال می‌نماید. تا اینجا کلید جلسه $K1$ (ارتباط بین *Alice* و *Bob*) تولید می‌گردد. همین روند در مرحله ۳ توسط *Alice* اما برای توافق کلید با *Carol* انجام می‌شود. نکته مهم اینست که اطلاعات مورد نظر (یعنی نیمه کلید) توسط کلید عمومی *Carol* رمز شده و با انتقال اطلاعات از مسیر *Bob*، برای وی قابل رویت نمی‌باشد. طی مراحل ۴، ۵ و ۶ کلید جلسه $K2$ (ارتباط بین *Alice* و *Carol*) ایجاد می‌شود. در مرحله ۷ نیز نیمه کلید توافقی با *Dan* ارسال خواهد شد. توجه کنید که برای گذر از هر لایه (یعنی از *Bob* و *Carol*) یک مرحله رمزنگاری و رمزگشایی با پروتکل *AES* فراهم شده است. *Bob* با کلید $K1$ اطلاعات لایه اول را رمزگشایی کرده و می‌داند که بسته باید برای *Carol* ارسال شود اما محتویات بسته را نمی‌داند چون از کلید جلسه $K2$ اطلاعی ندارد. همچنین *Carol* با کلید جلسه $K2$ اطلاعات را رمزگشایی کرده و می‌داند بسته ای باید به *Dan* برسد. توجه داشته باشید که این تنها نمونه‌ای مدل شده از نحوه رمزنگاری لایه‌ها و پروتکل‌های استفاده شده است که تنها در دو لایه میانی به تصویر کشیده شده است چرا که برای حفظ امنیت سیستم لازم است تا این لایه‌ها حداقل به سه لایه ارتقا یابند.



شکل ۱. مراحل توزیع کلید و ارسال پیام در شبکه‌های گمنام مبتنی بر سیستم رمزنگار *NTRU* و امضای دیجیتال *NSS*. این شکل ارسال بسته داده از گره شماره ۱ (*Alice*) به گره شماره ۴ (*Dan*) را نشان می‌دهد که توسط ۲ گره میانی و با پروتکل اصلاح شده شبکه‌های گمنام انتقال صورت می‌گیرد.

پس از دریافت بسته (توافق نیمه کلید) توسط *Dan*، آخرین کلید نیز تولید شده و همین مراحل رو به عقب اجرا می‌شوند. نهایتاً در

مرحله ۱۲، کلیدهای $K1$ تا $K3$ توافق شده و می‌توان انتقال اطلاعات و بسته‌های داده را از طریق شبکه گمنام اصلاح شده آغاز کرد. توجه شود که با افزایش تعداد گره‌های مسیر ارتباطی، تنها مراحل توافق کلید بیشتر می‌شود و تغییری در ماهیت و روش‌های رمزنگاری یاد شده، انجام نخواهد شد. از نکات دیگر قابل ذکر در این معماری این است که عملیات *Create*، *Relay* و *Extend* طبق معماری کلاسیک *TOR* انجام می‌پذیرد. در یک نگاه کلی، نکته شاخص این معماری، افزایش امنیت و کارایی شبکه‌های گمنام با تکیه بر پروتکل‌های مبتنی بر *Lattice* است. در معماری *TOR* کلاسیک، امنیت بیشتر بر اساس تعداد لایه‌ها بیان می‌شد و اکثر ارزیابی‌های امنیتی بر مبنای حداقل و حداکثر لایه‌های ارتباطی مورد نیاز بود. اما ما در این معماری بر روی جنبه دیگر و تا حدی مهم تر از امنیت در گمنامی تاکید کردیم و آن امنیت در مقابل حملات پروتکلی و حملات تجزیه اعداد صحیح و آسیب‌پذیری در سیستم توزیع کلید در محاسبات‌های کوانتومی است.

۶. تحلیل امنیتی *Lattice TOR*

در عصر پردازش‌های کوانتومی، حتی مقاوم‌ترین ساختارها هم باید بازبینی ساختاری شوند. چرا که وجود کوچک‌ترین آسیب‌پذیری در مقابل فرآیندهای پردازشی، می‌تواند به ضعف کل ساختار منجر شود. در این قسمت به بررسی نمونه‌هایی از حملات شبکه‌های گمنام می‌پردازیم. اهداف این حملات بهره‌برداری اطلاعاتی از داده‌های کاربران، مشخص کردن هویت آنها، اختلال در شبکه‌های ارتباطی و نهایتاً سرقت اطلاعات است. قسمت بزرگی از این حملات با تغییر معماری و مقاوم‌سازی ساختاری رفع خواهند شد. می‌توان به این جمع‌بندی رسید که تغییرات اعمال شده در شبکه گمنام مبتنی بر *Lattice* و امضای دیجیتال یاد شده، به تکمیل این فرآیند کمک شایانی می‌نماید.

طبق اسناد منتشر شده از ادوارد اسنودن و براساس تحلیل امنیتی *Schneier*، تمامی اطلاعات کاربرانی که از شبکه گمنام *TOR* استفاده کرده‌اند، برای سرویس اطلاعاتی آمریکا قابل رویت بوده است [۲۳]. این رؤیت از طریق یک فرآیند چندگانه انجام پذیرفته که در این قسمت به بررسی آن می‌پردازیم. تاکنون ساختار *TOR* بسیار قوی به نظر می‌رسید و حمله به آن کار مشکل و تقریباً نشدنی به نظر می‌آمد. اما حملاتی که در نهایت به افشای اطلاعات این کاربران و هویت آنها منجر شد، مربوط به‌وجود باگ‌های نرم‌افزاری در بسته‌های نرم‌افزاری مربوط به مرورگرهایی از جمله فایرفاکس بود. در این حمله، داده‌ها از طریق سیستم‌های آنالیز اطلاعاتی سازمان کاوش می‌شوند:

- اولین مرحله یافتن کاربران *TOR* است. این مرحله با استفاده از بررسی داده‌های قسمت بزرگی از اینترنت انجام می‌شود. نکته مهم این است که در این بررسی‌ها یک سری الگوهای رفتاری و همیشگی *TOR* مورد بررسی قرار می‌گیرد.
- در مرحله بعد سامانه‌ای موسوم به *fingerprint* ایجاد می‌نماید که درخواست‌های *HTTP* از یک شبکه *TOR* به سمت سرور خاصی را پیدا می‌کند. این الگو باعث می‌شود تا سرورهای هدف به راحتی شناسایی شوند.
- یک سیستم مهم که تطبیق‌دهنده حملات با اهداف مورد نظر است، FoxAcid نام دارد. این سیستم حملات پیش فرض را با توجه به نوع اهداف انتخاب و کار تطبیق را به درستی انجام می‌دهد.

TOR یک محیط قابل اعتماد است اما نکته ایجاست که همیشه شروع حملات از بستر *TOR* نیست و وابستگی آن به سرویس‌هایی نظیر مرورگرها باعث آسیب‌پذیری آن می‌گردد. حملات *NSA* از طریق باگ‌های روی مرورگر فایرفاکس انجام می‌شد. البته این حملات از طریق سیستم‌های مخربی مانند *Flash* و *JavaScript* نیز امکان‌پذیر خواهد بود. سرورهای کوانتومی در بین راه وظیفه مهمی را بر عهده دارند. این سرورهای پر سرعت که بر روی ستون زیرین اینترنت و در نقاط حساس بنا شده‌اند، این قابلیت را ایجاد می‌کنند تا سرعت درخواست سرویس کاربران نسبت به سرورهای اصلی و اوریجینال افزایش یابد. در این شرایط نتایج سریع تر از سرورهای واقعی به درخواست‌کنندگان ارسال شده و در نتیجه این امر، اطلاعات می‌تواند به‌طور جعلی به کاربران ارسال شود. در اصطلاح به این حملات، حملات مرد میانی گفته می‌شود.

حملات کوانتومی دیگری نیز بر روی سیستم‌های گمنام *TOR* قابل اجرا بوده که حملات *Quantum Insert*، *Quantum Cookie* و *"degrade/deny/disrupt Tor access"* از جمله این حملات هستند و *TOR* در حالت فعلی نسبت به آنها آسیب‌پذیر است. *Quantum Insert* به تغییر مسیر داده‌ها در پاسخ به نتایج مربوط است. همچنین در بحث حملات کوانتومی مربوط به کوکی‌ها، کوکی مورد نظر به‌طور اجباری به مرورگر هدف ارسال می‌شود [۲۴].

قسمت دیگر حمله‌های عظیمی که *TOR* را مورد حمله قرار داده است مربوط به افزونه‌های سمت مرورگر است. این افزونه‌ها این قابلیت را برای مهاجمین فراهم می‌کنند که نقطه شروع حمله را مشخص نمایند. این حمله‌ها که در دسته‌بندی حملات روی شبکه‌های گمنام به حمله‌های مبتنی بر مرورگر معروف هستند، راه حل سیستماتیکی ندارند و می‌بایست در زمان استفاده از شبکه‌های گمنام تنها به ایجاد و گسترش محیط امن با غیرفعال کردن افزونه‌های یاد شده پرداخت. از جمله سایر حملاتی که می‌توان به آنها اشاره کرد، حملات *transmission-time* است. این حملات نیز که از دسته حملات *fingerprint* محسوب می‌شوند، قابلیت حمله مرد میانی را ایجاد می‌کنند. البته باید گفت قسمت بزرگی از حملات روی گره‌های خروجی اتفاق می‌افتد. این گره‌ها که نشان دهنده هویت کاربر نهایی سیستم هستند، می‌توانند توسط آنالیز داده‌های اینترنتی و نوع بسته‌های انتقالی شناسایی شوند[۲۶و۲۵].

همچنین با توجه به مشکلات موجود در حوزه رمزنگاری کلید

عمومی با الگوریتم *RSA*، دوره پردازش‌های کوانتومی مستلزم استفاده از روش‌های جایگزین رمزنگاری با الگوریتم‌های آسیب‌پذیر قبلی است. نکته مهم در این زمینه، حفظ امنیت سیستم‌های *TOR* است. همان‌طور که می‌دانیم برای انتقال کلید و توافق کلید جلسات در معماری *TOR* کلاسیک از معماری *RSA* استفاده می‌شد که با توجه به حملات کوانتومی مطرح شده به هیچ وجه نمی‌توان به این معماری اعتماد کرد. چرا که در کسری از زمان قابلیت شکستن آنها وجود دارد و می‌بایست از روش‌های معتبر دیگر بهره گرفت[۲۷]. در معماری پیشنهادی در این مقاله از طرح‌های مبتنی بر *Lattice* و سیستم رمزنگار و امضای دیجیتال مبتنی بر *NTRU* استفاده نمودیم که این روش‌ها خود در مقابل حملات کوانتومی مقاوم هستند [۲۸].

با توجه به حملات مطرح شده فوق که حملات شناخته شده در شبکه‌های گمنام بود، باید گفت که معماری پیشنهادی ما عملکرد بسیار کارا، بهینه و امنی دارد. در مقابله با حملات *NSA* و *FoxAcid*، استفاده از معماری جدید مبتنی بر *Lattice* می‌تواند الگوی جدید از تبادل داده را در شبکه اینترنت رقم بزند. این الگوی جدید خود باعث می‌شود تا ساختاری متفاوت از شبکه‌های *TOR* کلاسیک ایجاد شده و شناسایی بسته‌های ارسالی توسط کاربران شبکه‌های گمنام دشوارتر شود. پس اولین اثر مثبت شبکه‌های گمنام مبتنی بر *Lattice* و *NTRU* تغییر الگوی رفتاری در بستر شبکه اینترنت بوده و با ساختارهای موجود و کلاسیک تفاوت زیربنایی دارد.

همچنین در مقابل حملات مرد میانی می‌تواند قوی‌تر عمل کند زیرا در معماری شبکه گمنام *TOR* کلاسیک از امضای دیجیتال استفاده نمی‌شد و این امر باعث بروز مشکلاتی در اعتماد به بسته‌های ارسالی از سمت کاربران می‌شد. این امر با وجود سیستم امضای دیجیتال *NSS* ارتقای امنیتی مناسبی پیدا می‌کند تا آنجا که تبادل کلیدها نیز در شبکه با اعتماد بیشتری انجام گرفته و تصدیق کاربران با صحت و امنیت بالایی اجرا می‌شود. سیستم‌های مبتنی بر *NTRU* می‌توانند به صورت سبک وزن نیز پیاده‌سازی شوند. با توجه به اینکه میزان زمان ایجاد داده‌های رمزنگاری شده در سیستم با توزیع $4N^2+2N$ و $3N^2+27N$ به‌ترتیب برای *NTRU* و *ETRU* ارزیابی می‌شود، ممکن است سربار اجرایی سیستم تا حدی زیاد شود. البته این سربار زمانی با پشتیبانی‌های سخت افزاری قابل جبران است چرا که با توجه به ذات سیستم‌های مبتنی بر مشبکه‌ها، تمامی عملیات *ETRU* و *NTRU* به‌وسیله شیفت‌های سخت‌افزاری قابل پیاده‌سازی است و این مسئله می‌تواند بر سرعت سیستم بیفزاید. همچنین باید به این نکته توجه کرد که ورودی داده‌های خام تغییر ثابتی بر روی داده‌های رمزنگاری شده دارد. برای مثال در *NTRU* تابع خروجی رمزنگاری مبتنی بر $n[log_2q]$ است که خروجی ثابت می‌تواند به‌صورت پویا با تغییر قطعات ورودی تغییر نماید. این تغییرات به‌طور ویژه می‌بایست در معماری نرم‌افزار مورد توجه قرار گیرد.

نکته مهم و پایانی در خصوص برتری مدل امنیتی مبتنی بر *Lattice*، مقاومت آنها در برابر حملات کوانتومی است. همان طور که پیش از این نیز اشاره شد، حملات محاسبات کوانتومی می‌توانند تأثیرات مخربی بر روی سازوکار سیستم‌های رمزنگاری مبتنی بر *RSA* داشته باشند. به‌طوری که کلید به راحتی و در کسری از ثانیه، با استفاده از تکنیک‌های تجزیه اعداد قابل شکستن و شناسایی خواهد بود. لذا در این دوره وجود یک معماری مقاوم در برابر این گونه حملات می‌تواند باعث ارتقای امنیتی سیستم شود.

۷. نتیجه‌گیری

در این مقاله ابتدا به بررسی نقاط ضعف شبکه‌های گمنام کلاسیک از جمله *TOR* پرداختیم و لزوم این موضوع مشخص گردید که معماری‌های کلاسیک برای مقابله با حملات جدید می‌بایست اصلاح ساختاری شوند. یکی از بزرگ‌ترین مخاطرات عصر جدید در حوزه رمزنگاری، افزایش توان پردازشی حمله‌کنندگان از جمله حملات کوانتومی است که معماری مبتنی بر *Lattice*، *NTRU* و *NSS* برای مقابله با آن ارائه شد. در مراحل اجرایی این معماری، جزئیات جدید تبادل کلید و رمزنگاری‌های مورد نیاز اضافه شد و اثبات گردید که این معماری در مقابل حملات کوانتومی امن خواهد بود. سپس تحلیل امنیتی در مقابل حملات شایع انجام شد. به‌طور کلی می‌توان به این نتیجه رسید که در عصر پردازش‌های کوانتومی و با افزایش توان پردازشی مهاجمان، می‌بایست معماری شبکه‌های گمنام در مقابل حملات کوانتومی مقاوم باشد تا بتوانیم دو اصل محرمانگی اطلاعات و گمنامی را حفظ کنیم. معماری مبتنی بر *Lattice* علاوه بر مقاوم کردن شبکه‌های گمنام در برابر حملات کوانتومی، الگوی پردازشی و انتقال داده‌ها در بستر شبکه اینترنت را تغییر داده و با افزایش کارایی، نقش تعیین‌کننده‌ای در مقابله با حملات موجود از جمله سرورهای *NSA* و *FoxAcid* را دارد.

۸. مراجع

[1] A. Egners, D. Gatzen, A. Panchenko and U. Meyer, "Introducing SOR: SSH-based Onion Routing", in proceeding of 26th International Conference on Advanced Information Networking and Applications, Pages 280 – 286, March 2012.

[2] P. Winter and S. Lindskog. Spoiled Onions: Exposing Malicious Tor Exit Relays. Technical report, Karlstad University, 2014.

[3] B. Westermann, R. Wendolsky, L. Pimenidis and Dogan Kesdogan, "Cryptographic Protocol Analysis of AN.ON", Springer Berlin Heidelberg, volume 6052. p. 114–28, 2010.

[4] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", Society for Industrial and Applied Mathematics, Volume 26, Issue 5, Pages 1484–1509, 1997.

[5] J. Hoffstein, J. Pipher and J. H. Silverman, NTRU: A Ring-Based Public Key Cryptosystem, Algorithmic Number Theory, Lecture Notes in Computer Science 1423, pages 267-288, Springer-Verlag, 1998.

[6] J. Hoffstein, N. Howgrave-Graham, J. Pipher and W. Whyte, Practical lattice-Based cryptography: NTRUEncrypt and NTRUSign, The LLL Algorithm: Survey and Applications, pages 349-390, Information Security and Cryptography, Springer-Verlag, 2010.

[7] E.F. Brickell and K.S. McCurley. Interactive Identification and Digital Signatures, AT&T Technical Journal, November/ December, 1991, 73–86.

[8] L.C. Guillou and J.-J. Quisquater. A practical zero-knowledge protocol fitted to Security microprocessor minimizing both transmission and memory, Advances In Cryptology—Eurocrypt ’88, Lecture Notes in Computer Science 330 (C.G. G¨unther, ed.), Springer-Verlag, 1988, 123–128.

[9] J. Hoffstein, D. Lieman, J.H. Silverman, Polynomial Rings and Efficient Public Key Authentication, in Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC ’99), Hong Kong, (M. Blum and C.H. Lee, eds.), City University of Hong Kong Press.

[10] J. Hoffstein, J.H. Silverman, Polynomial Rings and Efficient Public Key Authen- tication II, in Proceedings of a Conference on Cryptography and Number Theory (CCNT ’99), (I. Shparlinski, ed.), Birkhauser.

[11] A.J. Menezes and P.C. van Oorschot and S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, 1996.

[12] T. Okamoto. Provably secure and practical identification schemes and correspond- ing signature schemes, Advances in Cryptology—Crypto ’92, Lecture Notes in Computer Science 740 (E.F. Brickell, Ed.) Springer-Verlag, 1993, 31–53.

[13] C.P. Schnorr. Efficient identification and signatures for smart cards, Advances in Cryptology—Crypto ’89, Lecture Notes in Computer Science 435 (G. Brassard, ed), Springer-Verlag, 1990, 239–251.

[14] J. Stern. A new identification scheme based on syndrome decoding, Advances in Cryptology—Crypto ’93, Lecture Notes in Computer Science 773 (D. Stinson, Ed.), Springer-Verlag, 1994, 13–21.

[15] J. Stern. Designing identification schemes with keys of short size, Advances in Cryptology—Crypto ’94, Lecture Notes in Computer Science 839 (Y.G. Desmedt, ed), Springer-Verlag, 1994, 164–173.

[16] D. Stinson, Cryptography: Theory and Practice. CRC Press, 1997.

[17] www.ntru.com.

[18] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman, and W. Whyte. "NTRU Sign: digital signature using the NTRU lattice." In Topics in cryptology-CT-RSA 2003, Vol. 2612 of Lecture Notes in compt. Sci., pp. 122-140, Springer, Berlin.

[19] J. Hoffstein, J. Pipher, J.H. Silverman, "An Introduction to mathematical cryptography." Springer-Verlag, last edition, 2008.

[20] R. Kouzmenko. "Generalization of the NTRU cryptosystem." Master's thesis, Polytechnique Montreal, Canada, 2006.

[21] D. Coppersmith and A. Shamir, Lattice Attacks on NTRU, Advances in Cryptology, EUROCRYPT '97, Lecture Notes in Computer Science 1233, pages 52-61, Springer-Verlag, 1997.

[22] NTRU Cryptosystems. Estimated breaking times for NTRU lattices. Technical report, 1999, Updated 2003. Tech. Note 012, www.ntru.com/cryptolab/tech_notes.htm.

[23] B. Schneier, “How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID”, A blog covering security and security technology, Technical Report, October 2013.

[24] SPIEGEL Staff, “Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers”, DER SPIEGEL, November 2013.

[25] Y. Zhu, X. Fu, B. Graham and R. Bettati, “Correlation-Based Traffic Analysis Attacks on Anonymity Networks”, IEEE Transactions on Parallel and Distributed Systems, Volume 21, Issue 7, Pages 954 – 967, July 2010.

[26] C. Forst, “Attacks on anonymity networks”, Selected Topics in Distributed Systems, Technical Report, Institute of Distributed Systems, Ulm University, 2013.

[27] T. Okamoto, K. Tanaka and S. Uchiyama, “Quantum Public-Key Cryptosystems”, In proceeding of CRYPTO '00 Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology, Pages 147-165, 2000.

[28] R. A. Perlner and David A. Cooper, “Quantum resistant public key cryptography: a survey”, In Proceeding of IDtrust '09 Proceedings of the 8th Symposium on Identity and Trust on the Internet, Pages 85-93, 2009.