# بررسی و تحلیل طرح های رمز اشتراکی چندگانه جدید

**ودود جوادی زارع(دانشجوی کارشناسی ارشد مخابرات)**

**تهران،اتوبان شهید بابایی،دانشگاه امام حسین(ع)،دانشکده برق و کامپیوتر گروه مخابرات**

E-mail: v.javadi@gmail.com

**چکیده – در این مقاله چندین طرح رمز اشتراکی چندگانه که از سال ۲۰۰۰ به بعد ارائه شده مورد بررسی قرار گرفته است.از جمله طرح چاین و طرح یانگ که به عنوان طرح های اصلی محسوب شده اند.علاوه بر آن طرح هایی نیز که بر پایه طرح های فوق بوده و برخی پارامتر های آن ها را اصلاح کرده اند نیز مورد بررسی قرار گرفته اند.و در نهایت یک جمع بندی و مقایسه تحلیلی صورت گرفته است.**

**کلید واژه- رمز اشتراکی چندگانه،تابع یکطرفه دو متغیره،چند جمله ای درونیابی لاگرانژ**

## ۱- مقدمه

**رمز اشتراکی،نقش مهمی را در حفاظت اطلاعات مهم از گم شدن،خراب شدن،یا بدست افراد نا مطمئن افتادن بازی می کند.در سال ۱۹۷۹،اولین (t,n)-طرح آستانه رمز اشتراکی توسط شامیر[۶] و بلیکلی[۱] بطور مستقل ارائه شدند.یک رمز می تواند بین n مشترک تقسیم شود.حداقل t یا بیشتر از آن مشترک می توانند رمز را بازسازی کنند.اما (t-1) تا یا کمتر از آن مشترک هیچ اطلاعاتی درباره رمز بدست نمی آورند.در طرح شامیر که بیشتر طرح های ارائه شده بر پایه آن می باشد از چند جمله ای های درونیابی لاگرانژ برای پیاده سازی استفاده می شود. اخیرا چندین طرح رمز اشتراکی چندگانه پیشنهاد شده است.در یک طرح رمز اشتراکی چندگانه،چندین رمز برای تقسیم شدن در طول یک فرآیند رمز اشتراکی وجود دارد.چنین طرح هایی در چند نوع کاربرد مفید است؛گاهی اوقات نیاز است که چندین رمز بوسیله اطلاعاتی که برای محافظت یک رمز نیاز است،محافظت شوند.و گاهی اوقات مردم نیاز دارند که یک رمز بزرگ را به چند تکه تقسیم کنند که هر تکه با مقدار کمتری از اطلاعات نسبت به محافظت همه رمز،محافظت شود.در یک تقسیم بندی می توان رمز اشتراکی چندگانه را به دو نوع یکبار مصرف و چند بار مصرف تقسیم کرد.در یک طرح یکبار مصرف،وقتی که چند رمز بخصوص باز سازی شدند.رمز نگهدار باید سهام جدیدی را به هر مشترک دوباره توزیع کند.به عبارت دیگر در یک طرح چند بار مصرف هر مشترک نیاز دارد که فقط یک سهم را نگهدارد. توزیع کردن سهام به هر مشترک می تواند فرایند پیچیده و نکته داری باشد.یک نقطه ضعف مشترک که تقریبا بین همه طرح های رمز اشتراکی چند گانه مشترک است،این است که آن ها طرح های یکبار مصرف می باشند.**

در سیستم های رمز اشتراکی بخش سومی به عنوان مقسم رمز وجود دارد که کار تقسیم رمز بین مشترکین را به عهده دارد.

## ۲- پیش نیاز ها

در این بخش به توضیح چند مفهوم عمومی طرح های رمز اشتراکی چند گانه می پردازیم.که در بیشتر طرح ها مورد نیاز بوده است.

### ۲-۱- رمز اشتراکی شامیر

طرح های آستانه مؤثر می توانند در مدیریت کلید رمز نگاری مفید باشند.طرح شامیر یک (k,n)-طرح آستانه می باشد که بر پایه درونیابی چند جمله ای می باشد.اگر k نقطه $(x_1,y_1),(x_2,y_2),\cdots(x_k,y_k)$ با $x_i$ های جدا از هم داده شده باشند،فقط و فقط یک چندجمله ای از درجه $k-1$ وجود دارد که $q(x_i)=y_i$ برای تمام i ها.برای تقسیم داده D به سهام های مختلف چند جمله ای $q(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}$ را در نظر می گیریم که q(o)=D می باشد.و n سهم را به طریق زیر تولید می کنیم:

$$D_1=q(1),D_2=q(2),\cdots,D_n=q(n)$$

حال اگر بخواهیم رمز D را محاسبه کنیم،حداقل k زیر مجموعه از این $D_i$ ها می توانند ضرایب چند جمله ای q(x) را با درونیابی محاسبه کنند و در نهایت رمز D=q(o) را بدست آورند.

### ۲-۲- توابع یکطرفه دومتغیره

تابع f(r,s) هر تابع یکطرفه دو متغیره را نمایش می دهد که هر r,s را به رشته بیت f(r,s) با طول ثابت می نگارد.تابع یکطرفه دو متغیره چندین خاصیت دارد:

(۱) اگر r,s داده شده باشند،محاسبه f(r,s) آسان باشد.

(۲) اگر f(r,s),s داده شده باشند،محاسبه r سخت باشد.

(۳) اگر هیچ اطلاعاتی در مورد s نداشته باشیم،محاسبه f(r,s) بازای هر r سخت باشد.

(۴) اگر s داده شده باشد،پیدا کردن دو مقدار متفاوت $r_1.r_2$ به نحوی که $f(r_1,s)=f(r_2,s)$ باشد،سخت باشد.

(۵) اگرf(r,s),r داده شده باشند،محاسبه s سخت باشد.

(۶) اگر زوج $f(r_i,s),r_i$ داده شده باشند،محاسبه $f(r',s)$ برای $r'\neq r_i$ سخت باشد.

خواص تابع یکطرفه دو متغیره در [۵] اثبات شده است.

## ۳- طرح های رمز اشتراکی چندگانه

در این بخش به معرفی و بررسی طرح های رمز اشتراکی چندگانه می پردازیم.

### ۳-۱- طرح چاین و دیگران [۲]

در سال ۲۰۰۰،چاین و دیگران[۲] یک طرح رمز اشتراکی چندگانه بر پایه کد های بلوکی سیستماتیک ارائه دادند.آنها در طرحشان نشان دادند که طرح هارن [۵] برای کاربردعمومی رمز اشتراکی چندگانه چندان مناسب نیست.برای گرفتن اطلاعات بیشتر با جزئیات به [۲] مراجعه نمایید.طرح چاین با استفاده از خواص تابع یکطرفه دو متغیره و کد های بلوکی سیستماتیک پیاده سازی شده است.با توجه به اینکه به خواص تابع یکطرفه دو متغیره در بخش قبل اشاره شد،در اینجا کد های سیستماتیک بلوکی مطرح می کنیم.

G(N,K) را برای نمایش نوع خاصی از ماتریس

مولد کد بلوکی سیستماتیک، $\begin{bmatrix} G(N,K)=I \\ P \end{bmatrix}$،بکار می بریم که I ،ماتریس مشخصه K×K و P، $[g^{(i-1)(j-1)}]$ ماتریس (N-K)×K می باشد که g عضو اولیه در $GF(2^m)$ می باشد.$K<2^m$ بوده و I,P می توانند به شکل زیر نمایش داده شوند:

$$I=\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

$$P=\begin{bmatrix} ۱ & ۱ & ۱ & \cdots & ۱ \\ ۱ & g^{۱} & g^{۲} & \cdots & g^{k-۱} \\ ۱ & g^{۲} & g^{۴} & \cdots & g^{۲(k-۱)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ ۱ & g^{N-k-۱} & g^{(N-k-۱)۲} & \cdots & g^{(N-k-۱)(k-۱)} \end{bmatrix}$$

در اینجا، $(P_1,P_2,\cdots,P_n)$ ، p تا رمز را نشان می دهند که مابین n مشترک تقسیم می شود.قبل از اشتراک رمز ، مقسم رمز،بطور تصادفی n تا سهم رمز $s_1,s_2,\ldots,s_n$ را انتخاب و به هر یک از مشترکین از طریق یک کانال امن می فرستد.آنگاه مقسم رمز مراحل زیر را انجام می دهد:

۱- بطور تصادفی عدد r را انتخاب و $f(r,s_i)$ را بازای $i=۱,۲,\cdots,n$ محاسبه می کند.

۲- ماتریس مولد $G(۲(n+p)-t,n+p)$ را تولید می کند و $n+p<2^m$ می باشد.

۳- بردار D را بصورت زیر در نظر می گیرد:

$$D=(P_1,P_2,\cdots,P_p,f(r,s_1),f(r,s_2),\cdots,f(r,s_n))^T$$

که بالا نویس T به معنای ترانهاده می باشد.

۴- ماتریس V را محاسبه می کند:

$$V=G\times D=\begin{bmatrix} I \\ P \end{bmatrix}\times D$$

V می تواند به شکل زیر نمایش داده شود:

$$V=(P_1,P_2,\cdots,P_p,f(r,s_1),f(r,s_2),\cdots,f(r,s_n),\cdots,C_1,C_2,\cdots,C_{n+p-t}) \quad (۱)$$

که

$$C_i=\sum_{j=1}^{p} g^{(i-1)(j-1)}P_j+\sum_{j=p}^{n+p} g^{(i-1)(j-1)}P_j f(r,s_{j-p})$$
$$1\le i\le p+n-t \quad (۲)$$

$(r,C_1,C_2,\cdots,C_{n+p-t})$ در روش معتبر منتشر می شود.همچنانچه در [۷و۴] انجام می شود.

اگر حداقل t مشترک شبه سهام خود،$f(r,s_i)$ را بازای $i=۱,۲,\cdots,t$ روی هم بگذارند،(n+p-t) تا رابطه در رابطه (۲) فقط شامل (n+p-t) تا متغیر مجهول خواهد بود.بنا بر این رمز های $(P_1,P_2,\cdots,P_n)$ و شبه سهام دیگر مشترکین،$f(r,s_i)$ ها را (برای $i=t+1,t+2,\cdots,n$) می توان با حل همزمان (n+p-t) تا رابطه در رابطه (۲) بدست آورد.بر طبق خاصیت های تابع یکطرفه دو متغیره،مقسم دیگر نیاز به توزیع مجدد سهام رمز تازه به مشترکین در هر دور از رمز اشتراکی ندارد.مقسم فقط مجبور است که عدد تصادفی دیگر r را منشر کند.در طرح چاین و دیگران فقط $(n+p-t+1)$ تا مقدار عمومی مورد نیاز است.

### ۳-۲- طرح یانگ و دیگران[۹]

نمادهای این طرح با طرح چاین یکسان می باشد.مقسم ابتدا بطور تصادفی n سهم رمز $s_1,s_2,\cdots,s_n$ را انتخاب می کند و آنها را از طریق کانال امن توزیع می کند.آنگاه مقسم عدد r را بطور تصادفی انتخاب و $f(r,s_i)$ را برای

$i=1,2,\cdots,n$ محاسبه می کند.آنگاه مقسم مراحل زیر را بطور متفاوت با شرایط متفاوت اجرا می کند.اگر $p\le t$ باشد،مقسم مراحل زیر را اجرا می کند:

۱-عدد اول q را انتخاب و چند جمله ای از درجه $t-1$، h(x) (mod q) را تولید می کند. که $0 < P_1, P_2, \cdots, P_p, a_1, a_2, \cdots, a_{t-p} < q$ .

$$h(x) = P_1 + P_2 x + \cdots + P_p x^{p-1} + a_1 x^p + a_2 x^{p+1} + \cdots + a_{t-p} x^{t-1} \bmod q$$

۲- $y_i=h(f(r,s_i))$ در هنگ q را برای $i=1,2,\cdots,n$ محاسبه می کند.

۳- $(r, y_1, y_2, \cdots, y_n)$ را به طریق معتبر همچنانچه در[۷و۴] است،منتشر می کند.مجموع مقادیر عمومی $n+1$ تا می باشد.

اگر $p>t$ باشد،مقسم مراحل زیر را اجرا می کند:

۱- عدد اول q را انتخاب و چند جمله ای از درجه $t-1$، h(x) (mod q) را تولید می کند. که $0 < P_1, P_2, \cdots, P_p < q$ .

$$h(x) = P_1 + P_2 x + \cdots + P_p x^{p-1} \bmod q$$

۲- $y_i=h(f(r,s_i))$ در هنگ q را برای $i=1,2,\cdots,n$ محاسبه می کند.

۳- h(i) را در هنگ q برای $i=1,2,\cdots,p-t$ محاسبه می کند.

۴- $(r, h(1), h(2), \cdots, h(p-t), y_1, y_2, \cdots, y_n)$ را در روش معتبر مانند نظیرش در [۷و۴] منتشر می کند.مجموع مقادیر عمومی $(n+p-t+1)$ تا می باشد.

در اینجا نشان می دهیم که چگونه رمز را در دو حالت جداگانه باز سازی می کنیم.

حالت۱. $p\le t$

حداقل t مشترک شبه سهام خود $f(r,s_i)$ (برای $i=1,2,\cdots,t$ ) را روی هم می گذارند.با استفاده از چند جمله ای درونیابی لاگرانژ، با دانستن t زوج از $(f(r,s_i),y_i)$ ها،چند جمله ای درجه $t-1$، h(x) در هنگ q می تواند بطور یکتا به صورت زیر مشخص شود:

$$h(x) = \sum_{i=1}^{t} y_i \prod_{j=1,\, j\neq i}^{t} \frac{x - f(r,s_j)}{f(r.s_i) - f(r,s_j)} \bmod q$$

$$= P_1 + P_2 x + \cdots + P_p x^{p-1} + a_1 x^p + a_2 x^{p+1} + \cdots + a_{t-p} x^{t-1} \bmod q$$

حالت۲. $p>t$

در مجموع،مقسم به حداقل t تا مشترک که شبه سهام خود،$f(r,s_i)$ (برای $i=1,2,\cdots,t$ ) را روی هم میگذارند، h(i) را منتشر می کند. (برای $i=1,2,\cdots,p-t$ ).با دانستن t زوج از $(f(r,s_i),y_i)$ ها چند جمله ای درجه $p-1$، h(x) درهنگ q را می توانیم بطور یکتا به صورت زیر مشخص کنیم:

$$h(x) = \sum_{i=1}^{t} y_i \prod_{j=1,\, j\neq i}^{t} \frac{x - f(r,s_j)}{f(r.s_i) - f(r,s_j)} + \sum_{i=1}^{p-t} h(i) \prod_{i=1,\, j\neq i}^{p-t} \frac{x-j}{i-j} \bmod q$$

$$= P_1 + P_2 x + \cdots + P_p x^{p-1} \bmod q$$

### ۳-۳- طرح پانگ و وانگ [۸]

مشابه طرح یانگ،این طرح نیز بر پایه رمز اشتراکی شامیر می باشد.این طرح را می توان به صورت زیر توضیح داد:

(i) پارامتر های سیستم. f(r,s) را یک تابع یکطرفه دومتغیره در نظر می گیریم که تعریف آن مشابه طرح های چاین و یانگ می باشد.q را یک عدد اول بزرگ و تمام اعداد را اعضا میدان متناهی GF(q)

فرض می کنیم.مقسم امین n عدد صحیح جدا از هم $s_1, s_2, \cdots, s_n$ را به عنوان سهام رمز مشترکین بطور تصادفی انتخاب می کند.و n عدد صحیح جدا از هم $u_1, u_2, \cdots, u_n$ را از $[p, q-1]$ به عنوان اطلاعات مشخصه عمومی مشترکین انتخاب می کند.در اینجا ما هنوز $(P_1, P_2, \cdots, P_n)$ را برای نمایش دادن p رمز که مابین n مشترک تقسیم می شود بکار می بریم.

(ii) توریع رمز. مقسم امین، می تواند گام های زیر را برای توزیع p رمز مابین n مشترک بکار ببرد

(a) بطور تصادفی یک عدد صحیح r را انتخاب و $f(r,s_i)$ را بازای $i = 1,2,\cdots,n$ محاسبه می کند.

(b) تا زوج (n+p)

$(u_i, f(r,s_i)), (0,P_1), (1,P_2), \cdots, (p-1,P_p)$،

$i = 1,2,\cdots,n$،را برای تولید چند جمله ای درجه

$(n+p-1)$ام زیر بکار می برد.

$$h(x) = a_0 + a_1 x + \cdots + a_{n+p-1} x^{n+p-1} \mod q .$$

(c) تا عدد صحیح (n+p-t) مینیمم $d_1, d_2, \cdots, d_{n+p-t}$ را از $[p, q-1] - \{u_i \mid i = 1,2,\cdots,n\}$ بدست آورده،$h(d_i)$ را بازای $i = 1,2,\cdots,n+p-t$ محاسبه می کند.

(d) $(r, h(d_1), h(d_2), \cdots, h(d_{n+p-t}))$ را در هر روش تأیید شده مانند نظایر آن در [۷و۴] منتشر می کند.

(iii) بازسازی رمز.به منظور باز سازی p رمز،حداقل t مشترک شبه سهام خود $f(r,s_i)$ ها ، $i = 1',2',\cdots,t'$ را روی هم میگذارند.با t شبه سهام $f(r,s_i)$ ما می توانیم t زوج $(u_i, f(r,s_i))$، $i = 1',2',\cdots,t'$، را بدست آوریم.سپس بطریق مشابه در (ii)، (n+p-t) تا عدد صحیح مینیمم $d_1, d_2, \cdots, d_{n+p-t}$ را از $[p, q-1] - \{u_i \mid i = 1,2,\cdots,n\}$ پیدا می کند.با دانستن مقادیر عمومی $h(d_1), h(d_2), \cdots, h(d_{n+p-t})$ می توانیم (n+p-t) تا زوج $(d_i, h(d_i))$، $i = 1,2,\cdots,n+p-t$ را بدست آوریم.بنابراین n+p تا زوج با همدیگر بدست می آیند.ما $(X_i, Y_i)$، $i = 1,2,\cdots,n+p$ را برای نشان دادن این n+p زوج به ترتیب بکار می بریم.و چند جمله ای درجه(n+p-۱) ام h(x) بطور یکتا بصورت زیر مشخص می شود:

$$h(x) = \sum_{i=1}^{n+t} Y_i \prod_{j=1,\, j\neq i}^{n+t} \frac{x - X_j}{X_i - X_j} \mod q$$

$$h(x) = a_0 + a_1 x + \cdots + a_{n+p-1} x^{n+p-1} \mod q$$

در نتیجه p رمز را می شود با محاسبه $P_i = h(i-1)$ به ترتیب بازای $i = 1,2,\cdots,p$ بدست آورد.

## ۴- تحلیل و مقایسه طرح ها

همه طرح های ارائه شده یک (t,n)–طرح رمز اشتراکی چندگانه می باشند. p رمز می تواند میان n مشترک تقسیم شود و t یا بیشتر از آن مشترک می توانند با همکاری این رمز ها را بازسازی کنند.اما (t-۱) یا کمتر از آن مشترک،هیچ چیز درباره این رمزها بدست نمی آورند.

همه طرح های بخش قبل دارای مزایای یکسانی می باشند که در زیر آورده می شود:

(۱) اجازه بازسازی موازی را می دهند.یعنی چندین رمز بطور

همزمان می توانند باز سازی شوند.

(۲) مقسم بطور پویا تعداد رمز های توزیع شده را می تواند مشخص کند.

(۳) یک طرح چندبار مصرف می باشد که می تواند در بسیاری از نشست های رمز اشتراکی بدون توزیع مجدد سهام مشترکین بکار رود.

در این بخش همچنین برخی مقایسه کارآیی مابین سه طرح،بر حسب پیچیدگی محاسبات بازسازی رمز و تعداد مقادیر عمومی انجام می دهیم.

در طرح چاین،بازسازی رمز معادل با حل (n+p-t) تا رابطه همزمان در رابطه (۱) بخش ۳-۱ می باشد. در حالیکه در طرح یانگ و طرح پانگ و وانگ بازسازی رمز فقط با استفاده از چندجمله ای درونیابی لاگرانژ انجام می شود.بنا بر این بازسازی رمز دو طرح فوق آسانتر از طرح چاین می باشد.بخاطر اینکه استفاده از چندجمله ای درونیابی لاگرانژ برای بازسازی چندجمله ای آسانتر از حل رابطه های همزمان می باشد.[۳]

تعداد مقادیر عمومی یک پارامتر مهم می باشد که کارآیی یک طرح را مشخص می کند.به منظور تقسیم p رمز،طرح چاین و طرح پانگ و وانگ $(n+p-t+1)$ تا مقدار عمومی نیاز دارد.اما در طرح یانگ، $(n+p-t+1)$ تا مقدار عمومی وقتیکه p>t ،نیاز است و $(n+1)$ مقدار عمومی وقتیکه p≤t نیاز است.واضح است که مقدار عمومی بیشتری در طرح یانگ از طرح چاین و طرح پانگ و وانگ وقتیکه p≤t باشد،نیاز است.بخصوص وقتیکه p به ۱ و t به n خیلی نزدیک باشد.اگر p=۱ و t=n باشد،فقط دو مقدار عمومی در طرح چاین و طرح پانگ و وانگ نیاز است. اما هنوز $(p+1)$ تا مقدار عمومی در طرح یانگ مورد نیاز است.علاوه بر آن در طرح یانگ هر دو کار توزیع و بازسازی دو بکار گیری متفاوت در دو حالت جداگانه دارد که طرح یانگ را پیچیده تر از طرح های دیگر می کند.

## مراجع


[1] G.R. Blakley, Safeguarding cryptographic keys, in: Proc. AFIPS 1979 NCC, vol. 48, Arlington, VA, June 1979, pp. 313–317.

[2] H.-Y. Chien, J.-K. Jan, Y.-M. Tseng, A practical (t,n) multi-secret sharing scheme, IEICE Transactions on Fundamentals E83-A (12) (2000) 2762–2765.

[3] G. Di Crescenzo, Sharing one secret vs. sharing many secrets: tight bounds on the average improvement ratio, in: Proc. of 11th Annu. ACM-SIAM Symp. on Discrete Algorithms (SODA 2000), San Francisco, pp. 273–274.

[4] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory IT-31 (July) (1985) 469–472.

[5] L. Harn, Efficient sharing (broadcasting) of multiple secret, IEE Proceedings—Computers and Digital Techniques 142 (3) (1995) 237–240.

[6] A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612–613.

[7] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM 21 (February) (1978) 120–126.

[8] Liao-Jun Pang, Yu-Min Wang
A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing
State Key Laboratory of Integrated Service Networks, Xidian University,
P.O. Box 119, Xi'an 710071, China

[9] Chou-Chen Yang[a], Ting-Yi Chang[b], Min-Shiang Hwang [b]
A( t, n) multi-secret sharing scheme
a Department of Computer and Information Science, Chaoyang University of Technology,
168 Gifeng E. Rd., Wufeng, Taichung County, 413 Taiwan, ROC
b Institute of Networks and Communications, Chaoyang University of Technology, 168 Gifeng E. Rd.,
Wufeng, Taichung County, 413 Taiwan, ROC