
بسم الله الرحمن الرحيم

دانشگاه ولی عصر(عج) رفسنجان
دانشکده علوم ریاضی
گروه ریاضی

پایان‌نامه کارشناسی ارشد
رشته ریاضی محض، گرایش آنالیز

طرح‌های تسهیم راز دیداری براساس شبکه تصادفی با قابلیت رمزگشایی چندگانه

استاد راهنما:
دکتر محمدعلی دهقان

استاد مشاور:
رضا پورکانی

نگارنده :
جابر کریمی رحمت آبادی

اسفند ۱۳۹۲

دانشگاه ولی‌عصر(عج) رفسنجان

دانشکده‌ی علوم ریاضی

گروه ریاضی

پایان‌نامه‌ی کارشناسی‌ارشد رشته‌ی ریاضی کاربردی گرایش آنالیز عددی

علی محبیان

بررسی تقریب معادلات دیفرانسیل جزئی تصادفی با استفاده از روش‌های تفاضل متناهی

در تاریخ ۹۲/۷/۱۵ توسط هیأت داوران زیر بررسی و با درجه عالی به تصویب نهایی رسید.

۱- استاد/ استادان راهنمای پایان‌نامه **دکتر مهران نامجو** با مرتبه ی علمی **استادیار**

امضاء

۲- استاد/ استادان داور داخل گروه **دکتر علی توکلی** با مرتبه ی علمی **دانشیار**

امضاء

۳- استاد/ استادان داور داخل از گروه **دکتر سیدعلی‌محمد محسنی‌الحسینی** با مرتبه‌ی علمی **استادیار**

امضاء

۴ – نماینده‌ی تحصیلات تکمیلی **دکتر محمد حشمتی** با مرتبه ی علمی **استادیار** امضاء

تقدیر و تشکر

شکر شایان نثار پروردگاری که توفیق را رفیق راهم ساخت تا این پایان‌نامه را به پایان برسانم، پروردگاری که سخنوران، در ستودن او بمانند و ریاضی‌دانان، هیچ فرمولی برای شمردن نعمتهای او ندانند و نویسندگان توانایی شکرگزاری از او را آنگونه که شایستگی اوست در قالب هیچ جمله‌ای نتوانند نوشت.

بر حسب وظیفه و از باب " من لم یشکر المنعم من المخلوقین لم یشکر الله عزوجل " از استاد راهنمایم جناب آقای دکتر محمد علی دهقان، اسوه اخلاق و علم و ادب، کسی که اندیشیدن را به من آموخت، صمیمانه تشکر می‌کنم.

همچنین با امتنان بی‌کران از مساعدت‌های بی‌شائبه‌ی جناب آقای رضا پورکانی که به عنوان استاد مشاور همراهیم کردند. همچنین از جناب آقای دکتر ابراهیمی و سرکار خانم دکتر علیجانی که داوری این پایان‌نامه را برعهده داشتند و همه کسانی که بنده‌ی حقیر را در این امر مساعدت کردند کمال تشکر را دارم.

جابر کریمی رحمت آبادی
j.karimi@stu.vru.ac.ir

تقدیم به

تمامی آزادمردانی که نیک می اندیشند و عقل و منطق را پیشه خود نموده اند و جز رضای پرودگار و پیشرفت و سعادت جامعه هدفی ندارند.

و

همچنین دانشمندان، بزرگان و جوانمردانی که جان و مال خود را در حفظ و اعتلای این مرز و بوم فدا نموده اند و مینمایند.

تقدیم به

پدرم که ناتوان شد تا من به توانایی برسم و مادرم که موهایش سفید شد، تا من رو سفید شوم. و هرچه دارم از دعاهای ایشان است که بدرقه ی راهم بوده است.

و

برادرانم که تکیه گاه من در طول زندگی ام بوده اند.

همچنین به خانواده ام و هر کس که به گردن من حق دارد.

چکیده

شبکـه‌ی تصـادفی (RG) [۱] یـک روش بـرای سـاخت طرح تـسهیـم راز دیـداری (VSS) [۲] بدون گسترش پیکسل [۳] است. در این پایان نامه ابتدا چند طرح تسهیم راز دیداری بر اساس شبکه‌ی تصادفی که تصویر اصلی با روی هم قرار دادن سهام به‌طور مستقیم بازسازی می‌شود مورد مطالعه قرار می‌گیرد. سپس به بررسی یک طرح تسهیم راز دیداری بر اساس شبکه‌ی تصادفی با قابلیت بازسازی به دو روش پرداخته شده است. اگر دستگاه‌های محاسباتی در دسترس نباشند، تصویر اصلی با عملیات روی هم قرار دادن سهام، بازسازی می‌شود. اما اگر دستگاه‌های محاسباتی در اختیار باشند، تصویر اصلی با عملیات XOR بازسازی می‌شود. تفاوت روش اول و دوم از چند جنبه قابل بررسی است، برتری روش اول نسبت به روش دوم این است که در این روش تصویر رمز بدون هیچ‌گونه محاسباتی رمزگشایی می‌شود. در حالی که در روش دوم نیاز به دستگاه‌های سبک محاسباتی است. همچنین مزیت روش دوم کیفیت بالاتر تصویر رمزگشایی شده نسبت به روش اول است. [۴]

کلمات کلیدی: تسهیم راز دیداری، شبکه تصادفی، عمل XOR، عمل OR، گسترش پیکسل، رمزگشایی، کنتراست (تباین)

---

[۱] Random Grid

[۲] Visual Secret Sharing

[۳] Pixel

[۴] در این پایان‌نامه اصطلاح رمزگشایی و بازسازی تصویر به یک معنی بکار رفته است و به تناسب زیبایی جمله از هر دو کلمه در متن استفاده می‌شود.

پیش‌گفتار

رمزنگاری [1] از دو واژه‌ی یونانی رمز(crypt) و نوشتن یا نگارش (graphy) تشکیل شده است. هدف این علم به رمز در آوردن و مخفی کردن اطلاعات و مطالعه بر روی اطلاعات رمزنشده است. علم رمزنگاری به دو دسته مهم کلاسیک و مدرن تقسیم می‌شود.

به طور کلی رمزنگاری کلاسیک به رمزنگاری محدود می‌شود، یعنی تبدیل اطلاعات عادی به اطلاعات غیر قابل کشف که البته قسمت مهمی از رمزنگاری مدرن را نیز به خود اختصاص می‌دهد.

رمزنگاری مدرن علاوه بر رمزنگاری شاخه‌های مهم دیگری را نیز در بر می‌گیرد، از جمله رمزنگاری نامتقارن، توابع فشرده‌ساز، احراز هویت پیام، اعداد تصادفی، امضاء دیجیتالی و غیره.

امروزه رمزنگاری یکی از شاخه‌های ریاضی و علوم کامپیوتر محسوب می‌شود. همچنین این علم رابطه تنگاتنگی با علوم نظریه اطلاعات، امنیت رایانه‌ای و مهندسی داراست. در دنیای امروز با رشد اینترنت و امکانات ارتباطی دیگر نقش امنیت و تضمین صحت روابط بیشتر و بیشتر می‌شود.

امروزه با توجه به پیچیدگی‌های روابط انسانی و عدم اعتماد متقابل در روابط الکترونیکی، نیاز به یک علم تضمین ارتباطات (رمزنگاری) می‌باشد. به طوری که می‌توان گفت بدون رمزنگاری هیچ تضمینی در دنیای دیجیتال وجود ندارد.

علم رمزنگاری علاوه بر جذابیتی که دارد، پیچیدگی بسیار زیادی نیز دارد، تا حدی که بسیاری از بزرگان ریاضی و رمزنگاری این علم را دشوارترین علوم دانسته‌اند.

برای تسلط کافی به مباحث رمزنگاری تلاش بسیار کافی نیست، بلکه باید فرد تفکر رمزنگاری نیز داشته باشد.

از دشوارترین مباحث رمزنگاری که همیشه طرفداران بسیاری را به خود اختصاص داده،

---

[1] cryptography

می‌توان به رمزشکنی اشاره کرد. رمزشکنی به فرایند تلاش برای شکستن تمامی رمز یا قسمتی از اطلاعات رمزی گفته می‌شود.

در زمان‌های گذشته رمزنگاری عملیاتی پرهزینه به حساب می‌آمد، لذا تنها برای محافظت از اطلاعات طبقه‌بندی شده و حساس مانند اطلاعات نظامی، سرویس‌های امنیتی، نقل و انتقالات مالی و کلمات عبور مورد استفاده قرار می‌گرفت. ولی امروزه رمزنگاری به روشی ارزان قیمت برای محافظت ارتباطات و اطلاعات تبدیل شده است.

تاریخ دقیقی برای رمزنگاری وجود ندارد. اینکه رمزنگاری دقیقاً از کی شروع و تا کی ادامه خواهد داشت را نمی‌توان مشخص کرد. در حالت کلی از زمانی که انسان شیوه‌ی انتقال اطلاعات را یاد گرفت، رمزنگاری کشف و تا زمانی که بشر نیاز به انتقال اطلاعات داشته باشد ادامه خواهد داشت. سابقه‌ی سیستم‌های اولیه رمزنگاری که گاهی به آنها کد یا رمز گفته می‌شود، به مصر باستان و حدود ۲۰۰۰ سال پیش برمی‌گردد. حال به اختصار تاریخچه‌ی این علم را از زمان جنگ جهانی اول بررسی می‌کنیم.

در اواخر جنگ جهانی اول آلمان‌ها سیستم رمزکننده‌ی ADFGVX را اختراع کردند که توسط رمزشکن مشهور فرانسوی پینیون [۱] شکسته شد و تا سال ۱۹۲۴ رمز وون کریا [۲] که به شدت مورد استفاده دیپلمات‌های آلمانی قرار می‌گرفت، توسط رمزشکنان آمریکایی و در مدت ۲ ساعت و ۴۵ دقیقه شکسته شد. بین سال‌های ۱۹۴۲ تا ۱۹۴۵ رمز انیگما[۳] که به آلمان برده شد و مورد استفاده آنها قرار گرفت توسط یک ریاضیدان لهستانی به نام مارین رجوسکی[۴] شکسته شد. همچنین در انگلیس نیز این رمز توسط گروهی به سرکردگی ویلیام فریدمن [۵] شکسته شد [۶].

با توجه به مطالبی که گفته شد، می‌توان به این نکته پی‌برد که در گذشته رمز کردن و رمزگشایی هر دو با دستگاه و ماشین‌های رمزنگاری انجام می‌شده است و همچنین نیاز به افراد متخصص برای این کار بوده است، بنابراین فقط در موارد خاص مانند اطلاعات نظامی و حکومتی و غیره مورد استفاده قرار می‌گرفت. از این رو متخصصین به فکر کشف روش‌هایی برای تبدیل سیستم رمزنگاری به یک سیستم دیداری و بدون هیچ گونه محاسبات افتادند.

---

[۱] Pinion

[۲] Won Kerya

[۳] Enigma

[۴] Marian Rejewski

[۵] William Friedman

[۶] در شکستن این رمز از علم مهندسی معکوس استفاده شده است.

اولین بار در سال ۱۹۷۹ روش تسهیم راز دیداری توسط ا.شامیر [۱] و ج.ر.بلکلی [۲] [۱۵]،[۳] جایگزین روش‌های قبل در برقراری امنیت برای جلوگیری از تخریب یا از بین بردن اطلاعات مهم شد. در سال ۱۹۹۵ اصول اساسی تسهیم راز دیداری توسط م.نائور [۳] و ا.شامیر در[۱۴] معرفی شد که در آن هر تصویر به n تصویر تبدیل و بین n نفر تقسیم می‌شود. حال در طرح (k, n) اگر تصویر k نفر از n نفر (یا بیشتر) را روی هم قرار دهیم تصویر اصلی بازسازی می‌شود. در سال ۱۹۹۸ س.بلاندا [۴] و ا.سانتیس [۵] [۴] و همچنین در سال ۲۰۰۶، چ.کوگا [۶] و ا.یودا [۷] مطالعاتی به منظور افزایش کیفیت دیداری تصویر رمزگشایی شده انجام دادند[۱۱]. علاوه بر این در سال‌های ۲۰۰۵ توسط ح.المان، [۸] ج.لینت، [۹] ل.تول هویزن [۱۰] و پ.تولس [۱۱] [۱۸] و در سال ۲۰۰۷ توسط ل.ژانگ [۱۲] و د.وانگ [۱۳] [۱۹] با استفاده از طرح‌های تسهیم راز دیداری بر اساس XOR کیفیت بهتری بدست آمد که در این روش مشکل گسترش پیکسل داریم. برای حل این مشکل می‌توان از طرح‌های تسهیم راز دیداری با استفاده از شبکه تصادفی که توسط س.کیماتو [۱۴]، ر.پریسکو [۱۵] و ا.سانتیس [۱۶] در سال ۲۰۰۶ مطرح شده است، استفاده کرد.

---

[۱] A. Shamir
[۲] G. R. Blakely
[۳] M.Naor
[۴] C. Blundo
[۵] A.De Santis
[۶] H. Koga
[۷] E.ueda
[۸] H. Hillmann
[۹] J. Lint
[۱۰] L.Tolhuizen
[۱۱] P.Tuyls
[۱۲] L. Zhang
[۱۳] D. Wang
[۱۴] S. Cimato
[۱۵] R. De Prisco
[۱۶] A. De Sentis

فهرست مطالب

فهرست تصاویر

فهرست جداول

فصل ۱

تسهیم راز دیداری

۱.۱ مقدمه‌ای بر رمزنگاری

کلمه‌ی رمزنگاری [۱] برگرفته از لغات یونانی رمز[۲] و نگارش [۳] می‌باشد. از آنجا که بشر همیشه چیزهایی برای مخفی کردن داشته است، رمزنگاری برای مخفی کردن اطلاعات، قدمتی برابر عمر بشر دارد. از پیغام رساندن با دود تا رمزنگاری سزاری، رمزهای جایگشتی و روش‌های متنوع دیگر. رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و در طول قرن‌ها به منظور محافظت از پیغام‌هایی که بین فرماندهان، جاسوسان، عشاق و دیگران رد و بدل می‌شد، استفاده شده است. هنگامی که با امنیت داده‌ها سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده‌ی پیغام است و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی، محرمانه بودن، تصدیق هویت و جامعیت، در قلب امنیت ارتباطات داده‌های مدرن قرار دارند. پس این مسئله باید تضمین شود که یک پیغام فقط می‌تواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران توانایی انجام این کار را نداشته باشند. روشی که تأمین کننده‌ی این مسئله باشد رمزنگاری نام دارد. رمزنگاری هنر نوشتن به صورت رمز است به طوری‌که هیچ‌کس به غیر از دریافت کننده‌ی مورد نظر نتواند محتوای پیغام را بخواند.

متخصصین رمزنگاری بین رمز [۴] و کد [۵] تمایز قائل می‌شوند. رمز عبارت است از تبدیل

---

[۱] cryptography
[۲] Crypt
[۳] Graphy
[۴] cipher
[۵] code

کاراکتر به کاراکتر یا بیت به بیت بدون آن که به محتویات زبان شناختی آن پیام توجه شود. در طرف مقابل کد تبدیلی است که کلمه‌ای را با یک کلمه یا علامت دیگر جایگزین می‌کند. امروزه از کدها استفاده چندانی نمی‌شود اگر چه استفاده از آن پیشینه طولانی دارد. موفق‌ترین کدهایی که تا کنون ابداع شده‌اند توسط ارتش ایالات متحده و درخلال جنگ جهانی دوم در اقیانوس به کار گرفته شده است. از دیدگاه تاریخی چهار گروه از مردم در شکل‌گیری هنر رمزنگاری دخیل بوده‌اند: نظامیان، هیئت‌های سیاسی، واقعه‌نگاران و عشاق. از بین این‌ها نظامیان نقش بسیار مهم‌تری دارند. سابقاً در موسسات نظامی پیام‌هایی را که باید رمز می‌شد به یک کارمند یا منشی حقوق بگیر تحویل می‌گردید تا آن‌ها را رمز و ارسال کند. حجم عظیم پیام‌هایی که در طول یک روز باید ارسال می‌شد مانع از آن بود که این کار بر عهده معدود متخصصین خبره حاضر در یک موسسه گذاشته شود. تا زمان ابداع کامپیوترها، در عرصه جنگ واقعی و با تجهیزات اندک، بزرگ‌ترین نقطه ضعف استراتژی رمزنگاری آن بود که همه چیز به توانایی و سرعت عمل کارمندان رمزنگار پیام، بستگی داشت. لذا باید این امکان مهیا می‌شد که روش رمزنگاری تغییر کند.

به طور کلی رمزنگاری را می‌توان به دو دسته سنتی و مدرن تقسیم‌بندی کرد که به اختصار به بررسی روش‌های این دو دسته می‌پردازیم.

۲.۱ روش های رمزنگاری سنتی

روش های رمزنگاری سنتی به طور کلی به دو دسته تقسیم می‌شوند.

الف) رمزهای جانشینی [۱]: در این رمزنگاری هر حرف یا گروهی از حروف با یک حرف یا گروهی دیگر از حروف جابه‌جا می‌شوند تا شکل پیام به هم بریزد. یکی از قدیمی‌ترین رمزهای شناخته شده روش رمزنگاری سزار است. در این روش مثلاً حرف a به D و b به E و به همین ترتیب تا z که با C جایگزین می‌شود. حالت عمومی و ساده از رمزنگاری سزار آن است که هر حرف الفبا از متن اصلی با حرفی که در جدول الفباء k حرف بعدتر قرار گرفته جابه‌جا شود. روش رمز نگاری سزار امروزه نمی‌تواند کسی را فریب دهد. در سیستم رمزنگاری که در آن یک نماد با نماد دیگر جایگزین شود، سیستم یک حرفی گفته می‌شود که در آن کلید رمز یک رشته ۲۶ کاراکتری است.

[۱] substitution cipher

در روش فوق علیرغم آن‌که آزمایش تمام حالات یک کلید ممکن نیست ولی حتی برای یک قطعه متن رمز شده‌ی کوچک، رمز متن به راحتی شکسته خواهد شد. درحمله‌ی اصولی به این سیستم رمز از ویژگی‌های آماری زبان‌های طبیعی بهره گرفته شده است. به عنوان مثال در زبان انگلیسی حروفی که بیشترین تکرار را دارند به ترتیب عبارتند از: e، t، a، o، n و r. ترکیبات دو حرفی [۲] که بیشترین تکرار را دارند به ترتیب عبارتند از: th، he، an و re. همچنین ترکیبات سه حرفی [۳] که بیشترین تکرار را دارند به ترتیب عبارتند از: the، ing، and و ion.

تحلیل‌گر رمز (رمزشکن) برای شکستن سیستم رمزنگاری با شمارش حروف متن رمز شده و محاسبه تکرار نسبی هر حرف شروع می‌کند. سپس حرفی که دارای بیشترین تکرار است را با e و حرف پرتکرار بعد را با t جایگزین می‌کند و می‌تواند با در نظر داشتن سه حرفی the به دنبال سه حرفی های txe در متن رمز شده بگردد که به احتمال قوی x معادل با h است.

ب) رمزنگاری جایگشتی [۱]: در رمزنگاری جانشینی ترتیب نمادهای یک متن حفظ می‌شد ولی شکل نمادها تغییر پیدا می‌کرد. در حالی‌که در رمزنگاری جایگشتی، یک بلوک از کاراکترها به طول ثابت را از ورودی دریافت کرده و یک بلوک رمز شده با طول ثابت در خروجی تولید می‌کند. برای شکستن رمز فوق تحلیل‌گر رمز ابتدا باید مطمئن شود که آیا واقعاً با یک متن رمز شده به روش جایگشت رو به رو است یا خیر. گام بعد آن است که تعداد ستون‌ها حدس زده شود. کلید رمز یک کلمه یا عبارتی است که هیچ حرف تکراری ندارد و کاربرد آن شماره‌گذاری ستون‌ها می‌باشد. در این روش شماره‌ی هر ستون بر اساس ترتیب الفبایی هر حرف کلید نسبت به جدول الفبا تعیین می‌شود. مثلا ستون چهارم شماره ۱ است (حرف A) و به همین ترتیب متن اصلی به صورت افقی (سطری) نوشته می‌شود و در صورت لزوم تعدادی حرف مانند a و b و... به آخرین سطر اضافه می‌شود تا ماتریس مربوطه پر شود. متن رمز شده بر اساس شماره‌ی ستون‌ها به صورت عمودی خوانده شده و به هم متصل می‌شود. ترتیب خواندن ستون‌ها، از ستون با کوچک‌ترین شماره به بزرگ‌ترین شماره است. در زیر

[۲] Diagram
[۳] Trigram
[۱] permutation

یک مثال از این روش آورده شده است.

کلید رمز:

M E G A B U C K
7 3 4 1 2 8 6 5
p l e a s e t r
a n s f e r o n
e m i l l i o n
d o l l a r s a

متن آشکار:

Pleasetransferonemilliondollars

متن رمزشده:

afllselalnmoesilrnnatoospaederir

۳.۱ روش‌های رمزنگاری مدرن مبتنی بر کلید

روش‌های رمزنگاری مدرن مبتنی بر کلید به دو دسته تقسیم می‌شوند:

الف) رمزنگاری با کلید متقارن [۱]: روش‌های پیشرفته رمزنگاری از اصول و قواعدی مشابه رمزگذاری سنتی (مانند روش های جانشینی و جایگشتی) بهره گرفته‌اند، در حالی‌که راه کارها متفاوت هستند. در قدیم رمزنگاران از الگوریتم‌های ساده استفاده می‌کردند ولی الان به عکس، هدف آن است که یک الگوریتم به قدری پیچیده طراحی شود که حتی اگر رمزشکن توده عظیمی از متن رمز شده را به انتخاب خود در اختیار بگیرد، بدون کلید نتواند چیزی از آن استخراج کند. الگوریتم‌های با کلید متقارن برای رمزنگاری و رمزگشایی از یک کلید استفاده می‌کنند. به عنوان مثال فرض کنید

[۱] symmetric key

پیامی را برای یکی از دوستان خود رمز و سپس ارسال می‌نمایید و شما برای رمزگذاری اطلاعات از روشی استفاده نموده‌اید که بر اساس آن، هر یک از حروف موجود در متن پیام را به دو حرف بعد از خود تبدیل کرده‌اید. مثلاً حرف A در متن پیام به حرف C و حرف B به حرف D تبدیل گردند. پس از ارسال پیام رمز شده برای دوست خود می‌بایست با استفاده از یک روش ایمن و مطمئن کلید رمز را نیز برای وی مشخص کرد. در صورتی که گیرنده‌ی پیام دارای کلید رمز مناسب نباشد قادر به رمزگشایی و استفاده از اطلاعات نخواهد بود. در چنین حالتی باید به دوست خود متذکر گردید که کلید رمز، شیفت دادن هر حرف به سمت جلو و به اندازه دو واحد است. گیرنده پیام با انجام عملیات معکوس قادر به شکستن رمز و استفاده از اطلاعات خواهد بود.

ب) رمزنگاری با کلید نامتقارن یا عمومی [۱]: این الگوریتم‌ها برای رمزنگاری و رمزگشایی دو کلید مجزا دارند. به این معنی که کلیدی که رمزگذاری می‌کند توانایی باز کردن رمز را ندارد. به کلیدی که رمزگذاری می‌کند کلید عمومی و به کلیدی که رمزگشایی می‌کند کلید خصوصی گفته می‌شود. مانند این است که نامه را در صندوقی بیندازید و در آن را با کلیدی که دارید قفل کنید، اما آن کلید دیگر نتواند در صندوق را باز کند. بنابراین وقتی خود شما نتوانید در صندوق را باز کنید اگر کسان دیگر هم کلید شما را داشته باشند نمی‌توانند در صندوق را باز کنند. الگوریتم‌های کلید عمومی تضمین می‌کنند که از روی کلید عمومی نتوان کلید خصوصی را به دست آورد و کلید رمزنگاری را می‌توان در اختیار همه قرار داد.

رمزنگاری روش‌های مختلف دیگری نیز دارد که از تسهیم راز به عنوان یک روش دیگر می‌توان نام برد. در تسهیم راز ابتدایی، یک راز به چندین قسمت تقسیم می‌شد که با کنار هم گذاشتن آنها راز مشخص می‌شد. تسهیم راز انواع متفاوتی دارد که نوع دیداری آن که برای رمزگشایی نیاز به هیچ دستگاه محاسباتی ندارد موضوع مورد مطالعه می‌باشد.

به عنوان یک مثال در این زمینه به طرح‌های رمزنگاری دیداری (VCS)[۲] می‌توان اشاره کرد که در ادامه به بررسی این روش می‌پردازیم.

---

[۱] public key

[۲] Visual cryptography scheme