پنجمین کنفرانس انجمن رمز ایران
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران
انجمن رمز ایران
Iranian Society of Cryptology



# طرحی جدید برای تعیین هویت بر مبنای منحنی‌های بیضوی و دوتایی ویل

مسعود هادیان دهکردی
دانشکده ریاضی
دانشگاه علم و صنعت ایران
mhadian@iust.ac.ir

رضا علیمرادی
مرکز تحقیقات ریاضیات کاربردی
دانشگاه علم و صنعت ایران
reza_alimoradi61@yahoo.com

**چکیده:** هدف اصلی در پروتکل‌های تعیین هویت شناسایی دقیق افراد مجاز برای ورود به یک سیستم می‌باشد. مهمترین ویژگی‌های یک پروتکل عبارتند از سطح امنیت و میزان اجرایی بودن آن. ما در این مقاله ابتدا منحنی بیضوی و دوتایی ویل را معرفی و سپس به بیان برخی روابط ریاضی موجود می‌پردازیم و بعد از آن با معرفی برخی پروتکل‌ها در زمینه تعیین هویت روش‌هایی جدید برای تعیین هویت بر مبنای منحنی‌های بیضوی و دوتایی ویل ارائه و سطح امنیت و میزان اجرایی بودن آنها را نشان می‌دهیم.

**واژه‌های کلیدی:** تعیین هویت، منحنی بیضوی، دوتایی ویل، پروتکل چالش و واکنش، اثبات با اطلاع صفر.

## ۱- مقدمه:

در سال‌های اخیر پروتکل‌های تعیین هویت[1] کاربردهای فراوانی در زمینه‌های مختلف مانند تجارت الکترونیکی و مباحث مربوط به آن پیدا کرده‌اند.

ما در اینجا بطور مختصر توضیحاتی در مورد تعیین هویت بیان می‌کنیم.

در یک پروتکل تعیین هویت؛ کاربر (آلیس) به سیستم (باب) ثابت می‌کند که واقعاً آلیس است که با او در حال ارتباط است.

انواع پروتکل‌های تعیین هویت عبارتند از:

الف) تعیین هویت با کلمات عبور،

ب) تعیین هویت چالش و واکنش[2].

آلیس می‌خواهد خود را به باب از طریق سیستم چالش و واکنش معرفی کند.

آلیس و باب اقدامات زیر را انجام می‌دهند:

- **چالش:** باب از آلیس یک سؤال می‌پرسد.

[1] Identification

[2] Challenge-Response

– **واکنش:** آلیس جواب سؤال را با استفاده از کلید مخفی[3] خود محاسبه و برای باب می‌فرستد.

– **تصدیق:** باب پاسخ را با استفاده از همان کلید مخفی یا کلید عمومی[4] متناظر با آن تصدیق می‌کند.

انواع سیستم‌های مورد استفاده در پروتکل‌های تعیین هویت عبارتند از:

الف) استفاده از سیستم‌های متقارن[5] که باب برای تصدیق نیازمند به دانستن کلید خصوصی آلیس می‌باشد.

ب) استفاده از سیستم‌های کلید عمومی که باب عمل تصدیق را بدون بدست آوردن کمترین اطلاعات از کلید مخفی آلیس انجام می‌دهد. این پروتکل‌ها را پروتکل‌های اثبات با اطلاع صفر[6] می‌نامند.[2,12]

بیشتر پروتکل‌های موجود براساس سختی مسأله تجزیه اعداد بنا نهاده شده‌اند مانند طرح فیات – شامیر در سیستم RSA و این امکان وجود دارد که این مسأله در آینده سخت نباشد بنابراین ما به دنبال یافتن طرح‌هایی با امنیت مناسب هستیم تا درمواقع ضروی از آنها به عنوان جایگزین استفاده کنیم.

در طرح ارائه شده در این مقاله از منحنی‌های بیضوی[7] و دوتایی ویل[8] استفاده شده و این طرح از نوع پروتکل‌های اثبات با اطلاع صفر است. جزئیات بیشتر در رابطه با پروتکل‌های اثبات با اطلاع صفر در [7] آمده است.

## ۲– تعاریف و قضایای مربوط به منحنی‌های بیضوی:

**تعریف ۱:** فرض کنیم $p>3$ یک عدد اول باشد. مجموعه جواب‌های $(x,y)$ عضو $Z_p \times Z_p$ که در معادله $y^2 \equiv x^3+ax+b \bmod p$ صدق می‌کنند که a و b ثابت‌هایی عضو $Z_p$ می‌باشند که رابطه $4a^3+27b^2 \neq 0 \bmod p$ برای آنها برقرار می‌باشد.

مجموعه فوق به همراه نقطه در بینهایت $\infty$ به همراه عمل دوتایی زیر تشکیل یک گروه آبلی جمع $E(Z_p)$ می‌دهند.

فرض کنیم $S=(x_1,y_1)$ و $Q=(x_2,y_2)$ نقاطی روی منحنی E باشند.

اگر $x_1=x_2$ و $y_1=-y_2$ آنگاه حاصل جمع دو نقطه را بصورت $Q+S=\infty$ در نظر می‌گیریم.

در غیر اینصورت قرار می‌دهیم $Q+S=(x_3,y_3)$ که در آن داریم:

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$
$$m = \begin{cases} (y_2-y_1)(x_2-x_1)^{-1} & S \neq Q \\ (3x_1^2+a)(2y_1)^{-1} & S = Q \end{cases}$$

و نیز داریم $Q+\infty=\infty+Q=Q$ یعنی $\infty$ عنصر همانی گروه فوق است.

گروه حاصل از منحنی بیضوی روی $E$ روی میدان $K$ نیز مانند فوق محاسبه می‌شود.

فرض کنیم $S_1, S_2$ دو عضو $E(Z_p)$ باشند بطوریکه $S_2=aS_1$. مسئله یافتن عدد $a$ به مسئله لگاریتم گسسته[9] $(DLP)$ معروف می‌باشد و ثابت شده است که حل این مسئله در گروه $E(Z_p)$ که با $(ECDLP)$[10] نمایش می‌دهند بسیار مشکل است.[3,5,10]

**تعریف ۲:** $E$ را منحنی بیضوی روی میدان $K$ در نظر می‌گیریم. مجموعه $E[n]=\{Q \in E(\overline{K}) \mid nQ=\infty\}$ را مجموعه نقاط تاب $n$ام[11] می‌نامیم که در آن n یک عدد طبیعی و $\overline{K}$ بستار جبری[12] $K$ است.

**قضیه۳:** فرض کنیم $E$ یک منحنی بیضوی بر روی میدان $K$ و $n$ یک عدد طبیعی باشد اگر مشخص میدان $K$، $n$ را عاد نکند و یا این مشخص برابر صفر باشد آنگاه $E[n] \cong Z_n \oplus Z_n$ و اگر مشخص میدان $K$ برابر $p>0$

[3] Private key
[4] Public key
[5] Symmetric System
[6] Zero-Knowledge Proof
[7] Elliptic Curve
[8] Weil Pairing
[9] Discrete Logarithm Problem
[10] Elliptic Curve Discrete Logarithm Problem
[11] n-Torsion
[12] Algebraic Closure

باشد بطوریکه $p \mid n$ و $n = p^r n'$ و p عاد نکند $n'$ را آنگاه داریم: $E[n] \cong Z_n \oplus Z_n$ یا $E[n] \cong Z_{n'} \oplus Z_{n'}$.

اثبات: به قضیه ۲ . ۳ از [11] مراجعه شود.

### ۲-۱- دوتایی ویل:

دوتایی ویل که روی مجموعه تاب nام یک منحنی بیضوی تعریف می‌شود نقش مهمی در مطالعه این منحنی‌ها ایفا می‌کند.

**قضیه۴:** فرض کنیم E یک منحنی بیضوی روی میدان $K$ و $n$ یک عدد صحیح مثبت که توسط مشخص میدان K عاد نمی‌شود.

یک دوتایی $e_n : E[n] \times E[n] \to \mu_n$ وجود دارد که آن را دوتایی ویل می‌نامیم و نیز دارای خواص زیر می‌باشد:

۱- $e_n$ دوخطی است[13] یعنی که برای هر $S, S_1, S_2, T, T_1, T_2 \in E[n]$ داریم:

$$e_n(S, T_1 + T_2) = e_n(S, T_1)\ e_n(S, T_2),$$
$$e_n(S_1 + S_2, T) = e_n(S_1, T)\ e_n(S_2, T).$$

۲- $e_n$ نسبت به هر دو متغیر ناتباهیده[14] است. یعنی
اگر برای هر $T \in E[n]$ رابطه $e_n(S, T) = 1$ برقرار باشد آنگاه $S = \infty$ و همچنین
اگر برای هر $S \in E[n]$ رابطه $e_n(S, T) = 1$ برقرار باشد آنگاه $T = \infty$ است.

۳- برای هر $T \in E[n]$ داریم: $e_n(T, T) = 1$.

۴- برای هر $S, T \in E[n]$ داریم:
$e_n(S, T) = e_n(T, S)^{-1}$.

اثبات: به قضیه ۹ . ۳ از [11] مراجعه شود.

در قضیه فوق داریم $E[n] \cong Z_n \oplus Z_n$ و نیز $\mu_n = \{x \in \overline{K} \mid x^n = 1\}$ را گروه ریشه‌های nام واحد می‌نامیم و از آنجا که مشخص میدان n را عاد نمی‌کند بنابراین $x^n = 1$ دارای n ریشه در $\overline{K}$ است. پس $\mu_n$ گروه دوری از مرتبه n است.

**قضیه۵:** فرض کنیم $\{T_1, T_2\}$ یک پایه برای $E[n] \cong Z_n \oplus Z_n$ باشد آنگاه $e_n(T_1, T_2)$ یک ریشه اولیه n ام واحد است.

اثبات: فرض کنیم $e_n(T_1, T_2) = \xi$ که $\xi^d = 1$. بنابراین $e_n(T_1, dT_2) = 1$ و همچنین داریم
$e_n(T_1, dT_2) = e_n(T_1, T_2)^d$.

فرض کنیم $S \in E[n]$ پس اعداد صحیح m , r وجود دارند که $S = rT_1 + mT_2$. بنابراین داریم:

$$\begin{aligned} e_n(S, dT_2) &= e_n(rT_1 + mT_2, dT_2) \\ &= e_n(rT_1, dT_2) e_n(mT_2, dT_2) \\ &= e_n(T_1, dT_2)^r e_n(T_2, T_2)^{md} \\ &= 1^{r+md} \\ &= 1. \end{aligned}$$

با استفاده از ویژگی ۲ قضیه ۴ خواهیم داشت که $dT_2 = \infty$. از آنجا که $dT_2 = \infty$ اگر و فقط اگر $n \mid d$ پس $\xi$ یک ریشه $n$ ام واحد است.

## ۳- طرح پیشنهادی اول:

آلیس نقطه $S_1 \in E(Z_p)$ را در نظر می‌گیرد و عدد $a \in \{2, \ldots, p-1\}$ را به تصادف انتخاب کرده و نقطه $S_2 = aS_1$ را بدست می‌آورد.

کلید خصوصی آلیس عدد $a$ و کلید عمومی او $(E, p, S_2, S_1)$ است. بدست آوردن کلید خصوصی آلیس مستلزم حل مسئله لگاریتم گسسته در گروه $E(Z_p)$ است که بسیار مشکل است. [9,10]

[13] Billinear
[14] Non Degenerated

در این پروتکل اثبات با اطلاع صفر، آلیس به باب ثابت می‌کند که راز (کلید خصوصی) را می‌داند. روش اجرای طرح بدین گونه است :

۱- **تعهد**[15]: آلیس عدد $b \in \{2,...,p-1\}$ را به تصادف انتخاب و نقطه $S_3 = bS_1$ را محاسبه و سپس مقدار $S_3$ را برای باب می‌فرستد.

۲- **چالش**[16]: باب عدد $d \in \{0,1\}$ را به تصادف انتخاب و برای آلیس می‌فرستد.

۳- **واکنش**[17]: آلیس مقدار $y = b + da$ را محاسبه و برای باب می‌فرستد.

۴- **تصدیق**[18]: باب هویت آلیس را می‌پذیرد اگر و فقط اگر رابطه $yS_1 = S_3 + dS_2$ برقرار باشد.

اثبات:

$$yS_1 = (b+da)S_1 = bS_1 + daS_1$$
$$= S_3 + dS_2$$

**لم ۶:** فرد مهاجم می‌تواند با احتمال $\frac{1}{2}$ خود را بجای آلیس به باب معرفی کند.

اثبات: فرد تصدیق کننده (باب) با احتمال $\frac{1}{2}$، مقدار $d=0$ را انتخاب می‌کند و آنگاه فرد مهاجم مقدار $y = b + 0a = b$ را برای باب می‌فرستد. آنگاه تصدیق کننده (باب) با محاسبه $yS_1 = bS_1 = S_3$ هویت مهاجم را قبول می‌کند.

### ۳-۱- تعمیم پروتکل فوق:

حال برای افزایش امنیت پروتکل فوق اقدامات زیر را انجام می‌دهیم. کلید خصوصی آلیس عدد $a$ و کلید عمومی او $(E, p, S_2, S_1)$ است.

آلیس و باب در پروتکل اول تغییرات زیر را انجام می‌دهند:

۱- **تعهد:** آلیس عدد $b_i \in \{2,...,p-1\}$ را به ازای هر $1 \le i \le t$ انتخاب و مقادیر $M_i = b_i S_1$ را محاسبه کرده و سپس مقدار $(M_1,...,M_t)$ را برای باب می‌فرستد.

۲- **چالش:** باب $(d_1,...,d_t) \in \{0,1\}^t$ را به تصادف انتخاب و برای آلیس می‌فرستد.

۳- **واکنش:** آلیس مقادیر $y_i = b_i + d_i a$ را برای هر $1 \le i \le t$ محاسبه کرده و سپس $y = (y_1,...,y_t)$ را برای باب می‌فرستد.

۴- **تصدیق:** باب هویت آلیس را می‌پذیرد اگر و فقط اگر برای هر $1 \le i \le t$ رابطه $y_i S_1 = M_i + d_i S_2$ برقرار باشد.

## ۴- طرح پیشنهادی دوم:

در این طرح از دوتایی ویل استفاده شده است. جزئیات بیشتر در رابطه با کاربردهای دوتایی ویل در رمزنگاری در [1,4,6,8] آمده است. کلید خصوصی آلیس عدد $a$ و کلید عمومی او $(E, p, S_2, S_1)$ است. آلیس و باب اقدامات زیر را انجام می‌دهند:

۱- ابتدا باب عدد صحیح n را بگونه‌ای انتخاب می‌کند که اولاً $p$ آنرا عاد نکند و ثانیاً $S_1, S_2 \in E[n]$ باشند و سپس $n$ و دوتایی ویل $e_n$ را برای آلیس می‌فرستد.

۲- **تعهد:** آلیس نقطه $S_3 \in E[n]$ و عدد $b \in \{2,...,n-1\}$ را انتخاب کرده و سپس آلیس مقادیر $S_3$ و $S_4 = bS_3$ و $e_n(S_1, S_4)$ را محاسبه و برای باب می‌فرستد.

۳- **چالش:** باب مقدار $d \in \{0,1\}$ را به تصادف انتخاب و برای آلیس می‌فرستد.

[15] Commitment
[16] Challenge
[17] Response
[18] Verification

۴- **واکنش:** آلیس مقدار $y = b + da$ را محاسبه و برای باب می‌فرستد.

۵- **تصدیق:** باب هویت آلیس را می‌پذیرد اگر و تنها اگررابطه

$$e_n(S_1, yS_3) = e_n(S_1, S_4)\ e_n(S_2, S_3)^d \qquad (1)$$

برقرار باشد.

اثبات:

$$\begin{aligned} e_n(S_1, yS_3) &= e_n(S_1, (b+da)S_3) \\ &= e_n(S_1, bS_3)\ e_n(S_1, daS_3) \\ &= e_n(S_1, S_4)\ e_n(S_1, S_3)^{da} \\ &= e_n(S_1, S_4)\ e_n(aS_1, S_3)^{d} \\ &= e_n(S_1, S_4)\ e_n(S_2, S_3)^{d}. \end{aligned}$$

**توجه:** در پروتکل فوق نقطه انتخابی $S_3$ نباید مضربی از $S_1$ باشد زیرا اگر به ازای عدد صحیح $k$ داشته باشیم $S_3 = kS_1$ آنگاه در مرحله تصدیق داریم:

طرف اول رابطه (۱) برابراست با:

$$\begin{aligned} e_n(S_1, yS_3) &= e_n(S_1, ykS_1) \\ &= e_n(S_1, S_1)^{ky} \\ &= 1^{ky} \\ &= 1 \end{aligned}$$

طرف دوم رابطه (۱) برابراست با:

$$\begin{aligned} e_n(S_1, S_4)\ e_n(S_2, S_3)^d &= e_n(S_1, bS_3)\, e_n(aS_1, kS_1)^d \\ &= e_n(S_1, bkS_1)\ e_n(S_1, S_1)^{akd} \\ &= e_n(S_1, S_1)^{bk}\ 1^{akd} \\ &= 1^{bk} \\ &= 1 \end{aligned}$$

بنابراین با تساوی این دو مقدار عمل تصدیق برای هر مقدار دلخواه $a$ برقرار خواهد شد.

برای آگاهی یافتن از اینکه آیا $S_3$ مضربی از $S_1$ است یا نه از قضیه زیر استفاده می‌کنیم.

**قضیه ۷:** فرض کنیم $S_1, S_3 \in E(Z_p)$ و $N$ مرتبهٔ نقطهٔ $S_1$ باشد و $\gcd(N, p) = 1$ آنگاه وجود دارد عدد صحیحی مانند $k$ که $S_3 = kS_1$ اگر و فقط اگر $NS_3 = \infty$ ، $e_N(S_1, S_3) = 1$.

اثبات: اگر $S_3 = kS_1$ آنگاه $NS_3 = kNS_1 = \infty$ و همچنین

$$\begin{aligned} e_N(S_1, S_3) &= e_N(S_1, kS_1) \\ &= e_N(S_1, S_1)^k \\ &= 1^k \\ &= 1 \end{aligned}$$

برعکس، اگر $NS_3 = \infty$ است و چون $\gcd(N, p) = 1$ بنابراین با استفاده از قضیه ۳ داریم $E[N] = Z_N \oplus Z_N$. یک نقطهٔ $T$ را چنان انتخاب می‌کنیم که $\{S_1, T\}$ یک پایه برای $E[N]$ باشد آنگاه برای اعداد صحیحی مانند $r, m$ داریم $S_3 = rS_1 + mT$. با استفاده از قضیه ۵، $e_N(S_1, T) = \xi$ یک ریشه اولیه $N$ ام واحد است.

بنابراین اگر $e_N(S_1, S_3) = 1$ آنگاه داریم:

$$\begin{aligned} 1 &= e_N(S_1, S_3) \\ &= e_N(S_1, rS_1 + mT) \\ &= e_N(S_1, rS_1)\ e_N(S_1, mT) \\ &= e_N(S_1, S_1)^r\ e_N(S_1, T)^m \\ &= 1^r \ .\ \xi^m \\ &= \xi^m \end{aligned}$$

این نتیجه می‌دهد که $m \equiv 0 \pmod N$

همچنین $mT = \infty$ بنابراین

$S_3$ یعنی $S_3 = rS_1 + mT = rS_1 + \infty = rS_1$

مضربی از $S_1$ است.

**لم ۸:** فرد مهاجم می‌تواند با احتمال $\frac{1}{2}$ خود را به جای آلیس به باب معرفی کند.

اثبات: فرد تصدیق کننده (باب) با احتمال $\frac{1}{2}$، عدد $d=0$ را انتخاب می‌کند آنگاه فرد مهاجم مقدار $y=b+0a$ را برای باب می‌فرستد. آنگاه تصدیق‌کننده (باب) با محاسبه

$$e_n(S_1, yS_3) = e_n(S_1, bS_3) = e_n(S_1, S_4)$$

برای طرف اول رابطه (۱) و با محاسبه

$$e_n(S_1, S_4)\ e_n(S_2, S_3)^0 = e_n(S_1, S_4)$$

برای طرف دوم رابطه (۱) هویت فرد مهاجم را می‌پذیرد.

### ۴-۱ تعمیم پروتکل فوق:

حال برای افزایش امنیت پروتکل فوق اقدامات زیر را انجام می‌دهیم. آلیس و باب در پروتکل دوم تغییرات زیر را انجام می‌دهند.

- در مرحله چالش باب $(d_1,...,d_t) \in \{0,1\}^t$ را انتخاب می‌کند که $d_i \in \{0,1\}$.

- در مرحله واکنش آلیس مقادیر $(y_1,...,y_t)$ را که در آن $y_i = b + d_i a$ می‌باشد را محاسبه و برای باب می‌فرستد.

- در مرحله تصدیق باب هویت آلیس را می‌پذیرد اگر و تنها اگر به ازای هر $1 \le i \le t$ رابطه زیر برقرار باشد:

$$e_n(S_1, y_i S_3) = e_n(S_1, S_4)\ e_n(S_2, S_3)^{d_i}.$$

**لم ۹:** در تعمیم پروتکل‌های اول و دوم، فرد مهاجم با احتمال $\frac{1}{2^t}$ می‌تواند تصدیق‌کننده را در پروتکل فریب دهد.

اثبات: چون برای هر $d_i$ دو انتخاب وجود دارد پس فضای نمونه برابر است با $2^t$. از طرفی فرد مهاجم زمانی نیازمند به دانستن مقدار صحیح a (کلید خصوصی آلیس) نیست که به ازای هر i، $d_i = 0$ یعنی $(d_1,...,d_t) = (0,...,0)$ روی دهد پس احتمال فریب دادن فرد تصدیق‌کننده توسط فرد مهاجم برابر $\frac{1}{2^t}$ است یعنی فرد مهاجم با احتمال $1-\frac{1}{2^t} = \frac{2^t-1}{2^t}$ لو خواهد رفت.

### ۴-۲ طراحی یک حمله برای پروتکل فوق؟!

با توجه به قضیه‌های ۳ و ۵ ذکر شده در بالا حمله کننده برای انجام موفق پروتکل اقدامات زیر را انجام می‌دهد:

نقطه $T_1 \in E[n]$ را به گونه‌ای می‌یابد که $\{S_3, T_1\}$ یک پایه برای $E[n]$ تشکیل دهند. از آنجا که $E[n] \cong Z_n \oplus Z_n$ بنابراین حتماً چنین $T_1 \in E[n]$ وجود دارد.

حال فرد مهاجم اعداد صحیح $r, m$ را به گونه‌ای تعیین می‌کند که رابطه $S_1 = rS_3 + mT_1$ برقرار باشد.

فرض کنیم $e_n(T_1, S_3) = \xi$ که $\xi$ یک ریشه اولیه $n$ام واحد است، حال باب در مرحله تصدیق اقدامات زیر را انجام می‌دهد:

برای طرف اول رابطه (۱) داریم:

$$\begin{aligned} e_n(S_1, yS_3) &= e_n(rS_3 + mT_1, yS_3) \\ &= e_n(rS_3, yS_3)\ e_n(mT_1, yS_3) \\ &= e_n(S_3, S_3)^{ry}\ e_n(T_1, S_3)^{my} \\ &= 1^{ry}\ \xi^{my} \\ &= \xi^{my}. \end{aligned}$$

و برای طرف دوم رابطه (۱) داریم:

$$\begin{aligned} & e_n(S_1, S_4)\ e_n(S_2, S_3)^d \\ &= e_n(rS_3 + mT_1, bS_3)\ e_n(a(rS_3 + mT_1), S_3)^d = \\ & e_n(S_3, S_3)^{rb} e_n(T_1, S_3)^{mb} e_n(S_3, S_3)^{ard} e_n(T_1, S_3)^{amd} \\ &= 1^{rb}\ \xi^{mb}\ 1^{ard}\ \xi^{amd} \\ &= \xi^{mb+amd} \\ &= \xi^{m(b+ad)} \\ &= \xi^{my}. \end{aligned}$$

با توجه به روابط فوق مشاهده می‌کنیم که دو مقدار بدست آمده برابر می‌باشند بنابراین طبق دستور پروتکل فوق باب عمل تصدیق را انجام می‌دهد و حمله‌کننده موفق خواهد شد!

( توجه: اگر فرد مهاجم نقطه $T_1 \in E[n]$ را به گونه‌ای بیابد که $\{S_1, T_1\}$ یک پایه برای $E[n]$ تشکیل دهند آنگاه رابطه $S_3 = r' S_1 + m' T_1$ برای برخی اعداد صحیح مانند $r', m'$ برقرار خواهد بود. بنابراین همانند عملیات فوق عمل تصدیق انجام خواهد گرفت.)

به نظر می‌رسد که روش فوق بتواند حمله‌ای موفق بر پروتکل ارائه شده باشد ولی باید توجه داشته باشیم که حمله‌کننده برای یافتن اعداد صحیح $r, m$ که در رابطه $S_1 = r S_3 + m T_1$ صدق کنند مجدداً با مسأله لگاریتم گسسته روبرو می‌شود که سختی حل آن قبلاً به اثبات رسیده است.

## ۵- نتیجه‌گیری:

در این مقاله به کمک منحنی‌های بیضوی و دوتایی ویل طرح‌هایی برای تعیین هویت ارائه شده که از نوع اثبات با اطلاع صفر بوده و ضمن داشتن امنیت کافی از توابع درهم نیز در آنها استفاده نشده است بنابراین می‌توانند جایگزینی مناسب برای پروتکل‌هایی باشند که براساس سختی مسأله تجزیه اعداد بنا نهاده شده‌اند مانند طرح فیات – شامیر در سیستم RSA.

## ۶- مراجع:

[1]Benho D., and Franklin M., Identity based encryption from the Weil pairing. In advances in Cryptology, Crypto (2001) (Santa Barbara, CA), volume 2139 of Lecture Notes in Comput.Sci., pages 213-229. *Spriner-Verlag*, Berlin, (2001).
[2]Buchmann J.A, Introduction to Cryptogaphy, *Springer-verlag*, (2001).
[3]Enge A., Elliptic curves and their applications to cryptography: An introduction. *Kluwer Academic Publishers*, ordrechet,(1999).
[4]Frey G., Muller M., and ruck H.G., The Tate pairng and the discrete logarithm applied to elliptic curve cryptosystems. IEEE Trans. Inform.Theory, 45(5):1717-1719,(1999).
[5]Frey G., and ruck H.G., A remark concerning m-divisiblity and the discrete logarithm in the divisor class group of curves. Math.Comp.,62(206):865-874, (1994).
[6]Galbraith S., Harrison K., and Soldera D., Implementing the Tate pairing. In Algorithmic number theory (Sydney Australia,2002), volume 2369 of Lecture Note in Comput.Sci., pages 324-337. *Spriner-Verlag*,Berlin,2002.
[7]Goldreich O., Modern Cryptography, Probabilistic Proofs and Pseudorandomness, *Springer-verlag*, (1999).
[8]Joux A., Weil and Tate pairing as building blocks for puplic key cryptosystems. In Algorithmic Number Theory (Sydney Australia, 2002) volum 2369 of Lecture Notes in Comput.Sci., pages 20-32. *Spriner-Verlag*, Berlin, (2002).
[9]Menzese A.J., Oorschot P.C., and Vanstone S.A., Handbook of applied cryptography. CRC Press Series on Discrete Mathematics and its Applications. *CRC Press, Boca Raton, FL* (1997). With a forward by R. L. Rivest.
[10]Stinson D., Cryptogaphy, *CRC Press, Boca Raton, Florida*, (1995).
[11]Washington L., Elliptic curve in Number theory and Cryptography CRC Press Series on Discrete Mathematics and its Applications.*CRC Press, Boca Raton, Florida* (2003).
[12]رضا علیمرادی- کاربرد منحنی‌های بیضوی در رمزنگاری- پایانامه کارشناسی ارشد رشته ریاضی محض- دانشگاه علم و صنعت ایران- پاییز ۱۳۸۵