تاریخ دریافت:۱۴۰۱/۰۱/۱۷ پژوهشنامه علوم دفاعی، شماره۱، بهار ۱۴۰۱
تاریخ پذیرش:۱۴۰۱/۰۱/۳۱ ص ص ۱۰۱ تا ۱۱۳

# تاثیر مفاهیم پایه رمزنگاری در حوزه دفاعی

آرش جوان*[۱]، جواد شرفی[۲]، حجت‌الله عبادی زاده[۳]

## چکیده

امنیت و حفاظت از اطلاعات همواره مد نظر دولت‌ها بوده و دانشمندان روش‌ها و الگوریتم‌های متنوعی را به مرور زمان ارائه نموده‌اند. در ریاضیات، از نظر شهودی، فضایی که به‌صورت آرایش منظم نقاط در فضا و زیرفضاهای برداری تشکیل می‌شود را مشبکه می‌نامیم. نظریه مشبکه‌ها کاربردهای بسیاری در علوم ریاضی، علوم رایانه مانند رمزنگاری، نظریه کدگذاری و کنترل خطا، امنیت شبکه‌ها و سیستم‌های رایانه‌ای، نظریه گروه‌ها، ترکیبی‌ات و نظریه گراف، نظریه اعداد و جبرهای لی دارند. استفاده از مشبکه‌ها در رمزنگاری مزایای فوق‌العاده‌ای فراهم کرده است. در حقیقت سامانه‌های رمزنگاری مشبکه مبنا مبتنی بر سختی مسائل ریاضی یا مسائل سخت مشبکه‌ها است که می‌توان از این سامانه‌ها در حوزه امنیت شبکه‌های دفاعی بهره برد.

**واژگان کلیدی:** رمزنگاری، علوم دفاعی، مستقل خطی، ریشه مختلط، تبدیل فوریه گسسته.

## مقدمه

مسئله اصلی روش‌های کلید عمومی، خصوصی بودن و قابلیت اعتماد به آن‌ها است. مسئله دیگر این است که این روش‌ها در مقایسه با روش‌های کلید متقارن کندترند؛ به‌همین دلیل اغلب از آن‌ها برای توافق و انتقال کلید متقارن استفاده می‌شود و داده اصلی به روش متقارن نیز منتقل می‌گردد (پیکرت،۲۰۱٤). در پروتکل‌های رمزنگاری هدف اصلی دشمن این است که پیام مخفی را بداند و اگر به این هدف برسد، آن سیستم را شکسته‌شده

۱.(*نویسندهٔ مسئول): دکتری ریاضی، دانشگاه پدافند هوایی خاتم الانبیاء (ص) آجا، دانشکده علوم پایه، تهران، ایران. ایمیل: arash.javan91@gmail.com
۲. دانشجوی دکتری رمزنگاری، دانشگاه افسری امام علی(ع)، تهران، ایران
۳. استادیار گروه ریاضی، دانشگاه افسری امام علی(ع)، تهران، ایران

می‌گویند (آجاتای، ۱۹۹۶). به‌همین دلیل الگوریتم‌های رمزنگاری برای مقاومت در برابر حملات دشمن بر اساس مسائلی که حل آن‌ها در حالت عادی غیر ممکن (سخت) است، بنا شده‌اند (رگیو، ۲۰۰۵). رمزنگاری کلید عمومی امن مبتنی بر مشبکه یکی از مفاهیم مهم رمزنگاری است که سنگ بنای بسیاری از پروتکل‌های رمزنگاری به‌خصوص علوم دفاعی و حوزه‌های نظامی را تشکیل می‌دهد (کرباسی، ۲۰۱٤).

در این بخش مقاله به دو قسمت مفاهیم جبری و حلقه چندجمله‌ای‌های کوتاه شده می‌پردازیم. که در قسمت اول به تفسیر و ارائه برخی از مفاهیم و تعاریف جبری و جبر خطی مورد نیاز به‌طور اختصار می‌پردازیم. در ادامه اولیه‌های مورد استفاده مانند ضرب در حلقه چندجمله‌ای‌ها را بیان می‌کنیم.

## مبانی نظری و پیشینه

رمزنگاری مبتنی بر مشبکه برای اولین بار در سال ۱۹۹٦ توسط آجاتای[1] ارائه شد که منجر به ارتباط میان حالت متوسط و بدترین حالت شد(پیکرت، ۲۰۱٤). سپس آجاتای و دورک[2] در مرجع (آجاتای، ۱۹۹٦) یک سیستم رمزنگاری کلید عمومی را بر اساس سختی بدترین حالت نوع خاصی از SVP به‌نام U-SVP ساختند. درسال ۱۹۹٤ شور[3] الگوریتمی برای کامپیوترهای کوانتومی ارائه کرد که توانست عوامل اول را به‌دست آورد و همچنین مسئله لگاریتم گسسته را حل نماید (رگیو، ۲۰۰۵). سامانه رمز NTRU یک سامانه رمزنگاری کلید عمومی است که توسط هافشتاین[4] ، پیفر[5] و سیلورمن[6] ارائه شد (لاگ لویس، ۲۰۱۵). حال می‌توانیم کاربرد و برخی مفاهیم پایه رمزنگاری در امنیت شبکه‌های علوم دفاعی و نظامی را در ذیل مشاهده کنیم.

1 Ajatai
2 Dwork
3 Shor
4 Hoffistein
5 Pipher
6 Silverman

تعریف: فرض کنید S یک مجموعه دلخواه باشد. هر نگاشت از مجموعه $S \times S$ در S را یک عمل دوتایی روی مجموعه S می‌نامیم.

تعریف: هرگاه G مجموعه‌ای ناتهی از اشیا و + عمل دوتایی روی اعضای G باشد، آنگاه در صورت برقراری ویژگی‌های زیر، دو تایی (G,+) را گروه می‌نامیم و آن‌را به تسامع با G نمایش می‌دهیم.

- G نسبت به عمل جمع بسته باشد، یعنی به ازای هر $a.b \in G$ نتیجه بگیریم $a+b \in G$
- عمل جمع روی G شرکت پذیر باشد، یعنی به ازای هر $a.b.c \in G$ داشته باشیم $(a+b)+c = a+(b+c)$
- G دارای عنصر همانی باشد، یعنی عنصری مانند 0 وجود داشته باشد به‌طوری‌که برای هر $a \in G$ داشته باشیم $a+0 = 0+a = a$
- هر عضو G دارای وارون باشد، یعنی برای هر $a \in G$ عنصری مانند $b \in G$ وجود داشته باشد به‌طوری‌که $a+b = b+a = 0$ ( که آن‌را با نماد a– نشان می‌دهیم).

همچنین هرگاه $a.b \in G$ باشند به‌قسمی‌که $a+b = b+a$، آنگاه G گروه جابجایی (آبلی) است.

مثال و تعریف: $(\mathbb{Z},+)$ مجموعه اعداد صحیح به همراه عمل جمع معمولی اعداد نیز گروه آبلی است. $\mathbb{Z}_n = \{[0],[1],\dots,[n-1]\}$ (که در آن n عدد صحیح مثبت است و $[a]_n = \{a+kn : k \in \mathbb{Z}\}$ ) با جمع به پیمانه n تشکیل یک گروه می‌دهد( عضو همانی [0] و وارون عضو i ، [n-i] عضو است). حال مجموعه $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$ (گروه ضربی به پیمانه n) را در نظر بگیرید. برای هر عضو $a \in \mathbb{Z}_n^*$ مرتبه a نسبت به پیمانه n یعنی کوچک‌ترین عدد صحیح مثبت k طوری‌که $a^k \equiv 1 \bmod n$ و به‌صورت $ord_n(a)$ نمایش می‌دهیم. یک ریشه اولیه در پیمانه n، عنصری مانند a است اگروفقط اگر $ord_n(a) = |\mathbb{Z}_n^*|$ . یعنی همه اعضای گروه را می‌توان به‌صورت توانی از a نوشت( $|\mathbb{Z}_n^*|$ اندازه مجموعه $\mathbb{Z}_n^*$ را مشخص می‌کند). می‌توان نشان داد که اگر p یک عدد اول باشد، $\mathbb{Z}_p$ یک گروه دوری از مرتبه p-1 است و حداقل یک ریشه اولیه دارد.

تعریف: هرگاه R مجموعه‌ای ناتهی از اشیا ، + و* اعمال دوتایی روی اعضای مجموعه R باشد، آنگاه در صورت برقراری ویژگی‌های زیر سه تایی $(R,+,*)$ را حلقه می‌نامیم و آن‌را به تسامع با نماد R نمایش می‌دهیم.

- $(R,+)$ گروه آبلی باشد.
- $(R,+)$ بسته و شرکت پذیر باشد( یعنی نیم‌گروه باشد).
- عمل ضرب(*) نسبت به جمع(+) روی مجموعه R دارای خاصیت توزیع پذیری (پخشی) باشد، یعنی به ازای هر $a.b.c \in R$ داشته باشیم

$$a*(b+c)=a*b+a*c \ . \ (b+c)*a=b*c+b*a$$

اصطلاحا عمل اول را عمل جمع و همل دوم را عمل ضرب حلقه می‌نامیم. عضو همانی نسبت به عمل جمع را با نماد 0 و عضو همانی نسبت به عمل ضرب را با نماد 1 نمایش می‌دهیم.

هرگاه برای هر $a.b \in R$ داشته باشیم $a*b=b*a$ ،آنگاه حلقه R را حلقه جابجایی می‌گویند. همچنین حلقه R را حلقه یک‌دار می‌نامند هرگاه شامل عنصر همانی نسبت به عمل ضرب باشد.

تعریف: اگر R حلقه‌ای یک‌دار باشد، عناصر معکوس پذیر یا یکال R، عناصری از حلقه R هستند که نسبت به عمل ضرب دارای وارون باشند. مجوعه عناصر یکال R را با U(R) نمایش می‌دهیم. می‌گوییم $0 \neq a \in R$ مقسوم علیه صفر است، هرگاه عنصر ناصفر $b \in R$ وجود داشته باشد به‌قسمی‌که $a*b=b*a=0$

تعریف: حلقه یک‌دار R که هر عضو ناصفر آن دارای وارون ضربی باشد را حلقه بخشی(تقسیم) می‌نامیم.

تعریف: حلقه جابجایی و یک‌دار D را دامنه صحیح می‌نامیم، هرگاه حلقه D فاقد مقسوم علیه صفر باشد. همچنین حلقه تقسیم جابجایی (حلقه جابجایی و یک‌دارF که هر عضو ناصفر آن دارای وارون ضربی باشد) F را میدان می‌گوییم.

گزاره: فرض کنید R یک حلقه و S زیرمجموعه ناتهی از R باشد. در این‌صورت S زیرحلقه R است اگر وتنها اگر

$i)\forall a,b\in S;\ a-b\in S \qquad ii)\forall a,b\in S\ ;a*b\in S$

تعریف: فرض کنید R یک حلقه و I زیرمجموعه ناتهی از R باشد. در این‌صورت I ایدآل R است اگروتنهااگر

$i)\forall a,b\in I;\ a-b\in I \qquad ii)\forall a\in I,\ \forall r\in R\ ;a*r\in I,\ r*a\in I$

توضیح و گزاره: می‌دانیم که اگر I یک ایدآل از حلقه R باشد، آنگاه I زیرگروه جمعی گروه آبلی R بوده، در نتیجه I در R نرمال است. بنابراین مجموعه هم‌دسته‌های $\frac{R}{I}=\{r+I\,|r\in R\}$ با عمل $(a+I)+(b+I)=(a+b)+I$ یک گروه آبلی است. به‌راحتی می‌توان ملاحظه کرد که عمل ضرب $(a+I)*(b+I)=a*b+I$ روی $\frac{R}{I}$ خوش تعریف است. در این‌صورت با اعمال جمع و ضرب تعریف شده تشکیل یک حلقه می‌دهد که آن‌را حلقه خارج قسمتی می‌نامیم.

تعریف: هرگاه R یک حلقه باشد و (M,+) گروه آبلی باشد. همچنین عمل ضرب اسکالر $\cdot:\ R\times M\longrightarrow M$ باشد، آنگاه گروه آبلی M را یک R–مدول می‌گوییم هرگاه به ازای هر $r,r'\in R$ و $m,m'\in M$ داشته باشیم

- $r\cdot(m+m')=r\cdot m+r\cdot m'$
- $(r+r')\cdot m=r\cdot m+r\cdot m'$
- $(r*r')\cdot m=r\cdot(r'\cdot m)$
- (اگر حلقه یک‌دار باشد این شرط اضافه می‌شود) $1\cdot m=m$

تعریف: گروه آبلی $(V,+)$ روی میدان F را فضای برداری می‌گوییم هرگاه به ازای هر $\alpha,\beta\in V$ و $c,c'\in F$ داشته باشیم :

- $1\cdot\alpha=\alpha$
- $(c*c')\cdot\alpha=c\cdot(c'\cdot\alpha)$
- $c\cdot(\alpha+\beta)=c\cdot\alpha+c\cdot\beta$
- $(c+c')\cdot\alpha=c\cdot\alpha+c'\cdot\alpha$

در واقع می‌توان گفت که فضای برداری همان مدول با اسکالرهایی از میدان است. یعنی

هر فضای برداری یک مدول است ولی هر مدولی لزوما فضای برداری نیست.

تعریف: به مجموعه بردارهای $v_1, v_2, \dots, v_k \in V$ مستقل خطی گفته می‌شود هرگاه تنها جواب معادله $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0$ این باشد که $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$ . اگر معادله فوق حداقل با یک غیر صفر، برقرار شود مجموعه وابسته خطی گفته می‌شود.

تعریف: فرض کنید $b_1, b_2, \dots, b_n \in \mathbb{R}^m$ ، n بردار مستقل خطی باشند به‌طوری‌که $m \geq n$. مجموعه تمام ترکیبات خطی حقیقی این بردارها، فضای تولید شده را تشکیل می‌دهند و آن‌را به شکل زیر نمایش می‌دهیم.

$$\text{span}(b_1, b_2, \dots, b_n) = \{ \sum_{i=1}^{n} c_i b_i : c_i \in \mathbb{R}, \forall\, i = 1,2, \dots, n \}$$

تعریف: فرض کنید V فضای برداری روی میدان F باشد. هر زیرمجموعه مستقل خطی از V، که فضای V را تولید کند، پایه فضای برداری V می‌نامیم. به بیان ریاضی، مجموعه مستقل خطی $\{b_i\}_{i \in N}$ پایه V است، هرگاه $V = \{\sum_{i=1}^{n} c_i b_i \ : \ c_i \in F\}$ .

همواره یک پایه برای فضای برداری V وجود دارد. هر دو پایه دلخواه از فضای برداری V ، دارای تعداد عناصر یکسانی هستند. به تعداد عناصر موجود در هر پایه V، بعد فضای برداری V گفته می‌شود.

به‌عنوان مثال $(\mathbb{R}^n, +)$ فضای برداری با پایه استاندارد $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ است.

هرگاه $\beta = \{b_1, b_2, \dots, b_n\}$ پایه V باشد، هر $v \in V$ را می‌توان به‌صورت منحصر به فرد به شکل $v = c_1 b_1 + c_2 b_2 + \cdots + c_n b_n$ نوشت. در این‌صورت $(c_1, c_2, \dots, c_n)$ را مختصات v می‌گویند و این نمایش منحصر به فرد است.

نکته: R–مدول M را آزاد می‌گوییم هرگاه دارای پایه باشد.

## روش شناسی تحقیق

در این روش ما ریشه‌های مختلط واحد را محاسبه می‌کنیم. در این تحقیق می‌خواهیم ریشه n ام یک عدد مختلط را توضیح داده‌ایم که در تبدیل NTT از آن استفاده شده است و

از این تبدیل در بیشتر چندجمله‌ای‌ها استفاده شده است.

تعریف: ریشه n ام مختلط عدد یک(واحد)، عدد مختلط $\omega$ است به‌طوری‌که $\omega^n = 1$.

تعداد ریشه‌های n ام مختلط عدد یک دقیقا برابر n است. به ازای $k = 0,1,\dots,n-1$ این ریشه‌ها برابرند با $e^{\frac{2k\pi i}{n}}$ که طبق تعاریف، e به توان یک عدد مختلط $i\theta$ برابر است با $e^{i\theta} = cos\theta + isin\theta$.

به‌عنوان مثال ریشه‌های هشتم مختلط عدد یک عبارتند از $\omega_8^8 = \omega_8^0, \omega_8^1, \omega_8^2, \dots, \omega_8^7$.

تعریف: به مقدار $\omega_n = e^{\frac{2\pi i}{n}}$ ریشه n ام اصلی عدد یک[1] می‌گویند و بقیه ریشه‌ها توان‌هایی طبیعی از $\omega_n$ هستند.

n ریشه n ام مختلط عدد یک، یعنی $\omega_n^0, \omega_n^1, \dots, \omega_n^{n-1}$ ، یک گروه تحت عمل ضرب تشکیل می‌دهند که این گروه ساختار یکسانی با گروه جمعی $(\mathbb{Z}_n, +)$ به پیمانه n دارد، چون $\omega_n^0 = \omega_n^n = 1$ دلالت بر $\omega_n^j \omega_n^k = \omega_n^{j+k} = \omega_n^{j+k \bmod n}$ دارد. به‌طور مشابه $\omega_n^{-1} = \omega_n^{n-1}$. خواص و ویژگی‌های دیگر ریشه‌های n ام مختلط عدد یک در لم‌های بعدی بررسی می‌شود.

تعریف: n–امین ریشه واحد (به ازای $n \in \mathbb{Z}$ ) برابر با عدد مختلط $\omega$ است به‌طوری‌که $\omega^n = 1$ . همچنین n–امین ریشه واحد، اولیه است هرگاه به ازای هر $k < n$ داشته باشیم $\omega^k \neq 1$ .

لم حذف: به ازای اعداد صحیح $n \geq 0$ ، $k \geq 0$ و $d > 0$ داریم: $\omega_{nd}^{kd} = \omega_n^k$.

اثبات: $\omega_{nd}^{kd} = \left(e^{\frac{2\pi i}{nd}}\right)^{kd} = \left(e^{\frac{2\pi i}{n}}\right)^{k} = \omega_n^k$.

نتیجه: به ازای هر عدد صحیح زوج $n > 0$ داریم: $\omega_n^{\frac{n}{2}} = \omega_2 = -1$.

اثبات: $\omega_2 = e^{\frac{2\pi i}{2}} = e^{\pi i} = cos\,\pi + i\,sin\,\pi = -1$.

لم تنصیف: اگر عددی زوج و مثبت باشد، آنگاه مجذورات n ریشه n ام مختلط عدد

[1] The principal n th root of unity

یک، k ریشه k ام مختلط عدد یک خواهند بود.

اثبات: طبق لم حذف می‌دانیم $(\omega_n^k)^2 = \omega_{\frac{n}{2}}^k$ . توجه داشته باشید که اگر تمام ریشه‌های n ام مختلط عدد یک را به توان ۲ برسانیم، آنگاه هر ریشه $\frac{n}{2}$ ام مختلط عدد یک دقیقا دو بار به‌دست می‌آید. زیرا

$$\left(\omega_n^{k+\frac{n}{2}}\right)^2 = \omega_n^{2k+n} = \omega_n^{2k}\omega_n^n = \omega_n^{2k} = (\omega_n^k)^2 .$$

تعریف: اگر $\sum_{i=0}^{n-1} \omega^{ik} = 0$ باشد، آنگاه $\omega$ را ریشه اصلی[1] عدد یک می‌نامیم.

نکته: هر ریشه اولیه از واحد در میدان‌های متناهی یک ریشه اصلی از عدد یک است. در این تحقیق چون حلقه خارج قسمتی نیز میدان متناهی است، لذا هر ریشه اولیه واحد یک ریشه اصلی واحد نیز محسوب می‌شود. همچنین برای n امین ریشه اصای از واحد می‌دانیم که $\omega^{k+\frac{n}{2}} = -\omega^k$ که به این خاصیت، انعکاسی می‌گویند.

لم جمع: به ازای هر عدد صحیح $n \geq 1$ و عدد صحیح نامنفی j، اگر n، j را نشمارد (یعنی j مضربی از n نباشد) داریم: $\sum_{k=0}^{n-1}\left(\omega_n^j\right)^k = 0$.

ویژگی کاهش: اگر $\psi$ ریشه دوم عدد یک باشد، آنگاه$\psi^2 = \omega$ یک ریشه n ام عدد یک است.

اثبات: رابطه جمع جملات یک سری هندسی در مورد اعداد مختلط نیز به‌کار می‌رود و لذا حکم برقرار می‌گردد.

$$\sum_{k=0}^{n-1}\left(\omega_n^j\right)^k = \frac{\left(\omega_n^j\right)^n - 1}{\omega_n^j - 1} = \frac{(\omega_n^n)^j - 1}{\omega_n^j - 1} = \frac{(1)^j - 1}{\omega_n^j - 1} = 0.$$

## تبدیل فوریه گسسته[2](DFT)

به خاطر بیاورید که می‌خواستیم چندجمله‌ای $a(x) = \sum_{i=0}^{n-1} a_i x^i$ از درجه n را در نقاط $\omega_n^0, \omega_n^1, \dots, \omega_n^{n-1}$ ارزیابی می‌کنیم. فرض می‌کنیم n توانی از ۲ باشد، چون اگر n بدین

[1] Pricipal
[2] Discrete Fourier Transform

صورت نیز نباشد به‌راحتی می‌توان با اضافه کردن ضرایب صفر در توان‌های بالا، درجه چندجمله‌ای را به‌شکل توان ۲ درآورد. با فرض اینکه چندجمله‌ای a نمایش با بردار داده شده باشد، یعنی به فرم$a = (a_0, a_1, \dots, a_{n-1})$ . به ازای $k = 0,1,2, \dots, n-1$ به شکل زیر تعریف می‌شود:

$$y_k = a(\omega_n^k) = \sum_{i=0}^{n-1} a_i \omega_n^{ik}$$

بردار $y = (y_0, y_1, \dots, y_{n-1})$ ، تبدیل فوریه گسسته بردار a نامیده می‌شود و آن‌را با نماد $y = DFT_n(a)$ نیز نشان می‌دهیم. نمایش ماتریسی بردار y به شکل زیر است.

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega^{n-1} \\ 1 & \omega^2 & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \dots & \omega^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

می‌توان بردار$y_k$ را به شکل $y_k = a_0 + a_1\omega + a_2\omega^{2k} + \cdots + a_{n-1}\omega^{(n-1)k}$ نیز نمایش داد. معکوس این عنصر به فرم $a_k = n^{-1}\sum_{i=0}^{n-1} y_i\ \omega^{-ik} \quad s.t\ i \in \{0,1,2, \dots, n-1\}$ است.حال معکوس تبدیل فوریه گسسته که با $DFT^{-1}$ نشان داده می‌شود و نمایش ماتریسی آن به‌صورت زیر است.

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix} = n^{-1} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega^{-1} & \dots & \omega^{1-n} \\ 1 & \omega^{-2} & \dots & \omega^{2-2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{1-n} & \dots & \omega^{(1-n)(n-1)} \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{n-1} \end{pmatrix}$$

برای محاسبه ضرب دو چندجمله‌ای $c = ab$ به‌صورت $\mathrm{c} = \mathrm{DFT}^{-1}(\mathrm{DFT(a)} \circ \mathrm{DFT(b)})$ عمل می‌کنیم. حال تبدیل NTT حالت خاصی از تبدیل DFT است که بردارهای آن در میدان متناهی است و ضرب دو چندجمله‌ای که در آن $a, b \in R_q$ به‌فرم $\mathrm{c} = \mathrm{NTT}^{-1}(\mathrm{NTT(a)} \circ \mathrm{NTT(b)})$ صورت می‌گیرد. $c = ab$ یادآوردی می‌کنیم که n امین ریشه اولیه از واحد وجود دارد درصورتی‌که $n|q-1$. به‌خاطر همین دلیل است که کوچک‌ترین عددی که در ویژگی $q \equiv 1 \bmod n$ با n=1024 صدق

می‌کند برابر $q = 12289$ است.

## یافته‌های تحقیق( حلقه چندجمله‌ای‌های کوتاه شده)

در ادامه این بخش رده‌ی خاصی از حلقه‌های خارج قسمتی چندجمله‌ای که در سیستم رمزنگاری برای امنیت حوزه‌های دفاعی به‌کار رفته‌اند، مورد بررسی یافته‌های تحقیق ما هستند که مورد مطالعه قرار می‌گیرند (رگیو، ۲۰۰۵).

تعریف: با در اختیار داشتن عدد طبیعی N، حلقه‌ی چند جمله‌ای‌های کوتاه شده از مرتبه‌ی N ( که حلقه‌ی چندجمله‌ای‌های پیچشی نیز گفته می‌شود) توسط حلقه‌ی خارج قسمتی رابطه‌ی زیر تعریف می‌شود:

$$R = \frac{\mathbb{Z}[x]}{x^N + 1}$$

به‌طور مشابه، حلقه‌ی چندجمله‌ای‌های پیچشی (به پیمانه q)، حلقه‌ی خارج قسمتی زیر است:

$$R_q = \frac{\left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)[x]}{x^N + 1}$$

هر عنصر از $R$ یا $R_q$ نمایشی یکتا به‌صورت زیر دارد ( با ضرایبی به ترتیب از $\mathbb{Z}$ و $\mathbb{Z}/q\mathbb{Z}$ ):

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$$

نشان داده می‌شود که محاسبات در حلقه‌ی $R$ یا $R_q$ ساده‌تر از محاسبات در حلقه‌های چندجمله‌ای عمومی است و این هم به خاطر وجود پیمانه‌ی چندجمله‌ای $x^N + 1$ است. وقتی که عملیات به پیمانه‌ی $x^N + 1$ انجام می‌شود، کافی است جملات $x^N$ تبدیل به $-1$ شود. پس در هر جمله‌ای که حاوی $x^N$ بود آن $x^N$ با $-1$ تعویض می‌شود؛ برای مثال در جمله‌ی $x^K$ هنگامی که $k = iN + j$ و $0 \leq j < N$ باشد، داریم:

$$x^k = x^{iN+j} = (x^N)^i x^j = (-1)^i x^j$$

## نتیجه‌گیری

به‌طور خلاصه می‌توان نتیجه گرفت که توان جملات چندجمله‌ای‌ها در این حلقه به پیمانه N کاهش داده می‌شوند و این خاصیت حلقه‌های چندجمله‌ای کوتاه شده است. همچنین از این چندجمله‌ای‌ها می‌توان در امنیت شبکه‌های حوزه‌ها و علوم دفاعی نیز بهره برد.

اغلب به‌منظور سادگی، چندجمله‌ای $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{N-1}x^{N-1} \in \mathbb{R}$ با برداری از ضرایبش به‌صورت $(a_0, a_1, a_2, \dots, a_{N-1}) \in \mathbb{Z}^N$ نشان داده می‌شود. در مورد چندجمله‌ای‌های $R_q$ نیز به همین شیوه عمل می‌کنیم.

جمع چندجمله‌ای‌ها در R ،مطابق با جمع معمولی بردارهاست:

$$a(x) + b(x) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_{N-1} + b_{N-1})$$

قاعده‌ی ضرب در R (که به آن ضرب پیچشی گفته می‌شود) به دلیل وجود پیمانه‌ی $x^N + 1$ اندکی پیچیده‌تر از ضرب معمولی بردارهاست. برای نشان دادن عملگر ضرب در حلقه‌های R و $R_q$ از نماد ⊛ استفاده شده است تا از ضرب معمولی قابل تشخیص باشد.

گزاره: ضرب دو چندجمله‌ای $a(x),b(x) \in R$ از طریق رابطه زیر به‌دست می‌آید:

$$a(x) * b(x) = c(x) \qquad : \qquad c_k = \sum_{i+j \equiv (mod\ N)} a_i b_j$$

که در آن مجموعی که تعریف کننده $c_k$ است، روی تمام i و j هایی که بین 0 و N-1 هستند با شرط $i+j \equiv k \pmod N$ کار می‌کند. ضرب دو چندجمله‌ای $a(x),b(x) \in R_q$ نیز توسط رابطه فوق محاسبه می‌شود، با این تفاوت که مقدار $c_k$ به پیمانه‌ی q کاهش می‌یابد.

نگاشتی طبیعی از R به $R_q$ وجود دارد که در آن ضرایب یک چندجمله‌ای به پیمانه‌ی q کاهش داده می‌شود. این نگاشت کاهش به پیمانه‌ی q دو خاصیت زیر را به همراه دارد:

$$(a(x) + b(x)) mod\ q = (a(x) mod\ q) + (b(x) mod\ q)$$
$$(a(x) * b(x)) mod\ q = (a(x) mod\ q) * (b(x) mod\ q)$$

(به زبان ریاضی نگاشت $R \rightarrow R_q$ یک همریختی حلقه‌ای است).

تعریف: فرض کنید $a(x) \in R_q$ باشد، چندجمله‌ای مرکزگرای $a(x)$، $a'(x) \in R$ است به‌طوری‌که داشته باشیم:

$$a'(x) mod\ q = a(x) \quad \text{s.t} \quad -\frac{q}{2} < a_i' \leq \frac{q}{2}$$

برای مثال اگر q=2 باشد، مرکزگرای a(x) یک چندجمله‌ای دودویی است.

تعریف: فرض کنید $a(x) \in R$ باشد، چندجمله‌ای $b(x) \in R$ معکوس ضربی $a(x)$ است اگر $a(x) * b(x) = 1$.

وقتی q اول باشد با استفاده از الگوریتم بسط یافته‌ی اقلیدسی برای چندجمله‌ای ها می‌توان مشخص کرد که کدام یک دارای معکوس بوده و چگونه می‌توان معکوس آن‌ها را در $R_q$ محاسبه کرد.

گزاره: فرض کنید q یک عدد اول باشد، آنگاه $a(x) \in R_q$ یک معکوس ضربی دارد اگر و تنها اگر:

$$in\ (\frac{\mathbb{Z}}{q\mathbb{Z}})[x] \gcd(a(x), x^N + 1) = 1$$

## پیشنهادها

در انتهای این تحقیق پیشنهاد می‌شود در سامانه‌های رمزنگاری و شبکه‌های علوم دفاعی از این ضرب و حلقه چند جمله‌ای‌ها نهایت استفاده را کرد. برای این‌کار با توجه به مطالب و مفروضات فوق می‌توان در علوم دفاعی این حلقه‌های چندجمله‌ای را با در نظر گرفتن یک عدد صحیح $N \geq 1$ و دو پیمانه‌ی p وq آغاز می‌شود. همچنین فرض کنید حلقه‌های R، $R_q$ و $R_p$ حلقه‌های چندجمله‌ای کوتاه شده به شکل زیر هستند :

$$R = \frac{\mathbb{Z}[x]}{x^N + 1} \quad , \quad R_q = \frac{(\frac{\mathbb{Z}}{q\mathbb{Z}})[x]}{x^N + 1} \quad , \quad R_p = \frac{(\frac{\mathbb{Z}}{p\mathbb{Z}})[x]}{x^N + 1}$$

همان‌طور که اشاره شد، می‌توان یک چندجمله‌ای $a(x) \in R$ را با کاهش به پیمانه‌ی p یا q به عضوی از $R_p$ یا $R_q$ تبدیل کرد. در جهت عکس، برای تبدیل چندجمله‌ای‌ها از $R_p$ یا $R_q$ به R از مرکزگرای آن‌ها استفاده می‌شود. مفروضات متعددی در این سامانه‌ها برای

استفاده در حوزه‌های دفاعی مورد استفاده قرار می‌گیرد. در مورد پارامترهای N،p وq می‌توان متغیرهای مفروض را به فرمی تعریف کرد که، N باید عددی اول باشد و $\gcd(N,q)= \gcd(p,q) = 1$ .

## فهرست منابع


Ajtai. M, Generating hard instances of lattice problems (extended abstract), in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing Philadelphia, Pennsylvania, United States: ACM (1996).

Bos. J, Ducas. L, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, and D. Stehlé. CRYSTALS – Kyberc: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy, EuroS&P (2018).

Bos. J. W, Costello. C, M. Naehrig, D. Stebila, Post-quantum key exchange for the tls protocol from the ring learning with errors problem. In 2015 IEEE Symposium on Security and Privacy. pp. 553–570 (May 2015).

Z. Eslamai, Coding Theory, Printing and publishing center of shahid beheshti University Of Tehran (2008).

Z. Genç, A; V. Iovino & A. Rial, The Simplest Protocol for Oblivious Transfer" Revisited, IACR Cryptology ePrint Archive (2017).

Hauck. E & Loss. J; Efficient and Universally Composable Protocols for Oblivious Transfer from the CDH Assumption. IACR Cryptology ePrint Archive (2017).

Hoffistein, J. Pipher and J.H. Silverman, An Introduction to Mathematical Cryptography, Springer-Verlag, 1 st edition (2008).

Hoffistein. J, Howgrave-Graham, J. Pipher and W. Whyte, Practical Lattic-Based Cryptography: NTRUEncrypt and NTRUSign, the LLL Algorithm: Survey and Applications, Informations Security and Cryptography Book, Springer-Verlag (2010).

Langlois. A and Stehlé. D, Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 75(3):565–599 (2015).

National Institute of Standards and Technology. FIPS PUB 202 – SHA-3 standard: Permutation-based hash and extendable-output functions (2015).

Peikert, C, Lattice Cryptography for the Internet, pp 197–219. Springer International Publishing, Cham (2014).