کاربرد اَبَرمنحنی‌های بیضوی در رمزنگاری

رضا علیمرادی

استادیارگروه ریاضی و علوم کامپیوتر دانشکدهٔ علوم پایه، دانشگاه قم، قم، ایران
r.alimoradi@qom.ac.ir; alimoradi.r@gmail.com

چکیده

در رمزنگاری کلید عمومی برای جایگزینی سامانه‌های مبتنی بر مسئله تجزیه اعداد[1] از سامانه‌های مبتنی بر مسئله لگاریتم گسسته استفاده می‌شود. درواقع رمزنگاری مبتنی بر منحنی‌های بیضوی[2] (ECC) به‌علت این‌که طول کلید را به‌طور محسوسی نسبت به سامانه‌های مشابه RSA کاهش می‌دهند بسیار مورد توجه طراحان سامانه‌های رمزنگاری قرار گرفتند. طراحان همیشه نیازمند دست‌یابی به سامانه‌های رمزنگاری با طول کلید کمتر و سطح امنیتی بالاتر هستند؛ به همین دلیل آن‌ها به سمت استفاده از اَبَرمنحنی‌های بیضوی[3] در رمزنگاری کشیده شدند. بنابراین ما در این مقاله به بررسی نحوهٔ استفادهٔ این نوع منحنی‌ها در رمزنگاری می‌پردازیم. در این پژوهش امنیت و کارایی این منحنی‌ها بررسی می‌شود.

واژگان کلیدی: رمزنگاری، مسئلهٔ لگاریتم گسسته، اَبَرمنحنی‌های بیضوی، ضرب اسکالر.

۱- مقدّمه

اَبَرمنحنی‌های بیضوی در بسیاری از زمینه‌های مهم پژوهشی مانند مولدهای اعداد شبه‌تصادفی[۱۸]، تئوری کدگذاری [۶،۴،۱۷]، الگوریتم‌های نظریه اعداد [۱،۱۶،۱۵] و رمزنگاری [۱۷،۲۱،۲۳،۱۹] مورد استفاده است. در سال ۱۹۸۹ کوبلیتز[4] [۲۰] پیشنهاد استفاده از ابرمنحنی‌های بیضوی را به‌عنوان جایگزینی برای منحنی‌های بیضوی به‌منظور طراحی سامانه‌های رمزنگاری مبتنی بر مسئله لگاریتم گسسته ارائه داد. نمونه‌هایی از پروتکل‌های رمزنگاری مبتنی بر ابرمنحنی‌های بیضوی در [۵،۱۳،۳۲،۲۲] آورده شده است. ابرمنحنی‌های بیضوی، تعمیم‌یافتهٔ منحنی‌های بیضوی هستند. به عبارت دیگر یک منحنی بیضوی یک ابرمنحنی بیضوی از جنس[5] یک است. کوتاه‌بودن طول کلید مزیت اصلی استفاده از ابرمنحنی‌های بیضوی است. بدین معنی که یک ابرمنحنی بیضوی در مقایسه با یک منحنی بیضوی برای رسیدن به یک سطح امنیتی، نیازمند میدان متناهی کوچک‌تری است. به‌عبارت دیگر مرتبهٔ گروه حاصل از تعریف یک ابرمنحنی بیضوی از جنس g بر روی یک میدان متناهی با q عنصر برابر q^g است. بنابراین برای ساختن یک گروه از مرتبهٔ 2^{160} با استفاده از منحنی‌های بیضوی ما نیازمند یک میدان متناهی با 2^{160} عضو هستیم. درحالی‌که برای ساختن یک گروه با اندازه مذکور با استفاده از ابرمنحنی‌های بیضوی از جنس دو فقط نیازمند یک میدان متناهی با عضو 2^{80} هستیم. به همین صورت برای ابرمنحنی‌های بیضوی از جنس سه و چهار به‌ترتیب نیازمند یک میدان متناهی با 2^{53} و 2^{51} هستیم [۲۳]. البته با توجه به پژوهش‌های انجام‌شده بر روی ابرمنحنی‌های بیضوی از جنس چهار و بالاتر، آشکار شده است که این نوع منحنی‌ها دارای سطح امنیتی کمتری هستند [۱۰]. برخلاف منحنی‌های بیضوی که ما برای حل مسئله لگاریتم گسسته امکان استفاده از الگوریتم حساب راهنما را نداریم، در ابرمنحنی‌های بیضوی، امکان استفاده از این حمله وجود دارد که این نقطه‌ضعفی مهم برای این منحنی‌ها در برابر منحنی‌های بیضوی است. با توجه به این‌که انجام محاسبات بر روی ابرمنحنی‌های

[1] Integer Factorization Problem
[2] Elliptic curve Cryptography (ECC)
[3] Hyperelliptic curve
[4] Koblitz
[5] Genus

* نویسندهٔ عهده‌دار مکاتبات

بیضوی پیچیده‌تر است، بنابراین پیداکردن ابرمنحنی‌های مناسب و بهبود محاسبات آنها از مهم‌ترین موارد برای عملی‌ساختن سامانه‌های رمزنگاری مبتنی بر این نوع منحنی‌ها است.

امروزه به‌طور کاملاً کارایی، می‌توانیم ابرمنحنی‌های از جنس سه و دو را به‌دست آوریم؛ به‌طوری‌که گروه حاصل دارای مرتبهٔ تاحدودی نخست باشد.

۲- مبانی ریاضی

در ادامه به توضیح برخی از مبانی ریاضی مورد نیاز می‌پردازیم.

تعریف۱: فرض کنیم $\overline{K}$ بستارجبری میدان K باشد. یک ابرمنحنی بیضوی از جنس[1] (درجه) $g(g\geq 1)$ بر روی K برابر است با معادله:

$$C: y^2+h(x)y=f(x)\in K[x,y] \quad (1).$$

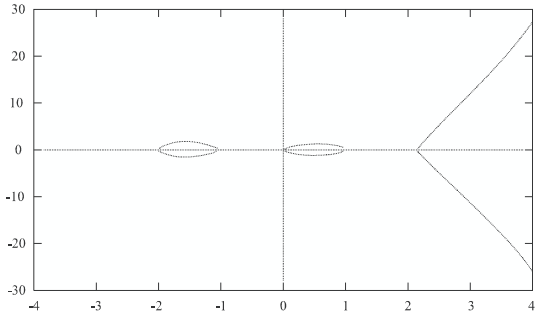
بطوریکه $h(x)\in K[x]$ یک چندجمله‌ای‌حداکثر از درجهٔ g، $f(x)\in K[x]$ یک چندجمله‌ای تکین از درجهٔ $2g+1$ هستند و درضمن این معادله و نیز معادلات مشتقات جزیی آن یعنی $h'(x)y-f'(x)=0$ و $2y+h(x)=0$ دارای جواب مشترک بر روی $\overline{K}$ نیستند. نقطهٔ $(x,y)\in\overline{K}\times\overline{K}$ بر روی منحنی C را یک نقطهٔ منفرد[2] می‌نامیم؛ هرگاه این نقطه به‌طور هم‌زمان جواب هر سه معادلهٔ اشاره شده در بالا باشد.

تعریف۲: فرض کنیم L یک میدان گسترش یافته از میدان K باشد. مجموعه C(L) عبارت است از همهٔ نقاط $P=(u,v)\in L\times L$ به‌طوری‌که در رابطهٔ (۱) صدق می‌کنند به همراه یک نقطه در بی‌نهایت که با ∞ نمایش داده می‌شود. مجموعهٔ $C(\overline{K})$ به‌طور خلاصه C نامیده می‌شود.

مثال۳: ابرمنحنی بیضوی با $g=2$ و $h(x)=0$ بر روی میدان اعداد حقیقی معرفی می‌کنیم.

$$C: y^2=x^5-5x^3+4x$$
$$=x(x-1)(x+1)(x-2)(x+2).$$

تعریف۴: فرض کنیم $P=(x,y)$ یک نقطهٔ متناهی بر روی منحنی C باشد. نقطهٔ مقابل P برابر $\tilde{P}=(x,-y-h(x))$ است، به‌طوری‌که $\tilde{P}$ بر روی C است. درضمن نقطهٔ مقابل ∞ را برابر خودش در نظر می‌گیریم. اگر یک نقطهٔ متناهی P در شرط $P=\tilde{P}$ صدق کند، آن‌را یک نقطهٔ مخصوص می‌نامیم و در غیر این‌صورت آن‌را یک نقطهٔ معمولی تعریف می‌کنیم.



(شکل-۱): منحنی C بر روی R

مثال۵: فرض کنیم منحنی $C: y^2+xy=x^5+5x^4+6x^2+x+3$ بر روی میدان متناهی Z_7 تعریف شده باشد. بنابراین $h(x)=x$، $f(x)=x^5+5x^4+6x^2+x+3$ و $g=2$ هستند. به‌طورکامل مشخص است که C دارای نقطهٔ منفرد نبوده و بنابراین C یک ابرمنحنی بیضوی است و داریم:

$$C(\mathbb{Z}_7)=\{\infty,(1,1),(1,5),(2,2),(2,3),(5,3),(5,6),(6,4)\}.$$

نقطهٔ (۴و۶) یک نقطهٔ مخصوص است.

۲-۱ محاسبهٔ مرتبهٔ گروه ابرمنحنی بیضوی

حال روشی برای محاسبهٔ تعداد اعضای گروه حاصل از یک ابرمنحنی بیضوی ارائه می‌دهیم. J را ژاکوبین ابرمنحنی بیضوی C تعریف شده بر روی F_q در نظر می‌گیریم. F_{q^n} را نیز بسط nام F_q و N_n را مرتبه گروه آبلی $J(F_{q^n})$ (یعنی $|J(F_{q^n})|$) در نظر می‌گیریم. M_n را نیز تعداد نقاط F_{q^n}- گویا بر روی C تعریف می‌کنیم.

تعریف۶: فرض کنیم C ابرمنحنی بیضوی تعریف‌شده بر روی F_q باشد. به‌ازای $r\geq 1$ مقدار $M_r=|C(F_{q^r})|$ را در نظر می‌گیریم. تابع زتا[3] ابرمنحنی C برابر سری توانی $Z_C(t)=\exp\left(\sum_{r\geq 1}M_r\frac{t^r}{r}\right)$ تعریف می‌کنیم.

حال به بیان خواصی از تابع زتا می‌پردازیم که از [۱۷] آورده شده‌اند.

قضیه ۷: فرض کنیم C ابرمنحنی بیضوی از جنس g تعریف‌شده بر روی F_q و $Z_C(t)$ تابع زتای C باشد.

i. $Z_C(t)\in Z(t)$، به‌طور دقیق‌تر داریم:

[1] Genus
[2] Singular
[3] Zeta

$Z_C(t)=\frac{P(t)}{(1-t)(1-qt)}$ به‌طوری‌که $P(t)$ یک چندجمله‌ای از درجهٔ $2g$ با ضرایب صحیح است. درحقیقت $P(t)$ به‌صورت زیر است:

$$P(t)=1+a_1t_0+\cdots+a_{g-1}t^{g-1}+a_gt^g+qa_{g-1}t^{g+1}+q^2a_{g-2}t^{g+2}+\cdots+q^{g-1}a_1t^{2g-1}+q^gt^{2g}.$$

ii. $P(t)$ به‌صورت $P(t)=\prod_{i=1}^{g}(1-\alpha_it)(1-\bar{\alpha}_it)$ تجزیه می‌شود به‌طوری‌که هر α_i یک عدد مختلط با قدر مطلق $\sqrt{q}$ بوده و $\bar{\alpha}_i$ مزدوج آن است.

iii. مقدار $N_n=\left|J\left(F_{q^n}\right)\right|$ برابر است با $N_n=\prod_{i=1}^{g}\left|1-\alpha_i^n\right|^2$.

بنابراین برای محاسبهٔ N_n کافی است که (i) ضرایب $a_1,a_2,\ldots,a_g$ چندجمله‌ای $P(t)$ را تعیین کنیم، (ii) $P(t)$ را تجزیه کرده و α_iها را به‌دست می‌آوریم، (iii) با استفاده از رابطهٔ بالا مقدار N_n را می‌یابیم. حال بدین منظور، اقدامات زیر را انجام می‌دهیم:

$$Z_C(t)=\frac{P(t)}{(1-t)(1-qt)}$$
$$\Rightarrow P(t)=(1-t)(1-qt)Z_C(t).$$

اکنون از طرفین رابطهٔ بالا لگاریتم گرفته و سپس نسبت به t مشتق می‌گیریم. بنابراین داریم:

$$\frac{P'(t)}{P(t)}=\sum_{r\geq 0}\left(M_{r+1}-1-q^{r+1}\right)t^r.$$

از آنجا که در دو طرف تساوی بالا ضرایب $t^0,t^1,\ldots,t^{g-1}$ برابر هستند. بنابراین g مقدار نخست $M_1,\ldots,M_g$ برای تعیین ضرایب $a_1,\ldots,a_g$ و درنتیجه N_n کافی هستند. اکنون روند محاسبه N_n را برای حالت $g=2$ به‌طور خلاصه بیان می‌کنیم:

۱- با استفاده از جستجوی جامع مقادیر M_1,M_2 را می‌یابیم.

۲- ضرایب $Z_C(t)$ را با استفاده از روابط $a_1=M_1-1-q$، $a_2=\frac{M_2-1-q^2+a_1^2}{2}$ به‌دست می‌آوریم.

۳- معادله $x^2+a_1x+(a_2-2q)=0$ را حل کرده تا جواب‌های λ_1,λ_2 را بیابیم.

۴- معادلات $x^2-\lambda_2x+q=0$, $x^2-\lambda_1x+q=0$ را حل می‌کنیم تا به‌ترتیب جواب‌های α_1,α_2 را بیابیم.

۵- مقدار $N_n=\left|1-\alpha_1^n\right|^2.\left|1-\alpha_2^n\right|^2$ نتیجه می‌شود.

نتیجه۸: فرض کنیم C ابرمنحنی بیضوی از جنس g تعریف‌شده بر روی F_q و $N_n=\left|J\left(F_{q^n}\right)\right|$ باشد. آن گاه رابطهٔ $\left(q^{\frac{n}{2}}-1\right)^{2g}\leq N_n\leq\left(q^{\frac{n}{2}}+1\right)^{2g}$ برقرار است و بنابراین $N_n\approx q^{ng}$.

اثبات: نتیجه بالا از قضیه ۷ (iii) به‌دست می‌آید.

مثال ۹: فرض کنیم C از جنس ۲ بر روی F_2 با معادله $C:y^2+y=x^5+x^3+x$ باشد. با استفاده از جستجوی جامع مقادیر $M_1=3,M_2=9$ را می‌یابیم. بنابراین $a_1=0,a_2=2$ هستند. جواب‌های معادله $x^2-2=0$ برابر $\lambda_1=\sqrt{2},\lambda_2=-\sqrt{2}$ است. با حل معادلهٔ $x^2-\sqrt{2}x+2=0$ جواب $\alpha_1=\frac{\sqrt{2}+\sqrt{6}i}{2}$ را و با حل معادلهٔ $x^2+\sqrt{2}x+2=0$ جواب $\alpha_1=\frac{-\sqrt{2}+\sqrt{6}i}{2}$ را به‌دست می‌آوریم. بنابراین داریم:

$$N_n=\left|1-\alpha_1^n\right|^2.\left|1-\alpha_2^n\right|^2=\begin{cases}2^{2n}+2^n+1 & n\equiv 1,5 \bmod 6\\ \left(2^n+2^{\frac{n}{2}}+1\right)^2 & n\equiv 2,4 \bmod 6\\ \left(2^n-1\right)^2 & n\equiv 3 \bmod 6\\ \left(2^{\frac{n}{2}}-1\right)^4 & n\equiv 0 \bmod 6\end{cases}$$

حال به ازای $n=101$ داریم:

$$N_{101}=6427752177035961102167848369367185711289268433934164747616257.$$

۲-۲ حملات

در این قسمت برخی از حملات ارائه‌شده به اَبَرمنحنی‌های بیضوی را بررسی می‌کنیم. ده سال بعد از این‌که کوبلیتز ابر منحنی‌های بیضوی را برای رمزنگاری (تبادل کلید دیفی-هلمن) معرفی کرد، بهترین حملات شناخته‌شده برای مسئله لگاریتم گسسته برروی این نوع منحنی‌ها الگوریتم‌های ریشهٔ مربع[1] بودند. الگوریتم‌های ریشهٔ مربع الگوریتم‌های عمومی هستند که برای حل مسئله لگاریتم گسسته در هر گروهی به‌کار می‌روند که شامل الگوریتم‌های قدم کوچک-قدم بزرگ شانک[2]، پلارد[3] و الگوریتم پلیگ-هلمن[1] هستند. زمان اجرای

[1] Square root
[2] Shanks Baby-Step Giant-Step
[3] Pollard

الگوریتم‌های نخست و دوم برابر مجذور اندازه گروه و زمان اجرای الگوریتم سوم برابر مجذور بزرگ‌ترین عامل نخست مرتبهٔ گروه است. ازآن‌جا که در کاربردهای رمزنگاری، مرتبهٔ گروه یا نخست و یا تاحدودی نخست است بنابراین تمام این الگوریتم‌ها را دارای زمان ریشه مربع می‌نامیم. نخستین الگوریتم حساب راهنما برای حل مسئله لگاریتم گسسته بر روی ژاکوبین یک اَبَرمنحنی بیضوی توسط آدلمن و همکارانش[2] [۲] ارائه شد. درضمن حملهٔ حساب راهنمای ارائه‌شده در [۱۰] نیز نخستین نمونه از یک حملهٔ عمومی به مسئله لگاریتم گسسته تعریف شده بر روی ژاکوبین یک ابر منحنی بیضوی با درجهٔ (جنس) کوچک بود که زمان اجرایی کمتر از مجذور مرتبهٔ گروه را داشت. البته فرض بر این است که درجهٔ ابر منحنی‌ها بزرگ‌تر از چهار است. حال در این قسمت به بیان برخی تعاریف و قضایای مورد نیاز می‌پردازیم.

تعریف۱۰: فرض کنیم D_1, D_2 دو عنصر عضو J_q باشند به‌طوری‌که $D_2 \in < D_1 >$ مسئله لگاریتم گسسته برروی ژاکوبین یک ابرمنحنی بیضوی به‌ازای جفت (D_1, D_2) برابر محاسبه کوچک‌ترین عدد صحیح $\lambda \in N$ است، به‌طوری‌که $D_2 = \lambda D_1$.

قضیه۱۱: فرض کنیم C یک اَبَرمنحنی بیضوی از درجهٔ g برروی میدان متناهی F_q باشد اگر $\ln q \le (2g+1)^{1-\varepsilon}$ باشد آن‌گاه ثابت $c \le 2.181$ وجود دارد، به‌طوری‌که مسئله لگاریتم گسسته در $J_C(F_q)$ در زمان $L_{q^{2g+1}}\left(\frac{1}{2}, c\right)$ قابل محاسبه باشد [۲].

قضیه۱۲: فرض کنیم C یک اَبَرمنحنی بیضوی از درجهٔ g برروی میدان متناهی F_q تعریف شده باشد. اگر $q > g!$ باشد آن گاه مسئله لگاریتم گسسته در $J_C(F_q)$ در زمان $O\left(g^3 q^{2+\varepsilon}\right)$ قابل محاسبه است [۱۰].

البته بهبودهای زیادی برای الگوریتم حساب راهنما بر روی ابر منحنی‌های بیضوی ارائه شده است که ما در اینجا به نتایج برخی از آن ها اشاره می‌کنیم:

فرض کنیم اندازهٔ پایهٔ تجزیه ($|P_B|$) برابر $O\left(g^2 q^{(g/(g+1))+\varepsilon}\right)$ باشد و C یک ابر منحنی بیضوی با درجهٔ g بر روی میدان متناهی F_q باشد، اگر $q > g!$ باشد آن‌گاه مسئله لگاریتم گسسته در $J_C(F_q)$ در زمان $O\left(g^5 q^{2-\frac{2}{g+1}+\varepsilon}\right)$ قابل حل است[۲۶]. حال اگر اندازهٔ پایهٔ تجزیه برابر $O\left(g^5 q^{\left(\left(g-\frac{1}{2}\right)/\left(g+\frac{1}{2}\right)\right)+\varepsilon}\right)$ باشد، آن‌گاه این زمان برابر $O\left(g^5 q^{2-\frac{4}{2g+1}+\varepsilon}\right)$ است[۳۱] و بنا فرض $O\left(g^5 q^{2-\frac{2}{g}+\varepsilon}\right)$ این زمان برابر $|P_B| = O\left(g^2 q^{((g-1)/g)+\varepsilon}\right)$ است [۱۲].

قضیه۱۳: به‌ازای $t > \frac{g}{Ln(q)}$ مسئلهٔ لگاریتم گسسته در $J_C(F_q)$ یک ابر منحنی بیضوی از درجهٔ g بر روی F_q حداکثر دارای پیچیدگی $L_{q^g}\left(\frac{1}{2}, \sqrt{2}\left(\left(1+\frac{1}{2t}\right)^{\frac{1}{2}} + \left(\frac{1}{2t}\right)^{\frac{1}{2}}\right)\right)$ است [۷،۸].

همان‌طور که گفته شد یک حملهٔ حساب راهنما با پیچیدگی $O\left(g^5 q^{2-\frac{2}{g}+\varepsilon}\right)$ وجود دارد و به‌ازای g=3,4 امنیت کمتر نیز است. به‌ازای ابر منحنی بیضوی از درجهٔ g=4 که بر روی F_2 تعریف‌شده، می‌توانیم مسئله لگاریتم گسسته در $J_C(F_q)$ را با پیچیدگی $O\left(\left|J_C(F_q)\right|^{0.375}\right) = O\left(q^{\frac{3}{2}+\varepsilon}\right)$ حل کنیم. بنابراین مسئلهٔ لگاریتم گسسته در این مورد از حالت کلی ذکرشده ضعیف‌تر است. به‌ازای g=3 این پیچیدگی برابر $O\left(\left|J_C(F_q)\right|^{0.44}\right) = O\left(q^{\frac{4}{3}+\varepsilon}\right)$ است. این نشان می‌دهد که به‌طور تقریبی ابر منحنی‌های از درجه g=3 از منحنی‌های بیضوی ضعیف‌تر هستند. بنابراین می‌توان گفت که به‌ازای اَبَرمنحنی‌های بیضوی از درجه $g \ge 5$ حملهٔ حساب راهنما قابل اعمال بوده و بنابراین برای استفاده در رمزنگاری کلید عمومی مناسب نیستند و یا در صورت استفاده از آن‌ها باید اندازه گروه را به‌طور مناسبی افزایش دهیم. همچنین از میان اَبَرمنحنی‌هایی بیضوی از درجات دیگر یعنی $g = 1,2,3,4$ به‌ازای $g = 3,4$ نیز باید اندازه گروه به‌گونه‌ای انتخاب شود که حملات حساب راهنما ارائه شده نظیر [۳۱] بر روی آن قابل اعمال نباشد.

یکی دیگر از انواع حملات موجود بر روی ابرمنحنی‌های بیضوی حملهٔ کاهش ویل[3] است. این حمله درصورتی‌که یا میدان متناهی مرکب باشد، یعنی به‌صورت F_{p^m} به‌طوری‌که m مرکب باشد، عملی است و یا m عددی اول است که به‌ازای یک عدد کوچک t در رابطهٔ

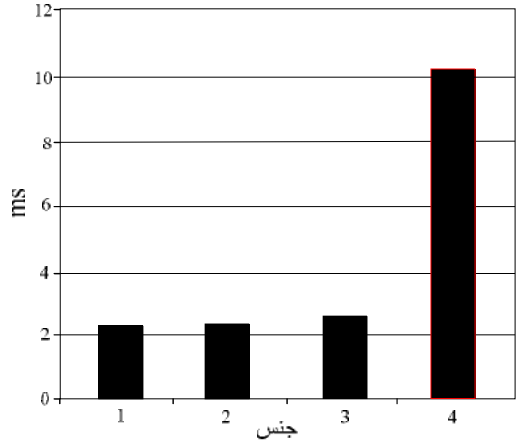
[1] Polling-Hellman
[2] Adelman, DeMarrais, Hang
[3] Weil Descent

$\left(2^t \equiv 1 \bmod m\right)$ صدق کند. بنابراین m نباید عدد اول مرسن[1] و یا عدد اول فرما[2] باشد. درصورت وقوع چنین حالاتی با استفاده از الگوریتم GHS و بهبودهای آن[۱۱] می‌توانیم مسئله لگاریتم گسسته را حل کنیم. بنابراین برای مقابله با این حمله منحنی مورد نظر باید یا بر روی یک میدان متناهی نخست به‌صورت F_p تعریف شود و یا این‌که میدان متناهی به‌صورت F_{p^m} باشد که m یک عدد اول باشد به‌طوری‌که مرتبهٔ عدد ۲ در گروه ضربی به هنگ p مقدار بزرگی باشد؛ یعنی در رابطهٔ $2^t \equiv 1 \bmod p$ مقدار t بزرگ باشد.

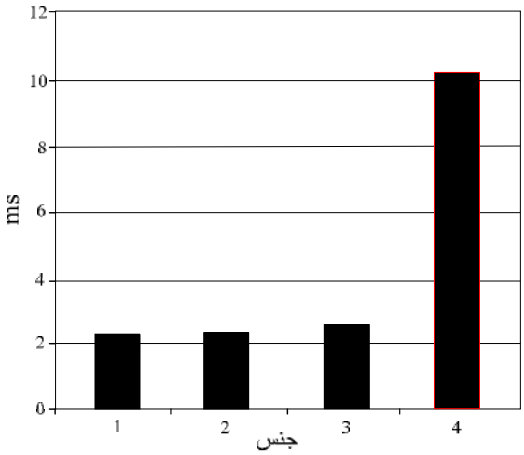
۳- مقایسهٔ بین HECC و ECC

حال برخی از نتایج ارائه‌شده در رابطه با مقایسهٔ بین HECC و ECC را ارائه می‌دهیم.

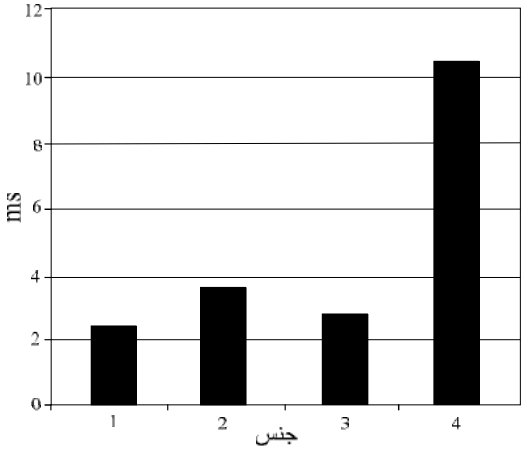
- ECC با مختصات تصویری به‌طورتقریبی در همه موارد کاراترین سامانه است؛
- ضرب اسکالر HECC با درجه g=3 و h(x)=1 همیشه سریع‌تر از HECC با درجه g=2 است؛
- ضرب اسکالر HECC با درجه g=3 در بیشتر موارد از ECC با مختصات آفینی سریع‌تر است؛
- به ازای سطح امنیتی یکسان پیاده‌سازی نرم‌افزاری HECC با درجه‌های g=2,3 و ECC کارایی مشابه‌ای دارند. درصورتی‌که برای پیاده‌سازی سخت‌افزاری HECC با درجات g=2,3 نسبت به ECC کاراتر است.
- ضرب اسکالر HECC از درجات g=2,3 و ECC با مختصات آفینی درصورتی‌که نسبت عمل ضرب به عمل معکوس‌کردن $\left(\frac{M}{I}\right)$ کوچک باشد، با هم برابرند و درصورتی‌که این نسبت بزرگ باشد، آن‌گاه HECC با درجات g=2,3 از ECC با مختصات آفینی کاراتر است.
- درصورتی‌که نسبت $\frac{M}{I}$ کوچک باشد، HECC با درجهٔ g=2 بسیارکارا است و اگر این نسبت بزرگ باشد HECC با درجهٔ g=3 کاراتر است.



(شکل-۲): مقایسه ضرب اسکالر بر روی Pentium 4 @ 1.8GHZ به ازای سطح امنیتی 2^{163} [۳۳]

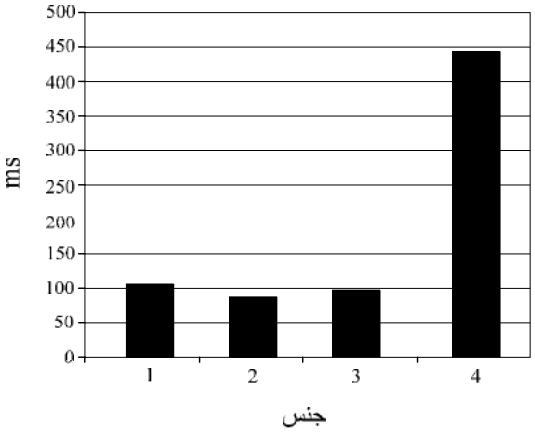


(شکل-۲): مقایسه ضرب اسکالر بر روی Pentium 4 @ 1.8GHZ به ازای سطح امنیتی 2^{163} [۳۳]



(شکل-۳): مقایسه ضرب اسکالر بر روی Pentium 4 @ 1.8GHZ به ازای سطح امنیتی 2^{180} [۳۳]

[1] Mersene
[2] Fermat



(شکل-۴): مقایسه ضرب اسکالر به‌ازای سطح امنیتی 2^{163} بر روی ARM 7 TDMI @ 80MHZ [۳۳]

همان‌طورکه مشاهده می‌کنیم در پیاده‌سازی سخت‌افزاری برای سطح امنیتی معادل 2^{160} منحنی HECC با درجهٔ g=2 از HECC با درجهٔ g=3 کاراتر است، درحالی‌که برای سطح امنیتی 2^{180} برعکس می‌باشد[۳۴].

تا قبل از این باور، بر این بود که با توجه به این‌که هزینهٔ محاسبات HECC با درجهٔ g=4 بسیار بیشتر از HECC با درجات کوچک‌تر است؛ بنابراین HECC با درجهٔ g=4برای کاربردهای عملی مناسب نیست. اما نتایج جدید به‌دست آمده نشان می‌دهد که برای کاربردهای با سطح امنیتی پایینHECC با درجهٔ g=4 از HECC با درجهٔ g=2سریع‌تر بوده و از نظر کارایی با HECC با درجهٔ g=3 برابری کرده و حتی می‌تواند جایگزینی برای ECC باشد. همچنین در پیاده‌سازی سخت‌افزاری برای کاربردهای با سطح امنیتی پایین مانند گروه‌هایی با مرتبهٔ 2^{128} محاسبات HECC ازدرجهٔ g=4 تاحدودی ۱.۴۶ برابر سریع‌تر از محاسبات HECC ازدرجهٔ g=2 بوده و کارایی مشابهی با HECC از درجهٔ g=3 دارند. درضمن در مقایسه با HECC از درجات g=2,3 HECC از درجهٔ g=4 برای پیاده‌سازی در ریزپردازنده‌های تعبیه‌شده[1] مناسب‌تر از پردازنده‌های با اهداف کلی است. برای دست‌یابی به سطح امنیتی معادل با 2^{128}می‌توانیم یک اَبرمنحنی بیضوی از درجهٔ g=4 را بر روی یک میدان متناهی $F_{2^{32}}$ تعریف کنیم. بنابراین پیاده‌سازی این منحنی‌ها بر روی پردازنده‌های ۳۲ بیتی بسیار کارا خواهد بود. این پیاده‌سازی نسبت به HECC با درجهٔ g=2 کاراتر و تاحدودی با نسبت به HECC با درجهٔ g=3 برابری می‌کند.

[1] Embedded Microprocessors

به‌طورمعمول در کاربردهایی که پردازنده‌های تعبیه‌شدهٔ کم هزینه استفاده می‌شود، نیاز به سطح امنیتی پایین‌تری داریم؛ درعمل یک گروه از مرتبهٔ 2^{128} کافی است. این سطح امنیتی به‌طورتقریبی بالاتر از سطح امنیتی حاصل از RSA-512 است [۳۰-۲۶]. نمونه‌هایی از طراحی و پیاده‌سازی پردازنده‌های ویژه برای ابرمنحنی‌های بیضوی در [۹،۳] آورده شده است.

۴- توابع زوج‌سازی بر روی اَبرمنحنی‌های بیضوی

فرض کنیم C یک ابرمنحنی بیضوی با درجهٔ g تعریف‌شده بر روی F_q باشد. همچنین فرض کنیم r یک عدد اول باشد. C را یک ابرمنحنی بیضوی از درجهٔ g تعریف‌شده بر روی F_q در نظر می‌گیریم؛ به‌طوری‌که $r \mid \neq J\left(F_q\right)$,$\gcd(r,g)=1$. همان‌طورکه می‌دانیم درجهٔ تعبیه $J\left(F_q\right)$ نسبت به r برابر است با کوچک‌ترین عدد صحیح k به‌طوری‌که $r \mid \left(q^k-1\right)$ به معادل درجهٔ تعبیه $J\left(F_q\right)$ نسبت به r برابر کوچک‌ترین عدد صحیح k است؛ به‌طوری‌که $F_{q^k}^*$ شامل گروه μ_r (ریشه‌های rام واحد) است. یکی دیگر از پارامترهای مهم در توابع زوج‌سازی پارامتری به‌نام ρ-value است که به‌صورت $\rho=\frac{g\log q}{\log r}$ تعریف می‌شود. این پارامتر به‌طورتقریبی برابر نسبت طول بیت $\#J\left(F_q\right)$ و طول بیت زیرگروه از مرتبهٔ r است. یک ژاکوبین با تعداد اعضای اولی دارای کوچک‌ترین مقدار ρ-value $(\rho\approx 1)$ است. اَبرمنحنی‌های بیضوی را که ژاکوبین آن‌ها دارای درجهٔ تعبیه کوچک و نیز دارای یک زیرگروه از مرتبهٔ اول بزرگ باشد مناسب استفاده در توابع زوج‌سازی یا به‌اصطلاح زوج‌سازی‌پسند[2] می‌نامیم. درعمل مقادیر $k \le 60$, $r>2^{160}$ مورد نیاز است. همان‌طور که درقبل اشاره شد، بهترین حمله به مسئله لگاریتم گسسته الگوریتم ρ- پلارد است که به‌صورت موازی پیاده‌سازی شده است. زمان اجرای این الگوریتم برابر $O\left(\sqrt{r}\right)$ است که r اندازهٔ بزرگ‌ترین زیرگروه نخست $J\left(F_q\right)$ است. به‌ازای اَبرمنحنی‌هایی از درجه $g=3,4$ حمله حساب راهنما به‌ترتیب با پیچیدگی‌های زیر موجود است:

[2] Pairing-friendly

$$O\left(q^{\frac{3}{2}+\varepsilon}\right)=O\left(\left|J\left(F_q\right)\right|^{\frac{3}{8}+\varepsilon}\right), O\left(q^{\frac{4}{3}+\varepsilon}\right)=O\left(\left|J\left(F_q\right)\right|^{\frac{4}{9}+\varepsilon}\right)$$

برای مقایسه با الگوریتم ρ - پلارد موازی‌سازی‌شده که وابسته به اندازهٔ زیرگروه از مرتبه r است، می‌توان گفت که اگر $\rho<\frac{9}{8}$ برای حالت g=3 و همچنین $\rho<\frac{4}{3}$ برای حالت g=4 باشد، آن‌گاه حملهٔ حساب راهنما به کران بالای حمله ρ - پلارد می‌رسد. به‌هرحال بهترین الگوریتم برای حل مسئله لگاریتم گسسته برای ابرمنحنی‌های از درجهٔ $g=2,3,4$ دارای زمان اجرای نمایی هستند. از سوی دیگر بهترین الگوریتم برای محاسله لگاریتم گسسته در میدان متناهی حمله حساب راهنما است که دارای زمان اجرای زیرنمایی نسبت به اندازه میدان است. بنابراین برای دست‌یابی به سطح امنیتی یکسان در هر دو گروه (گروه ضربی حاصل از میدان متناهی و گروه ژاکوبین حاصل از یک ابرمنحنی) باید اندازه q^k (گسترش‌یافتهٔ میدان) به‌طور مشخص از r بزرگ‌تر باشد. در جدول زیر مثال‌هایی برای اندازهٔ زیرگروه، اندازهٔ میدان گسترش‌یافته و اندازهٔ درجهٔ تعبیه به‌ازای سطح امنیتی یکسان ذکر شده است که در رابطهٔ $r\approx q^{g/\rho}$ صدق می‌کنند. زیرگروه‌ها از مرتبهٔ نخست و میدان‌های گسترش‌یافته (با مشخص‌های بزرگ) استاندارد NIST هستند.

(جدول-۶): درجهٔ تعبیه به‌ازای ابرمنحنی‌های بیضوی از جنس $g=2$ به‌ازای سطح امنیتی یکسان [26]

سطح امنیتی (بیت)	اندازهٔ زیرگروه (r)	اندازهٔ میدان گسترش‌یافته (q^k)	درجه تعبیه(k)					
			$\rho\approx1$	$\rho\approx2$	$\rho\approx3$	$\rho\approx4$	$\rho\approx6$	$\rho\approx8$
80	160	1024	6g	3g	2g	1.5g	g	0.8g
112	224	2048	10g	5g	3.3g	2.5g	1.6g	1.3g
128	256	3072	12g	6g	4g	3g	2g	1.5g
192	384	7680	20g	10g	6.6g	5g	3.3g	2.5g
256	512	15360	30g	15g	10g	7.5g	5g	3.8g

جدول بالا به‌ازای $\rho\approx2$ است. برای $g=2,3,4$ نیز می‌توانیم به‌صورت زیر عمل کنیم:

اگر مرتبهٔ ژاکوبین به‌طورتقریبی، نخست $(\rho\approx1)$ باشد آن‌گاه ما نیازمند تنظیم پارامترها برای مقابله با حمله حساب راهنما هستیم. برای $g=3$ ستون دوم جدول بالا را در مقدار $\frac{9}{8}$ و ستون چهارم را در مقدار $\frac{8}{9}$ ضرب می‌کنیم. برای $g=4$ ستون دوم را در مقدار $\frac{4}{3}$ و ستون چهارم را در مقدار $\frac{3}{4}$ ضرب می‌کنیم. درجهٔ تعبیه برای ابرمنحنی‌های بالا تکین از جنس $g=2$ در رابطهٔ $k\le12$ صدق می‌کند. برای ابرمنحنی‌های بیضوی معمولی از جنس $g=2$ در حالت‌های خاص نیز در رابطهٔ $k\le12$ صدق می‌کنند.

سریع‌ترین پیاده‌سازی ارائه‌شده برای توابع زوج‌سازی برای تابع زوج‌سازی η_T است که از یک ابرمنحنی بیضوی بالا تکین از درجهٔ $g=2$ تعریف‌شده بر روی میان متناهی با مشخص دو استفاده می‌کند. درجه تعبیه در این مورد برابر ۱۲ است[26]. در [26] نشان داده شده است که پیاده‌سازی زوج‌سازی موسوم به زوج‌سازی η بر روی ابرمنحنی‌های از درجه $g=2$ به‌طورتقریبی دارای کارایی مشابه با پیاده‌سازی زوج‌سازی تیت است. همچنین نشان داده شده است که بر روی ابرمنحنی‌های بیضوی از درجه $g=2$ زوج‌سازی موسوم به زوج‌سازی η_T نسبت به زوج‌سازی η کاراتر است.

درضمن نتایج ارائه‌شده در [26] نشان می‌دهد که پیاده‌سازی زوج‌سازی η_T بر روی ابرمنحنی‌های از درجه $g=2$ نسبت به پیاده‌سازی زوج‌سازی η_T بر روی منحنی‌های بیضوی بالا تکین تعریف‌شده بر روی F_{2^m} بسیار کاراتر است.

از نتایج دیگر ذکر شده در [26] می‌توان به این نکته اشاره کرد که محاسبه تابع زوج‌سازی بر روی ابرمنحنی‌های از درجه $g=3$ در مقایسه با ابرمنحنی‌های از درجه $g=2$ بسیار ناکارآمد است.

زمان پیاده‌سازی یک تابع زوج‌سازی بر روی آبَرمنحنی‌های از درجه $g=2$ تعریف‌شده بر روی F_p به‌طورتقریبی دو برابر زمان پیاده‌سازی زوج‌سازی بر روی منحنی‌های بیضوی تعریف‌شده بر روی F_p است. برای این‌که این فاصلهٔ زمانی را کاهش دهیم لازم است از ابر منحنی‌های بیضوی بالا تکین از درجه $g=2$ استفاده کنیم.

۴- نتیجه‌گیری

در این مقاله به معرفی ابرمنحنی‌های بیضوی پرداختیم و سعی کردیم، مقایسه‌هایی از نظر امنیت و کارایی انواع مختلف این منحنی‌ها ارائه دهیم. بنابراین به‌طور خلاصه می‌توان چنین نتیجه‌گیری کرد که به‌ازای اَبرمنحنی‌های بیضوی از درجهٔ $g \geq 5$ حملهٔ حساب راهنما قابل اعمال بوده و بنابراین برای استفاده در رمزنگاری کلید عمومی مناسب نیستند. در کاربردهایی که نیاز به سطح امنیتی پایین‌تری داریم، مانند شبکه‌های حس‌گر که دارای پردازنده‌های تعبیه‌شدهٔ کم‌هزینه هستند و در آنها الگوریتم‌های رمزنگاری با طول کلید کوچک‌تر استفاده می‌شوند، می‌توانیم از اَبرمنحنی‌های بیضوی از جنس $g = 2,3,4$ استفاده کنیم.

۵- مراجع

[1] L. Adleman and M. Huang, Primality Testing and Abelian Varieties over Finite Fields, Lecture Notes in Mathematics, 1512, Springer-Verlag, Berlin, 1992.

[2] L. Adleman, J. DeMarrais and M. Huang, A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q), Theoret. Comput. Sci. 226, 7–18, 1999.

[3] H.Ahmadi, A. Afzali-Kusha, M. Pedram, and M. Mosaffa, A Flexible, Prime-Field, Genus 2 Hyperelliptic- Curve Cryptography Processor with Low Power Consumption and Uniform Power Draw, ETRI Journal, http://dx.doi.org/10.4218/etrij.15.0114.0418.

[4] D. Le Brigand, Decoding of codes on hyperelliptic curves, Eurocode '90, Lecture Notes in Computer Science, 514, Springer-Verlag, 126-134, 1998.

[5] K. Chatterjee, A. De, and D. Gupta, Mutual Authentication Protocol Using Hyperelliptic Curve Cryptosystem in Constrained Devices, International Journal of Network Security, Vol.-15, No.1, PP.9-15, Jan. 2013.

[6] Y. Driencourt and J. Michon, Elliptic codes over a field of characteristic 2, Journal of Pure and Applied Algebra, 45, 15-39, 1987.

[7] A. Enge, P. Gaudry, A general framework for subexponential discrete logarithm algorithms, ActaArith. 102 No1, 83–103, 2002.

[8] A. Enge, Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time, Math. Comp. 71 No238, 729–742, 2002.

[9] J. Fan, L. Batina, and I. Verbauwhede, "Light-weight Implementation Options for Curve-based Cryptography: HECC, is Also Ready for RFID," in Proceedings of the 4th International Conference for Internet Technology and Secured Transactions, 2009. (ICITST 2009), London, UK, 2009, pp. 1-6.

[10] P. Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, Advances in Cryptology – Eurocrypt 2000, vol. 1807, Springer-Verlag, Berlin, 19–34, 2000.

[11] P. Gaudry, F. Hess, N. P. Smart, Extending the GHS Weil-descent attack, Advances in Cryptology – Eurocrypt 2002, Lecture Notes in Comput. Sci., vol. 2332, Springer-Verlag, Berlin, 29–44, 2002.

[12] P. Gaudry, N.The'riault, E. Thome , A double large prime variation for small genus hyperelliptic index calculus, preprint, 2004. http://eprint.iacr.org/2004/153/

[13] T. Gomathi, V. Manju, and N. Anuradha, An Efficient Blind Signature Authentication for Wireless Sensor Networks Using HECC, International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 10 No. 1 Oct. 2014, pp. 6-18 © 2014 Innovative Space of Scientific Research Journals http://www.ijisr.issr-journals.org/

[14] G. van der Geer, Codes and elliptic curves, in Efective Methods in Algebraic Geometry, Birkh auser, 159-168, 1991.

[15] H.W. Lenstra, Factoring integers with elliptic curves, Annals of Mathematics, 126, 649-673, 1987.

[16] H.W. Lenstra, J. Pila and C. Pomerance, A hyperelliptic smoothness test. I, Philosophical Transactions of the Royal Society of London A, 345, 397-408, 1993.

[17] J. van Lint and G. van der Geer, Introduction to Coding Theory and Algebraic Geometry, Birkh auser-Verlag, Basel, Germany, 1988.

[18] B. Kaliski, A pseudorandom bit generator based on elliptic logarithms, Advances in Cryptology { CRYPTO '86, Lecture Notes in Computer Science, 293, Springer- Verlag, 84-103, 1987.

[19] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48, 203-209, 1987.

[20] N. Koblitz, Hyperelliptic cryptosystems", Journal of Cryptology, 1, 139-150, 1989.

[21] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms tologarithms in a finite field. IEEE Transactions on Information Theory, 39:1639-1646,1993.

[22] D. Jian-zhi, C. Xiao-hui, and G. Qiong, "Design of Hyper Elliptic Curve Digital Signature, " International Conference on Information Technology and Computer Science, vol. 2 , no. 3, pp. 45-47, July 2009.

[23] A. Menezes, Y-H. Wu, R. J. Zuccherato. An elementary introduction to hyperelliptic curves, Published as Technical Report CORR 96-19, Department of C&O, University of Waterloo, Ontario,Canada, November 1996.

[24] V. Miller, Uses of elliptic curves in cryptography, Advances in Cryptology { Proceedings of Crypto '85, Lecture Notes in Computer Science, 218, Springer-Verlag, 417-426, 1986.

[25] L. B. Oliveira, D. F. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, TinyTate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes, Proceedings of the Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007), 318-323, 2007.

[26] Colm Ó Héigeartaigh, Michael Scott -Pairing Calculation on Supersingular Genus 2 Curves Selected Areas in Cryptography - SAC 2006, LNCS, 2007.

[27] J. Pelzi, Fast hyperelliptic curve cryptosystems for embedded microprocessors, Master's thesis, Ruhr-University of Bochum, 2002.

[28] J. Pelzl, T.Wollinger, J.Guajardo, J. and C. Paar.Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves. CHES 2003, LNCS 2779, 351–365. Springer, 2003.

[29] J. Pelzi,T. Wollinger,C. Paar Special hyperelliptic curve cryptosystems of genus two: Efficient arithmetic and fast implementation, Embedded Cryptographic Hardware: Design and Security, Nova Science Publishers, 2004.

[30] J. Pelzi, T. Wollinger, C. Paar, Low Cost Security: Explicit Formulae For Genus-4 Hyperelliptic curves, 2004.

[31] N. The'riault, Index calculus attack for hyperelliptic curves of small genus, Advances in Cryptology – Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer-Verlag, Berlin, 75–92, 2003.

[32] V. Vijayalakshmi , R. Sharmila , R. Shalini , Hierarchical key management scheme using Hyper Elliptic Curve Cryptography in Wireless Sensor Networks, 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), 2015 , DOI: 10.1109/ICSCN.2015.7219840.

[33] T. Wollinger, J. Pelzl, V. Wittelsberger, C. Paar, G. Saldamli, and, Elliptic &Hyperelliptic Curves on Embedded Platform, ACM Transactions in Embedded Computing Systems (TECS), vol. 3, no. 3, 509-533, 2004.

[34] T. Wollinger, Software and Hardware Implementation of Hyperelliptic Curv-e Cryptosystems.PhD thesis, Department of Elec-trical Engineering and Information Scien-ces, Ruhr-UniversitätBochum, Bochum, Ger-many, 2004.

رضا علیمرادی هم‌اکنون به‌عنوان استادیار گروه ریاضی و علوم کامپیوتر دانشگاه قم فعالیت می‌کند. ایشان کارشناسی خود را در رشتهٔ ریاضی از دانشگاه بوعلی سینای همدان و کارشناسی ارشد و دکترای خود را در همین رشته از دانشگاه علم و صنعت دریافت کرده‌اند. علایق پژوهشی ایشان رمزنگاری در شبکه‌های حس‌گر بی‌سیم و رمزنگاری نامتقارن مبتنی بر منحنی‌های بیضوی، به‌ویژه طراحی و تحلیل پروتکل‌های تعیین هویت و توافق کلید است.