امضای دیجیتال مقاوم کوانتومی بر اساس همسانی های بین خم های سوپرسینگولار

مصطفی قربانی

استاد راهنما: دکتر حسن دقیق

رمزنگاری دانشی است که به بررسی و شناخت اصول و روش‌های انتقال یا ذخیره‌ی اطلاعات به صورت امن (حتی اگر مسیر انتقال اطلاعات و کانال‌های ارتباطی یا محل ذخیره اطلاعات ناامن باشند) می‌پردازد.

رمزنگاری استفاده از تکنیک‌های ریاضی برای برقراری امنیت اطلاعات است. در اصل رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشد و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد نتواند به اطلاعات دسترسی پیدا کند. دانش رمزنگاری بر پایه مقدمات بسیاری از قبیل نظریه اعداد ، نظریه گروه‌ها ، آمار ، الگوریتم و پیچیدگی محاسبات بنا شده است.

موارد متعددی از اطلاعات حساس که نباید در دسترس دیگران قرار گیرد ، وجود دارند. این گونه اطلاعات جهت حفاظت باید رمزنگاری گردند. این اطلاعات شامل مواردی همچون اطلاعات کارت اعتباری ، اطلاعات حساس در یک سازمان ، اطلاعات مربوط به حساب‌های بانکی ، مخفی بودن رای در رای‌گیری الکترونیکی و .. می‌باشند.

معادل رمزنگاری در زبان انگلیسی، کلمه Cryptography است، که برگرفته از لغات یونانی Kryptos به مفهوم محرمانه و gráphien به معنای نوشتن است.

به طور کلی سیستم رمزنگاری به دو دسته کلی تقسیم می‌شود:

- رمزنگاری متقارن یا کلید خصوصی
- رمزنگاری نامتقارن یا کلید عمومی

در رمزنگاری متقارن ، رمزنگاری و رمزگشایی اطلاعات با کلیدی مشابه صورت می‌گیرد و این کلید باید بین طرفین ارتباط توافق شده باشد. ولی در رمزنگاری نامتقارن کلید رمزگذاری و رمزگشایی متفاوت است، در واقع از دو کلید عمومی و خصوصی مجزا برای رمزنگاری و رمزگشایی استفاده می‌شود.

امنیت بیشتر سیستم های رمزنگاری کلید عمومی که امروزه استفاده می‌شود بر اساس مسائل سخت ریاضیاتی همچون مساله تجزیه اعداد و لگاریتم گسسته می‌باشد. با این حال کامپیوترهای کوانتومی قادر خواهند بود این دو مساله سخت در کامپیوترهای کلاسیک را به طور موثری حل کنند که تهدیدی جدی برای رمزنگاری مدرن خواهد بود.

رمزنگاری پساکوانتومی ، مطالعه سیستم های رمزنگاری کلاسیک می‌باشد که در برابر حملات کوانتومی ایمن باقی می‌مانند. تاکنون چندین سیستم پیشنهادی برای رمزنگاری پسا کوانتومی کاندید شده اند ، از جمله سیستم‌های رمزنگاری معرفی شده می‌توان به رمزنگاری مشبکه مبنا ، کد مبنا ، هش مبنا و همین طور رمزنگاری چندمتغیره اشاره کرد.
اخیرا سیستم رمزنگاری بر اساس همسانی های بین خم های سوپرسینگولار توسط جائو و همکارانش معرفی شده است که این سیستم رمزنگاری شامل پروتکل تبادل کلید ، اثبات دانش صفر هویت و همچنین رمزنگاری کلید عمومی می‌باشد. همسانی ها به دلیل اندازه کلید کوچک و همچنین پیاده سازی موثر آن جز کاندیدهای تبادل کلید پسا کوانتومی می‌باشند.
چندین طرح احراز هویت بر مبنای همسانی ها ارائه شده است که ما در این پایان نامه قصد داریم به بررسی طرح امضای دیجیتال که قویا غیرقابل جعل در برابر حمله متن انتخاب شده در مدل اوراکل تصادفی کوانتومی هستند بپردازیم. طرح امضای معرفی شده ، بوسیله اجرای یک انتقال عمومی اثبات دانش صفر هویت به دست می‌آید. در سیستم های کلاسیک (قدیمی) رمزنگاری ، امنیت امضای دیجیتال از طریق اثبات دانش صفر تعاملی با اعمال مدل انتقالی فیات‌ـشمیر قابل پیاده سازی بود. اما برای امنیت درمدل های کوانتومی نیاز به طرحی جدید نیاز شد که به تازگی مدل انتقال آنره ارائه شده است که ما برای طرح پیشنهادی خود از این مدل استفاده خواهیم کرد.

رمزنگاری همسانی‌ـ مبنا

با داشتن دو خم بیضوی E_1 و E_2 در میدان متناهی F_q با مرتبه q ، یک همسانی ϕ عبارت است از یک نگاشت جبری از خم بیضوی E_1 به خم بیضوی E_2 که

$$\phi(x,y) = \left(\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)}\right)$$

چنان که $\phi(\infty) = \infty$. (f_1, f_2, g_1, g_2 چندجمله ای های دو متغیره و ∞ عنصر همانی روی خم بیضوی می‌باشد).دو خم بیضوی E_1 و E_2 را روی $\mathbb{F}_q$ همسان گوییم اگر و تنها اگر یک همسانی بین آنها وجود داشته باشد. قضیه ای معروف به قضیه تیت بیان می کند دو خم E_1 و E_2 همسان هستند اگر و تنها اگر :

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$$

با داشتن یک همسانی $\phi : E_1 \to E_2$ از درجه n ، همسانی $\hat{\phi} : E_2 \to E_1$ از درجه n وجود خواهد داشت که :

$$\phi o\hat{\phi} = \hat{\phi} o\phi = [n]$$

که $[n]$ یک نگاشت چندبرابر کردن و همسانی $\hat{\phi}$ دوگان همسانی ϕ می‌باشد.
برای هر عدد طبیعی n ، زیرگروه $E[n]$ را به صورت زیر معرفی می‌کنیم :

$$E[n] = \{P \in E(\bar{\mathbb{F}}_q) : nP = \infty\}$$

به عبارت دیگر ، $E[n]$ هسته نگاشت n برابر کردن بستار جبری $\bar{\mathbb{F}}_q$ روی میدان $\mathbb{F}_q$ می‌باشد. گروه $E[n]$ با گروه $(\mathbb{Z}/n\mathbb{Z})^2$ (که n و q نسبت به هم اول اند) یکریخت می‌باشد.
حلقه درون ریختی $End(E)$ را مجموعه ای از تمام همسانی ها از خم E به خودش روی بستار جبری $\bar{\mathbb{F}}_q$ از میدان $\mathbb{F}$ می‌نامیم. حلقه درون ریختی همراه با عمل جمع گروه و عمل ترکیب تشکیل یک گروه می‌دهد. اگر $dim_{\mathbb{Z}}(End(E)) = 2$ باشد آنگاه خم بیضوی E را یک خم معمولی گوییم و اگر $dim_{\mathbb{Z}}(End(E)) = 4$ آنگاه خم بیضوی E را سوپرسینگولار می نامیم. دو خم بیضوی همسان، یا هر دو معمولی اند یا هر دو سوپرسینگولار هستند.

گراف همسانی

یک گراف ℓ ـ همسانی گرافی است که راس های آن خم های بیضوی همریخت و بین دو خم E_1 و E_2 یک یال وجود دارد اگر وتنها اگر یک ℓ ـ همسانی بین این دو خم وجود داشته باشد. در خم های سوپرسینگولار ، گراف ℓ ـ همسانی گراف متصل است. با داشتن دو راس متفاوت از این گراف پیدا کردن مسیری با اندازه ثابت یک مسئله سخت منظور می‌شود که این سختی مسئله در طراحی سیستم های رمزنگاری همسانی مبنا مورد استفاده قرار می‌گیرد.

اثبات دانش صفر

برای بیان مفهوم اثبات دانش صفر لازم است دو شخصیت را معرفی کنیم ، از این رو پگی را به عنوان یک اثبات کننده و ویکتور را به عنوان یک تاییدکننده در نظر می‌گیریم. به طور رسمی ، یک سیستم اثبات دانش صفر یک رویه است که طی آن پگی ، ویکتور را متقاعد می‌کند که به یک حقیقت معین اشراف دارد بطوریکه هیچ اطلاعات اضافی نسبت به دانش خود در اختیار ویکتور

قرار نمی‌دهد تا خود ویکتور نتواند به عنوان یک مدعی دیگران را متقاعد کند که به حقیقت مورد بحث اشراف دارد.در نگاه اول این طور به نظر می‌رسد که با داشتن سیستم های رمزنگاری موجود هیچ شانسی برای ارائه این چالش وجود ندارد. برای مثال پگی (در نیویورک) چگونه می‌تواند ویکتور (در کالیفرنیا) را متقاعد سازد که رنگ خانه اش قرمز است بدون اینکه عکسی از خانه خود برای ویکتور ارسال کند؟ و همچنین اگر پگی عکس خانه خود را برای ویکتور ارسال کند آنگاه ویکتور این قابلیت را خواهد داشت که به دیگران اثبات کند که رنگ خانه پگی را می‌داند!

امضای دیجیتال

امضای دیجیتال نوعی رمزنگاری نامتقارن است. هنگامی که پیغامی از کانالی ناامن ارسال می‌شود، یک امضای دیجیتال که به شکل صحیح به انجام رسیده باشد می‌تواند برای شخص گیرنده پیام دلیلی باشد تا ادعای شخص فرستنده را باور کند یا به عبارت بهتر شخص گیرنده از طریق امضای دیجیتال می‌تواند این اطمینان را حاصل کند که همان شخص فرستنده، نامه را امضا کرده است و نامه جعلی نیست.

امضاهای دیجیتال در بسیاری از جنبه‌ها مشابه امضاهای سنتی دستی هستند؛انجام امضاهای دیجیتال به شکل صحیح بسیار مشکل تر از یک امضای دستی است. هر کاربر در امضای دیجیتال دو کلید دارد، کلید خصوصی که تنها در اختیار خودش است و کلید عمومی که در دست همه است. هر فرد برای امضای یک پیام، آن را با استفاده از کلید خصوصی خود امضا می‌کند و بررسی صحت امضای وی با استفاده از کلید عمومی‌اش برای هر فرد دیگری امکان‌پذیر است.

بر اساس نیازهای مختلف ، امضاهای دیجیتال متنوعی پا به عرصه وجود گذاشته‌اند. یکی از این نوع امضاها ، امضای دیجیتال غیرقابل انکار می‌باشد به این معنی که در فرایند تاییدسازی امضا، خود امضاکننده نیز باید مشارکت داشته باشد. این امضا اولین بار توسط شوام در سال ۱۹۸۹ معرفی شده است. از دیگر امضاهای پرکاربرد می‌توان به امضای کور اشاره کرد که در سال ۱۹۸۲ اولین بار توسط شوام معرفی شد. یک طرح امضای کور، پروتکلی است که به کاربر اجازه می‌دهد امضای معتبری برای پیام خود به دست آورد، بدون اینکه محتوای پیام برای امضاکننده آشکار شود. از کاربردهای این نوع امضا می‌توان به رای‌گیری الکترونیکی و همچنین پول الکترونیکی اشاره کرد.