وزارت علوم، تحقیقات و فناوری

دانشگاه تفرش

دانشکده ریاضی

پایان‌نامه کارشناسی ارشد

تحلیلی بر طرح تقسیم راز بصری در رمزنگاری

نگارش

مهدی حسامی‌فرد

استاد راهنما

دکتر سمانه مشهدی

بهمن ۱۳۹۰


بسم الله الرحمن الرحيم

دانشگاه تفرش

دانشکده ریاضی

رساله کارشناسی ارشد

تحلیلی بر طرح تقسیم راز بصری در رمزنگاری

دانشجو

مهدی حسامی‌فرد

استاد راهنما

دکتر سمانه مشهدی

در کمال احترام

با عشقی سرشار از محبت

تقدیم به

پدر و مادر مهربانم

سپاس گزاری

«سپاس خداوندگار حکیم را که با الطاف بی کران خود آدمی را به زیور عقل آراست.»

در آغاز وظیفه خود می دانم از راهنمایی ها و تلاش های خالصانه استادگران قدر سرکار خانم دکتر سمانه مشهدی که در تهیه و تنظیم این پایان نامه به این جانب کمک های فراوانی نموده اند، نهایت تشکر و قدردانی را بنمایم.

«و تقدیر و تشکر از همه کسانی که به نحوی در انجام و ارایه این پژوهش مرا یاری نموده اند.»

چکیده

طرح تقسیم راز بصری تکنیکی در رمزنگاری است که بشر در آن با بکارگیری از سیستم بینایی (بصری) خود به راحتی و بدون استفاده از هیچ محاسبه ریاضی از ماهیت تصویر رمز شده (که می تواند یک عکس، یک یاد داشت، یا یک دست نوشته باشد) مطلع می‌شود.

در یک طرح تقسیم راز بصری $(k,n) - VSS$ راز می‌تواند قابل دیدن باشد اگر kتا یا بیشتر از سهم‌ها در دسترس باشند. همانطور که می‌دانیم هر تصویر از پیکسل‌های متعددی تشکیل شده است و در واقع کدگذاری روی تک‌تک پیکسل‌ها انجام می‌گیرد. طرح مورد بحث از این جهت اهمیت دارد که در آن شخص استفاده کننده احتیاج به هیچ محاسبه ریاضی ندارد، بطور مثال چند فرمانده نظامی تنها با در دست داشتن سهم خود که یک صفحه شفاف است و قرار دادن آن روی سهم‌های مجاز دیگر به راحتی می‌توانند از اطلاعات تصویر (که ممکن است یک گذرواژه نهفته در تصویر و یا یک دستور نظامی از مافوق باشد) مطلع شوند.

در طرح تقسیم راز بصری (که ما آن را برای سادگی طرح VSS می‌نویسیم) به طور معمول تلاش برای بدست‌آوردن همسنجی بالا (معیاری برای اندازه‌گیری کیفیت تصویراصلی نسبت به تصویر بازسازی شده) است. ما در این پایان‌نامه طرح VSS احتمالی را برای تصاویر سیاه و سفید و تصاویر مقیاس خاکستری و تصاویر رنگی، ارایه خواهیم نمود.

کلمات کلیدی:

تقسیم راز بصری ، رمزنگاری بصری ، سهم، تصویر محرمانه ، تفاوت نسبت ، همسنجی

فهرست مطالب

پیش‌گفتار

طرح تقسیم راز بصری [۱] یک تکنیک در رمزنگاری است که در آن بشر از سیستم بینایی خود برای بازسازی تصاویر محرمانه استفاده می‌کند و هیچ محاسبه ریاضی برای بازسازی تصویر رمز شده لازم نیست.

بحث کلی طرح تقسیم راز بصری بسط پیکسل است. ما نیز در این پایان‌نامه قصد داریم طرح تقسیم راز بصری احتمالی عمومی (k, n) را برای تصاویر سیاه و سفید و سطح خاکستری [۲] و نیز برای تصاویر رنگی ارایه کنیم. در دو اخیر طرح بسط پیکسل توسط کاربر تعیین می‌شود . بسط پیکسل ۱ به منزله این است که هیچ بسط پیکسلی نخواهیم داشت. کیفیت تصاویر بازسازی شده محرمانه که با میانگین همسنجی [۳] (میانگین تفاوت نسبی) اندازه گیری می‌شود برابر همسنجی طرح تقسیم راز بصری غیراحتمالی توسعه یافته است. طرح‌های تقسیم راز بصری احتمالی قبلی برای تصاویر سیاه و سفید و تنها برای مقادیر خاصی مطرح شده بود، که ما آن‌ها را نیز بررسی خواهیم کرد .

طرح‌های تقسیم راز بصری برای رمز کردن یک تصویر محرمانه به n صفحه شفاف که هر صفحه را یک سهم می‌گوییم، مطرح شد. در طرح تقسیم راز بصری (k, n) ، تصویر رمزشده می‌تواند وقتی که k تا از n سهم یا بیشتر موجود باشد بازسازی و قابل دیدن شود. هر پیکسل در تصویر محرمانه به mزیر پیکسل در هر سهم گسترش پیدا می‌کند. در فرایند بازسازی، پشته سازی [۴] زیرپیکسل، یک عملگر بولی OR است. طرح VSS ابتدا برای تصاویر سیاه و سفید(باینری) توسط نائور [۵] و شمیر [۶] [۱۴] مطرح شد. بر اساس همان تعریف، ورهول [۷] و وان تیل بورگ [۸] [۱۹] تعریف های عمومی بیشتری بدست آوردند.

بر اساس طرح سیاه و سفید، دو طرح که یکی، طرح تقسیم راز بصری برای تصاویر سطح خاکستری و ما

---

[۱] visual secret sharing scheme

[۲] grey-scale

[۳] average contrast

[۴] stack

[۵] Naor

[۶] Shamir

[۷] Verheul

[۸] Van Tilborg

آن را به اختصار $(GVSS)$ می‌نامیم [۱، ۱۱، ۱۳] با بسط پیکسل m_g و دیگری طرح VSS برای تصاویر رنگی که به اختصار $(CVSS)$ نامیده می‌شود با گسترش پیکسل m_c در [۹، ۲۵] ارایه شده است. همه این طرح ها غیراحتمالی هستند، چون که هر پیکسل در تصویر محرمانه می تواند کاملا" از نو بازسازی شود. اما هر سهم m بار بزرگتر از سهم اولی است، بنابراین برای پیاده سازی ممکن است به مشکل پیاده‌سازی برخورد کنیم. برای حل مسئله‌ی بسط پیکسل ایتو [۹] و همکارانش [۱۲] ابتدا یک روند جدید برای رمزکردن تصویر سیاه و سفید نسبت به سهم هایی با اندازه برابر برای تصویر محرمانه ارئه داد.

یانگ [۱۰] [۲۳] یک طرح VSS احتمالی زیبا برای تصاویر باینری بدون بسط پیکسل ارایه کرد. فضای کوچک به جای پیکسل‌های منحصر بفرد از تصاویر محرمانه می تواند بطور صحیح بازسازی شود. طرح $Prob.VSS$ یانگ دارای تراز همسنجی برابر با طرح VSS معمولی است. حجم فضای تشخیص در [۲۳] آنالیز شده است. سیماتو و همکارانش [۸] مدل باینری $Prob.VSS$ [۲۳] را گسترش دادند بطوریکه $m \geq 1$ می‌پذیرد و رابطه بین طرح‌های احتمالی و غیراحتمالی را مطرح می‌کند. هسو [۱۱] و همکارانش از مفهوم احتمال [۱۰] برای ساختن یک مدل بهینه برای ساختار دسترسی کلی استفاده کرد.

یانگ و چن [۲۴] یک چهارچوب مطمئن معرفی کردند که در آن پیکسل‌ها را با بسط پیکسل‌های متفاوت برای استفاده‌های کاربردی مورد استفاده قرار می‌دهند بنابراین تمام طرح‌های VSS حاضر [۸، ۱۰، ۱۲، ۲۲، ۲۳] برای تصاویر باینری هستند.

وانگ و همکارانش [۲۱] طرح تقسیم راز احتمالی $(2, n)$ را برای تصاویر باینری بر مبنی عملگرهای بولین XOR و AND معرفی کردند. طرح تقسیم راز باینری $(2, n) - Prob.VSS$ به طرح $(2, n)$ تصویر خاکستری و رنگی تعمیم داده شده است. این طرح‌ها در منابع [۳، ۴، ۱۸، ۲۲] طرح VSS نیستند و از آنها بطور مستقیم برای ساختن یک طرح تقسیم راز با عملگر XOR استفاده می‌شود. چن و همکارانش [۵] یک تراز ضربی طرح (n, n) بدون بسط اندازه تصویر مبنی بر ماتریس‌های پایه طرح با استفاده از عملگر

[۹] R. Ito

[۱۰] Yang

[۱۱] Hsu

XOR برای بازسازی تصاویر محرمانه مطرح کردند. وانگ [۱۲] و همکارانش [۲۰] طرح $(n,n)-VSS$ برای تصویر سطح خاکستری بر اساس نتایجی از [۲۱] معرفی کردند. تسای [۱۳] [۱۷] یک طرح تقسیم راز بصری (n,n) برای تصاویر رنگی واقعی با اندازه های محدود، از طریق ترکیب شبکه‌های عصبی و VSS متغیر مطرح کرد. از نظر بصری کیفیت تصویر محرمانه و تصاویر استثمار شده همانند تصایر اصلی هستند. در این پایان نامه ما سه طرح VSS احتمالی، یکی برای تصاویر سیاه و سفید و برای تصاویر سطح خاکستری و دیگری برای تصاویر رنگی مورد بررسی قرار می‌دهیم، بطوریکه در آن همانند [۸] بسط پیکسل می‌تواند مجموعه‌ای از مقادیر خاص m که $m \geq 1$ باشد، جزئیات اندازه‌ی فضای قابل تشخیص آن در [۲۳] آنالیز شده است.

جدول ۱ طرح پیشنهاد شده و طرح‌های مربوطه را لیست کرده است. در این جدول و دیگر جاهای پایان‌نامه اندازه بسط پیکسل و نوع تصویر محرمانه را در عنوان طرح می‌گنجانیم تا طرح‌ها بسادگی مشخص شوند.

	طرح $Prob.VSS$[۲۳]	طرح $Prob.VSS$[۸]	طرح $Prob.GVSS$	طرح $Prob.CVSS$
نوع تصویر	سیاه و سفید	سیاه و سفید	مقیاس خاکستری	رنگی
بسط پیکسل	۱	$1,\ldots,m$	$1,\ldots,m_g$	$1,\ldots,m_c$
اندازه ناحیه	آنالیز شده	آنالیز نشده	آنالیز شده	آنالیز شده
میانگین همسنجی	α	محاسبه معادله	$\alpha^{(i+1,i)}, i=0,\ldots,g-2$	$\alpha^{(i+1,i)}, i=0,\ldots,g-2$

جدول ۱

توجه کنید که از این به بعد در این پایان نامه، g عدد تمایز تراز خاکستری تصویر محرمانه، c عدد تمایز رنگ ها در تصاویر محرمانه است پارامتر های m و m_g و m_c ، به ترتیب اندازه بسط پیکسل برای پایه‌ی باینری طرح VSS، تصویر خاکستری طرح $GVSS$ ، تصویر رنگی طرح $CVSS$ هستند. کیفیت تصویر بازسازی شده محرمانه، با همسنجی اندازه گیری می‌شود، که تفاوت نسبی بین ترازهای خاکستری پشت سر هم (متوالی)است. جزئیات بیشتر در بخش های دیگر بیان خواهد شد. در فصل ۱ این پایان نامه مقدمات

[۱۲] Wang

[۱۳] Tsai

ابتدایی و تعاریف اصلی را ارایه می دهیم و در فصل ۲ طرح تقسیم راز بصری غیراحتمالی و احتمالی را برای تصاویر باینری ارایه می‌دهیم و فضای تشخیص آن را مورد برررسی قرار می‌دهیم. در فصل ۳ طرح VSS احتمالی ما را برای تصاویر مقیاس خاکستری مهیا می کند، آنالیز اندازه فضای تشخیص برای این طرح نیز در همین فصل صورت می‌گیرد. در فصل ۴ ما شیوه‌ای برای تصاویر رنگی ارایه می‌دهیم و آنالیز اندازه فضای شناخته‌شده برای طرح $CVSS$ را بررسی خواهیم کرد. سرانجام در فصل آخر نتیجه گیری را خواهیم داشت. در جدول ۱ مقدار α همسنجی طرح VSS سیاه و سفید غیراحتمالی است. مقدار $\alpha^{(i+1,i)}$ همسنجی بین i ام و $i+1$ امین تراز -خاکستری طرح $GVSS$ غیراحتمالی است. $(i = 1, \cdots g-1)$. مقدار $(i = 1, \cdots c-1)\alpha^{(i,i)}$ همسنجی رنگ بازسازی شده i در یک طرح $CVSS$ غیراحتمالی است. در منبع [۲۳] ، اندیس α نشان دهنده میانگین همسنجی طرح VSS است و مقدار بسط پیکسل آن برابر با ۱ می باشد.

فصل ۱

مقدمه‌ای بر رمزنگاری

۱.۱ مقدمه

اگر بخواهیم اطلاعات مهمی را بین چند شخص در یک محیط نظامی یا غیر نظامی رد و بدل کنیم، بطوری که اشخاص دیگر پی به محتویات نوشته‌ی ما نبرند باید آن را طوری تغییر دهیم که اگر اشخاص دیگر محتویات نوشته‌ی ما را در دست داشتند، توانایی آشکار کردن اطلاعات را نداشته باشند. بنابراین هرچقدر شیوه‌ی ما برای رمزنگاری قوی تر باشد، امکان این که اطلاعات ما آشکار شود کمتر است. یک شیوه‌ی معروف و مطلوب آن، استفاده از الگوریتم های ریاضی است، بطوریکه هر چه این الگوریتم‌ها پیچیده‌تر باشد، ما در حفظ کردن اطلاعات موفق‌تر خواهیم بود. امروزه با توجه به اینکه از طریق محیط‌های مجازی اطلاعات محرمانه زیادی رد و بدل می‌شود و خطر فاش شدنشان توسط کاربرهای این گونه محیط‌ها همیشه وجود دارد، توجه همگان به سمت رمزنگاری اطلاعات معطوف شده است.

۲.۱ رمزنگاری چیست؟

اگر داده‌ی اطلاعات خود را به روشی خاص و محرمانه تغییر دهیم، بگونه‌ای که بجز افراد محدود که مجاز به دانستن این اطلاعات هستند دیگر افراد نتوانند آن را باز گشایی کنند، در اینصورت ما از تکنیک رمزنگاری استفاده کرده ایم. ابتدا یادآوری می‌کنیم که نباید کدگذاری را با رمزنگاری اشتباه بگیریم. زیرا در کد گذاری بطور معمول دارای علایم محدود و قراردادی استفاده می‌کنیم، منظور از قراردادی این است که بطور مثال، در پیام‌های تلگرافی مورس ما از کدگذاری‌هایی عمومی استفاده می‌کنیم و شخصی که کار با این وسیله ارتباطی را بداند به راحتی می‌تواند متن فرستاده شده را تبدیل کرده و از محتویات آن باخبر شود، در حالی که در رمزنگاری در صورت رعایت کردن امنیت شخص غیرمجاز حتی اگر اطلاعات را دریافت کند، قادر به بازگشایی متن رمز شده نمی‌باشد.

۳.۱ طرح تقسیم راز

با توجه به اینکه اکثر اطلاعات امروزه بصورت الکترنیکی بین چند نفر منتقل می‌شوند و نیز به علت استفاده از سیستم های کامپیوتری، امنیت و پیچیدگی آن از جایگاه ویژه‌ای برخوردار است. بنابراین یک راه بسیار امن استفاده از یک کلید مشارکتی است بطوری که تنها تعداد خاصی از افراد مجاز با روش‌های خاص بتوانند کلمه عبور را بازسازی کنند. طرح تقسیم راز روشی است برای توزیع یک راز در بین مجموعه‌ای از سهام‌داران به طوری که تنها زیرمجموعه‌های مجاز قادر به بازسازی راز باشند راز باشند در حالی که زیرمجموعه‌های غیر مجاز نتوانند هیچ گونه اطلاعاتی از راز به دست آورند . به مثال زیر توجه نمایید : فرض کنید کشوری دارای چندین پایگاه موشکی است، حال اگر کلمه فعال‌سازی آن در دست فردی خاص مثلا فرمانده کل باشد، در این صورت اگر در مواقع ضروری برای فرمانده مشکلی پیش آید، دیگر قادر به فعال سازی آن نمی شوند، از طرفی کلمه عبور را نمی توان بدست فرد دیگری داد، زیرا ممکن است افراد رده پایین‌تر دچار لغزش شوند. یک روش امن این است که تعدادی مشخص که دارای سهم مشخص شده ای هستند، با قرار دادن سهم‌های خود قادر به باز سازی کد عبور باشند. مثلا اگر فرمانده نباشد، سه فرد رده بالا بتوانند فقط با مشارکت سهم‌هایشان به کلمه عبور دست یابند و از طرف دیگر هیچ کدام نتوانند از سهم‌هایشان کلمه عبور را تشخیص دهند. ما قصد داریم در این فصل روش‌های تقسیم راز را بررسی کنیم.

۴.۱ ساختار دستیابی آستانه در طرح تقسیم راز

در سال ۱۹۷۹ شامیر در مقاله ای [۲۶] براساس درونیابی چند جمله‌ای‌ها روی میدان‌های متناهی، نشان داد که چگونه می‌توان برای هر دو عدد صحیح t و $\omega, (2 \leq t \leq \omega)$ یک طرح تقسیم راز t از ω ساخت . در این روش شخص D به نام توزیع کننده [۱] یا واسطه ، ω سهم را بین یک مجموعه ω نفری (این مجموعه

[۱] dealer

را با P نشان می‌دهیم و فرض می‌کنیم D عضو P نباشد) طوری تقسیم می‌کند که هر t نفر یا بیشتر بتواند رمز مورد نظر را بازسازی کنند و هیچ $t-1$ نفر یا کمتر نتوانند هیچ گونه اطلاعاتی از رمز بدست آورند. لذا زمانی که سهم‌های تقسیم شده دارای ارزش یکسان باشند روش تقسیم راز را یک روش آستانه‌ای [۲] می‌نامیم. در زیر تعریف دقیق‌تری از روش آستانه‌ای معرفی شده است.

تعریف ۱.۴.۱. *فرض کنید t و ω اعداد صحیح مثبت باشند و $t \leq \omega$ یک $(t,\omega)-$ روش آستانه شیوه ای است برای تقسیم یک کلید K بین یک مجموعه از ω سهام دار به گونه ای که هرt سهام دار یا بیشتر بتوانند مقدار K را محاسبه کنند اما هیچ گروهی از $t-1$ سهام دار نتوانند هیچ گونه ای اطلاعاتی از کلید K پیدا کنند.*

به طور مثال، رمزگشایی کلمه عبور برای فعال‌سازی موشک‌ها یک روش $(3,4)-$ آستانه است. در ادامه برای فهم بیشتر مطلب، مثالی بر مبنای روش چند جمله‌ای‌های شامیر ارائه می‌کنیم.

مثال ۱.۴.۱. *فعال‌سازی سلاح‌های اتمی در روسیه یک مکانسیم دسترسی ۲ از ۳ دارد. یعنی بین سه نفر رئیس جمهور وزیر دفاع و معاون وزیر دفاع بایستی حداقل دو نفر حضور داشته باشند تا بتوانند رمز کنترل سلاح اتمی مورد نظر را باز کند. اگر رمز کنترل سلاح اتمی را عرض از مبدا H خط راست $f(x)=mx+h$ در نظر بگیریم و معادله خط را مخفی نگه داریم، آنگاه با دادن سه نقطه متمایز $f(1)$ ، $f(2)$ و $f(3)$ به این سه نفر (به طور محرمانه) می توان یک روش آستانه $(2,3)-$ ارائه نمود . حال درزمان فعال سازی سلاح ها با حضور دو نفر از این سه نفر و داشتن دو نقطه متمایز از این خط راست می توان معادله خط را به صورت منحصر به فرد آورد و راز $f(0)$ را بازسازی نمود .(شکل۱ .۱ را ببینید).*

[۲] threshold scheme

۵.۱ روش آستانه ای شمیر در Z_q

شامیر در مقاله [۲۶]یک روش آستانه‌ای $(t,\omega)-$ برای طرح های تقسیم راز بر پایه جبر خطی عددی مطرح نمود. در این بخش به بررسی این روش می پردازیم. فرض کنیم $P=\{p_i|1\leq i\leq \omega\}$ مجموعه ω سهام‌دار، k مجموعه تمام کلیدهای ممکن و s مجموعه تمام سهم‌های ممکن باشد. قرار می‌دهیم $K=Z_q$ و $S=Z_q$ ، که در آنها q یک عدد اول است و $q\geq\omega+1$. بنابراین کلید مثل هر سهم داده شده به سهام‌داران یکی از اعضای Z_q است. اکنون طبق الگوریتم زیر به توزیع سهم‌ها می‌پردازد:

مرحله نخست.

۱. واسطه ω, D عنصر غیر مجزا از Z_q را که با x_i نمایش می‌دهیم، انتخاب می‌کند (به همین دلیل است که در نظر گرفتیم $q\geq\omega+1$ باشد).

۲. برای $1\leq i\leq\omega$ واسطه D برای هر مقدار x_i ، p_i را حساب می‌کند، بطوریکه x_i ها را می‌توانند اشخاص دیگر بدانند .

مرحله توزیع سهم‌ها .

۱. D برای تقسیم کلید K به صورت تصادفی $t-1$ عنصر مجزای $a_{t-1},\ldots,a_1$ را از Z_q به طور مخفیانه انتخاب می‌کند.

۲. برای هر $1\leq i\leq\omega$ ، D مقدار $y_i=a(x_i)$ را با کمک چند جمله‌ای زیر محاسبه می‌کند:

$$a(x)=k+\sum_{j=1}^{t-1}a_jx^j \qquad (modq) \qquad (۱.۱)$$

۳. به ازای هر $1\leq i\leq\omega$ ، D سهم y_i رابه p_i می‌دهد. مقدار y_i های هر شخص باید برای سهام‌داران دیگر مخفی بماند.

پس در این روش واسطه یک چند جمله‌ای تصادفی $a(x)$ از درجه حداکثر $t-1$ می سازد که در آن جمله ثابت همان کلید است و به هر سهام دار p_i یک زوج (x_i,y_i) از این چند جمله‌ای تعلق می‌گیرد.

مرحله بازسازی کلید.

یک زیرمجموعه b از t سهام دار توسط درونیابی چند جمله‌ای می‌توانند کلید را بازسازی نمایند. در ادامه دو روش موجود برای بازسازی کلید را بیان می‌نماییم.

۱.۵.۱ روش اول از دیدگاه حل دستگاه معالات خطی روی Z_q

فرض کنید که سهام‌داران $p_{i_t}, \ldots, p_{i_1}$ بخواهند k را پیدا کنند آن‌ها می‌دانند که

$$y_{i_j} = a(x_{ij}), \qquad 1 \leq j \leq t$$

که $a(x) \in Z_q[x]$ چند جمله‌ای مخفی بر گزیده توسط D است.چون $a(x)$ حداکثر از درجه $t-1$ است پس $a(x)$ را می توان به صورت زیر نوشت :

$$a(x) = a_0 + a_1 x + \ldots + a_{t-1}x^{t-1}$$

که ضرایب $a_{t-1}, \ldots, a_0$ مجهولند و $a_0 = k$. چون $y_{i_j} = a(x_{i_j})$ ، برای هر $1 \leq j \leq t$ ، زیرمجموعه B تعداد t معادله خطی بر اساس t مجهول $a_{t-1}, \ldots, a_0$ به دست می‌آورد که همه محاسبات در Z_q انجام می‌شود. اگر معادلات مستقل خطی باشند یک جواب یکتا به دست خواهد آمد و a_o به عنوان کلید مشخص می شود.

برای روشن شدن مطلب به مثال زیر توجه کنید.

مثال ۱.۵.۱. *فرض کنید که* $q = 13$ ، $t = 3$ و $\omega = 5$ *باشد و به ازای هر* $1 \leq i \leq 5$ *داشته باشیم* $x_i = i$. *فرض کنید که سهام‌داران* $B = p_1, p_3, p_5$ *سهم‌هایشان را که به ترتیب عبارتند از ۸ و ۱۰ و ۱۱ روی هم گذاشته باشند داریم:*

$$a(x) = a_0 + a_1 x + a_2 x^2$$

با محاسبه $a(1)$ ، $a(3)$ و $a(5)$ ، *معادلات خطی زیر در* Z_{17} *به دست می آیند:*

$$a_0 + a_1 + a_2 = 8$$

$$a_0 + 3a_1 + 9a_2 = 10$$

$$a_0 + 5a_1 + 8a_2 = 11$$

دستگاه فوق دارای جواب یکتا ی $a_0 = 13$ ، $a_1 = 10$ و $a_2 = 2$ *در* Z_{17} *است. بنابراین کلید* $k = a_0 = 13$ *است.*

در حالتی که t سهام دار تصمیم به بازسازی کلید بگیرند، کلید به صورت یکتا بازسازی می شود. در ادامه به بررسی یکتای جواب دستگاه t معادله خطی می‌پردازیم . در حالت کلی داریم:

$$y_{ij} = a(x_{ij}), \qquad 1 \leq j \leq t$$

به طوری‌که

$$a(x) = a_0x + a_1x + \ldots + a_{t-1}x^{t-1}$$

و

$$a_0 = k$$