هفتمین کنفرانس بین المللی انجمن رمز ایران
۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی
انجمن رمزایران
دانشگاه صنعتی خواجه نصیرالدین طوسی

پروتکل توافق کلید چندتایی مقاوم در برابر بازیابی قانونی کلید

مسعود هادیان دهکردی [۱]، رضا علیمرادی [۲و۱]
تهران، دانشگاه علم و صنعت ایران، دانشکده ریاضی [۱]
تهران، پژوهشکده پردازش هوشمند علائم [۲]
mhadian@iust.ac.ir ، *alimoradi.r@gmail.com*

چکیده

بازیابی قانونی کلید یکی از نقاط ضعف اساسی سیستم‌های رمزنگاری مبتنی بر شناسه می‌باشد. برای حل این مشکل سیستم‌های رمزنگاری کلید عمومی بدون گواهی ارائه شد. ما در این مقاله یک طرح توافق کلید چندتایی از نوع کلید عمومی بدون گواهی ارائه می‌دهیم که دارای ویژگی‌های امنیتی مهم مانند امنیت پیشرو کامل، امنیت قوی و اثبات با اطلاع صفر می‌باشد. تعداد کلیدهای مخفی مشترک که درهر نشست توسط این طرح تولید می‌شوند نسبت به بسیاری از طرح‌های موجود بیشتر می‌باشد. در این مقاله امنیت و کارائی طرح خود را با چندین طرح معروف مقایسه می‌کنیم.

واژه های کلیدی

توافق کلید چندتایی، توابع زوج سازی، بازیابی قانونی کلید، سیستم‌های رمزنگاری کلید عمومی بدون گواهی.

۱- مقدمه !

در یک سیستم کلید عمومی مبتنی بر گواهی[۱] قبل از استفاده کلید عمومی[۲] یک کاربر، باید گواهی وی توسط دیگر کاربران تأیید شود. بنابراین این سیستم نیازمند حافظه و زمان محاسبه زیادی برای ذخیره و تأیید کلید عمومی هر کاربر و گواهی متناظر با آن می‌باشد. Shamir [24] در سال ۱۹۸۴ به منظور ساده کردن فرآیند مدیریت کلید در سیستم کلید عمومی مبتنی بر گواهی، طرح‌های رمزنگاری مبتنی بر شناسه[۳] را معرفی نمود. بعد از آن طرح‌های رمزنگاری مبتنی بر شناسه زیادی ارائه شد. ایده اصلی در رمزنگاری مبتنی بر شناسه این است که اطلاعات شناسه هر کاربر مانند شماره تلفن، آدرس IP یا آدرس پست الکترونیکی به عنوان کلید عمومی وی در نظر گرفته می‌شود. به عبارت دیگر کلید عمومی یک کاربر به‌جای اینکه از گواهی صادر شده توسط یک مرکز صدور گواهی[۴] استخراج شود مستقیماً از شناسه عمومی وی حاصل می‌شود. بعد از مطرح شدن ایده رمزنگاری مبتنی بر شناسه توسط Shamir طرح‌های زیادی در این زمینه ارائه شد ولی مسئله طراحی یک سیستم رمزنگاری مبتنی بر شناسه کارا و امن حل نشده باقی مانده تا اینکه در سال ۲۰۰۱ یک طرح رمزنگاری مبتنی بر شناسه توسط Boneh-Fronklin[3] ارائه شد که بسیار عملی بود و دیگر نیازی به گواهی دیجیتال نداشت. در این روش کاربر کلید مخفی خود را بعد از انجام واکنش با یک مرکز تولید کلید مورد اطمینان بدست می‌آورد. در حقیقت مرکز تولید کلید با استفاده از ترکیب کلید اصلی مخفی خود و شناسه عمومی یک کاربر برای وی کلید خصوصی تولید و آنرا از طریق یک کانال امن به وی می‌رساند. همان‌طور که مشخص است مرکز تولید کلید مقدار کلید خصوصی کاربر را دارا می‌باشد. بنابراین این مرکز قادر است هویت کاربر را جعل کند و یا از این کلید به نحوی استفاده کند که برای شخص کاربر نامطلوب باشد مانند بازیابی قانونی کلید[۵] . در سال ۲۰۰۳، برای حل این مشکل Al-Riyami-Paterson [1] طرحی ارائه دادند که بنام رمزنگاری کلید عمومی بدون گواهی[۶] معروف شد. در این روش کاربر علاوه بر کلید خصوصی طولانی مدت که توسط مرکز تولید کلید صادر می‌شود یک کلید خصوصی موقت نیز تولید می‌کند که مقدار آن فقط در اختیار خود می‌باشد. شخص کاربر حین انجام پروتکل از هر دو کلید خصوصی خود استفاده می‌کند. به دلیل اینکه مرکز تولید کلید توانایی بدست آوردن کلید خصوصی تولید شده توسط کاربر را ندارد بنابراین مشکلات سیستم‌های مبتنی بر شناسه مانند بازیابی قانونی کلید رفع خواهد شد. در این مقاله، ما به یک طرح توافق کلید چندتایی ارائه می‌دهیم که از نوع کلید عمومی بدون گواهی

[1] Certificate-based public key system
[2] Public Key
[3] Identity – Based Cryptography (IBC)
[4] Certificate Authority(CA)
[5] Key scrow
[6] Certificate less public key cryptography (CL-PKG)

می‌باشد. طرح‌های توافق کلید یکی از مباحث مهم حوزه رمزنگاری می‌باشد و برای ساخت کلید مخفی مشترک بین دو قسمت از یک شبکه نا امن می‌باشند. طرحهای توافق کلید چندتایی[1] توانایی توافق بر روی تعداد بیشتری کلید نسبت به طرحهای توافق تک کلیدی دارا می‌باشند و بنابراین بسیار کاراتر می‌باشند. طرح ارائه شده در این مقاله برای تصدیق هویت یکی از طرفین از روش تعیین هویت چالش– واکنش مبتنی بر کلید عمومی استفاده می‌کند. بنابراین این طرح نسبت به بسیاری از طرحهای توافق کلید موجود دارای امنیت و کارائی بیشتر می‌باشد. ادامهٔ مطالب این مقاله بدین ترتیب می‌باشد که در بخش بعدی برخی مقدمات را ارائه می‌دهیم. در بخش ۳ یک طرح توافق کلید چند تایی از نوع بدون گواهی ارائه می‌دهیم. در بخش ۴ پیچیدگی محاسباتی را بیان می‌کنیم و در بخش ۵ بررسی‌های امنیتی طرح خود را نشان می‌دهیم. در بخش ۶ نیز به مقایسه خود با برخی از طرح‌های موجود می‌پردازیم.

۲- مفاهیم مقدماتی:

تعریف۱: فرض کنیم q یک عدد اول باشد. فرض کنیم G_1 و G_2 دو گروه دوری از مرتبه q باشند. یک زوج سازی[2] نگاشتی است به صورت $e:G_1\times G_1\to G_2$ که دارای خواص زیر باشد:

۱. *دوخطی بودن*[3]: به ازای هر $P,Q\in G_1$ و به ازای هر $a,b\in Z_q^*$ داریم:
$$e(aP,bQ)=e(P,Q)^{ab}.$$

۲. *ناتباهیدگی*[4]: نقطه‌ای مانند $P\in G_1$ وجود دارد به طوری که $e(P,P)\neq 1$.

۳. *محاسبه پذیری*: مقدار $e(P,P)$ در یک زمان چند جمله‌ای قابل محاسبه باشد.

علائم اختصاری به کار رفته در این مقاله در جدول زیر آورده شده است.

IDA,IDB	شناسه‌های آلیس و باب
H,H_1	توابع درهم‌ساز
p,q	اعداد اول بزرگ
P	نقطه مولد G از مرتبه q
G_1,G_3	زیر گروه‌هایی از مرتبه q
e	تابع زوج سازی
KGC	مرکز تولید کلید
s	کلید خصوصی KGC
P_{pub}	کلید عمومی KGC
S_{IDA},S_{IDB}	کلید خصوصی تولیدی KGC برای آلیس و باب
Q_{IDA},Q_{IDB}	نقاط متناظر با شناسه‌های آلیس و باب
a,b	کلید خصوصی تولید شده توسط آلیس و باب
$P_{A,pub},P_{B,pub}$	کلید عمومی تولید شده توسط آلیس و باب
m,n	مقادیر تصادفی تولید شده توسط آلیس و باب در اجرای پروتکل
M,N	نقاط متناظر با مقادیر تصادفی تولید شده توسط آلیس و باب
f,f'	اعداد متناظر با مقادیر تصادفی تولید شده توسط آلیس و باب در طول اجرای پروتکل
Y	جواب امضاء ارسال شده توسط باب برای آلیس
S	محاسبه شده توسط آلیس برای ارسال به باب
D	امضای آلیس جهت ارسال به باب

جدول ۱

۳- طرح پیشنهادی:

طرح ارائه شده در این مقاله از نوع کلید عمومی بدون گواهی بوده و دارای سه مرحلهٔ کلی آماده‌سازی[5]، استخراج کلید[6] و توافق کلید می‌باشد. حال هر یک از مراحل را بیان می‌کنیم.

- *مرحلهٔ آماده‌سازی:*

فرض کنیم E یک منحنی بیضوی که بر روی میدان F_p تعریف شده است. مرکز تولید کلید KGC یک نقطه $P\in E(F_p)$ را به گونه‌ای انتخاب می‌کند که مرتبهٔ آن برابر عدد اول q باشد. حال KGC گروههای دوری $G_1=\langle P\rangle, G_2$ را که از مرتبهٔ q می‌باشند انتخاب و سپس تابع زوج‌سازی $e:G_1\times G_1\to G_2$ را در نظر می‌گیرد.سپس (KGC) توابع درهم $H:\{0,1\}^*\to Z_q^*, H_1:\{0,1\}^*\to G_1$ را انتخاب می‌کند. تابع H یک رشته به طول دلخواه را به یک نقطه عضو

[1] Multiple Key Agreement
[2] Pairing
[3] Bilinear
[4] Non Degenerated
[5] Setup
[6] Extract

$G_1 = \langle P \rangle$ می‌برد. مرکز تولید کلید (KGC) برای تولید کلید خصوصی خود مقدار $s \in Z_q^*$ رابه تصادف انتخاب و مقدار کلید عمومی خود یعنی $P_{pub} = sP$ را محاسبه می‌کند. پارامترهای عمومی سیستم برابر $\{p, q, G_1, G_2, E, P, P_{pub}, H, H_1, e\}$ بوده و مقدار $s \in Z_q^*$ نیز باید مخفی بماند.

- *مرحلهٔ استخراج کلید:*

مرکز تولید کلید برای هر کاربر با شناسه $ID \in \{0,1\}^*$ و کلید عمومی $Q_{ID} = H_1(ID)$ مقدار $S_{ID} = sQ_{ID}$ را بعنوان کلید خصوصی کاربر مورد نظر محاسبه و از طریق یک کانال امن برای وی ارسال می‌کند. بنابراین یک جفت کلید مبتنی بر شناسه برابر $\{Q_{ID}, S_{ID}\}$ می‌باشد بطوریکه $ID \in \{0,1\}^*$. هر کاربر با شناسه $Q_{ID}, S_{ID} \in G_1$ می‌تواند با بررسی رابطهٔ $e(P, S_{ID}) = e(P_{pub}, Q_{ID})$ کلید خصوصی خود را تصدیق کند. بنابراین KGC برای هر یک از طرفین آلیس و باب یک جفت کلید مبتنی بر شناسه تولید می‌کند بطوریکه مقدار $\{Q_{IDA}, S_{IDA}\}$ برای طرف آلیس و مقدار $\{Q_{IDB}, S_{IDB}\}$ برای طرف باب می‌باشد. حال آلیس و باب برای تولید کلید خصوصی دیگر خود بدین ترتیب عمل می‌کنند. آلیس مقدار $a \in Z_r^*$ را بصورت تصادفی انتخاب و مقدار $P_{A,pub} = aP_{pub} = asP$ را محاسبه می‌کند. کلید عمومی متناظر با این کلید خصوصی می‌باشد. حال باب نیز مقدار $b \in Z_r^*$ را انتخاب و مقدار $P_{B,pub} = bP_{pub} = bsP$ را محاسبه می‌کند. بنابراین این مقدار کلید عمومی متناظر با کلید خصوصی دوم باب می‌باشد.

مرحلهٔ توافق کلید چند تایی:

حال آلیس و باب برای ساخت کلیدهای مشترک بدین ترتیب عمل می‌کنند.

۱. تعهد[1]: باب مقدار تصادفی $m \in Z_r^*$ را انتخاب و مقدار $M = mQ_{IDB}$ را محاسبه و سپس مقادیر $\{M, P_{B,pub}\}$ را برای آلیس ارسال می‌کند.

۲. چالش[2]: آلیس مقدار $n \in Z_r^*$ را انتخاب و مقادیر $N = nQ_{IDA}$, $S = e(S_{IDA}, M)^n$ را محاسبه می‌کند. حال آلیس مقادیر $\{P_{A,pub}, N, D = H(S \| IDA \| IDB)\}$ را برای باب می‌فرستد.

۳. واکنش[3]: باب ابتدا مقادیر $Y = (m + fb)S_{IDB}$, $f = H(N \| IDA \| IDB)$ سپس مقدار Y را برای آلیس ارسال می‌کند.

۴. تصدیق[4]: آلیس ابتدا مقدار $f = H(N \| IDA \| IDB)$ را محاسبه و سپس هویت باب را می‌پذیرد اگر و تنها اگر رابطهٔ زیر برقرار شود:

$$e(P, Y) = e(P_{pub}, M)\, e(P_{B,pub}, Q_{IDB})^f \quad (1).$$

۵. توافق کلید: آلیس بعد از تأیید هویت باب کلیدهای مشترک را بدین ترتیب می‌سازد.

$$\begin{aligned} K_1 &= e(M, S_{IDA})^n\, e(P_{A,pub}, P_{B,pub})^a \\ &= e(mQ_{IDB}, sQ_{IDA})^n\, e(asP, bsP)^a \\ &= e(Q_{IDB}, Q_{IDA})^{nms}\, e(P, P)^{ba^2s^2}, \end{aligned}$$

$$\begin{aligned} K_2 &= e(M, S_{IDA})^n\, e(P_{B,pub}, P_{B,pub})^a \\ &= e(mQ_{IDB}, sQ_{IDA})^n\, e(bsP, bsP)^a \\ &= e(Q_{IDB}, Q_{IDA})^{nms}\, e(P, P)^{ab^2s^2}. \end{aligned}$$

برای اینکه بقیهٔ کلیدهای تولیدی توسط آلیس برخی خواص امنیتی مهم را حفظ کنند از این کلیدها (K_i به ازای $i = 1, 2$) استفاده می‌کنیم:

$$\begin{aligned} K_3 &= e(Q_{IDB}, S_{IDA})^n K_i \\ &= e(Q_{IDB}, sQ_{IDA})^n K_i \\ &= e(Q_{IDB}, Q_{IDA})^{ns} K_i, \end{aligned}$$

[1] *Commitment*

[2] *Challenge*

[3] *Response*

[4] *Verification*

$$K_{12} = e(Q_{IDA}, P_{B,pub})^a K_i$$
$$= e(Q_{IDA}, bsP)^a K_i$$
$$= e(Q_{IDA}, P)^{abs} K_i \quad ,$$

$$K_{13} = e(Q_{IDA}, P_{B,pub})^a K_i$$
$$= e(Q_{IDA}, bsP)^a K_i$$
$$= e(Q_{IDA}, P)^{abs} K_i \quad ,$$

باب برای تصدیق آلیس ابتدا رابطه زیر را بررسی می‌کند:

$$D = H(e(N, S_{IDB})^m \,||\, IDA \,||\, IDB) \quad (2).$$

حال باب در صورت تأیید هویت آلیس کلیدهای مشترک را بدین ترتیب به‌دست می‌آورد:

$$K_1 = e(S_{IDB}, N)^m e(P_{A,pub}, P_{A,pub})^b$$
$$= e(sQ_{IDB}, nQ_{IDA})^m e(asP, asP)^b$$
$$= e(Q_{IDB}, Q_{IDA})^{mns} e(P, P)^{ba^2s^2} \quad ,$$

$$K_2 = e(S_{IDB}, N)^m e(P_{A,pub}, P_{B,pub})^b$$
$$= e(sQ_{IDB}, nQ_{IDB})^m e(asP, bsP)^b$$
$$= e(Q_{IDB}, Q_{IDB})^{mns} e(P, P)^{ab^2s^2},$$

$$K_3 = e(S_{IDB}, N)K_i$$
$$= e(sQ_{IDB}, nQ_{IDA})K_i$$
$$= e(Q_{IDB}, Q_{IDA})^{ns} K_i \quad ,$$

$$K_4 = e(S_{IDB}, Q_{IDA})^m K_i$$
$$= e(sQ_{IDB}, Q_{IDA})^m K_i$$
$$= e(Q_{IDB}, Q_{IDA})^{ms} K_i \quad ,$$

$$K_5 = e(S_{IDB}, Q_{IDA})K_i$$
$$= e(sQ_{IDB}, Q_{IDA})K_i$$
$$= e(Q_{IDB}, Q_{IDA})^s K_i \quad ,$$

$$K_6 = e(P, P_{A,pub})^b K_i$$
$$= e(P, asP)^b K_i$$
$$= e(P, P)^{bas} K_i \quad ,$$

$$K_4 = e(M, S_{IDA})K_i$$
$$= e(mQ_{IDB}, Q_{IDA})^{ms} K_i$$
$$= e(Q_{IDB}, Q_{IDA})^{ms} K_i \quad ,$$

$$K_5 = e(Q_{IDB}, S_{IDA})K_i$$
$$= e(Q_{IDB}, sQ_{IDA})K_i$$
$$= e(Q_{IDB}, Q_{IDA})^s K_i \quad ,$$

$$K_6 = e(P, P_{B,pub})^a K_i$$
$$= e(P, bsP)^a K_i$$
$$= e(P, P)^{abs} K_i \quad ,$$

$$K_7 = e(P_{A,pub}, P_{B,pub})^a K_i$$
$$= e(asP, bsP)^a K_i$$
$$= e(P, P)^{a^2s^2b} K_i \quad ,$$

$$K_8 = e(P_{B,pub}, P_{B,pub})^a K_i$$
$$= e(bsP, bsP)^a K_i$$
$$= e(P, P)^{ab^2s^2} K_i \quad ,$$

$$K_9 = e(P_{pub}, P_{B,pub})^a K_i$$
$$= e(sP, bsP)^a K_i$$
$$= e(P, P)^{abs^2} K_i \quad ,$$

$$K_{10} = e(M, P_{B,pub})^a K_i$$
$$= e(mQ_{IDB}, bsP)^a K_i$$
$$= e(Q_{IDB}, P)^{ambs} K_i \quad ,$$

$$K_{11} = e(N, P_{B,pub})^a K_i$$
$$= e(nQ_{IDA}, bsP)^a K_i$$
$$= e(Q_{IDA}, P)^{anbs} K_i \quad ,$$

$$K_7 = e(P_{A,pub}, P_{A,pub})^b K_i$$
$$= e(asP, asP)^b K_i$$
$$= e(P,P)^{a^2 s^2 b} K_i \quad ,$$

$$K_8 = e(P_{A,pub}, P_{b,pub})^b K_i$$
$$= e(asP, bsP)^b K_i$$
$$= e(P,P)^{b^2 s^2 a} K_i \quad ,$$
$$K_9 = e(P_{pub}, P_{A,pub})^b K_i$$
$$= e(sP, asP)^b K_i$$
$$= e(P,P)^{as^2 b} K_i \quad ,$$

$$K_{10} = e(M, P_{A,pub})^b K_i$$
$$= e(mQ_{IDB}, asP)^b K_i$$
$$= e(Q_{IDB}, P)^{bmas} K_i \quad ,$$

$$K_{11} = e(N, P_{A,pub})^b K_i$$
$$= e(nQ_{IDA}, asP)^b K_i$$
$$= e(Q_{IDA}, P)^{bnas} K_i \quad ,$$

$$K_{12} = e(Q_{IDA}, P_{A,pub})^b K_i$$
$$= e(Q_{IDA}, asP)^b K_i$$
$$= e(Q_{IDA}, P)^{bas} K_i \quad ,$$

$$K_{13} = e(Q_{IDB}, P_{A,pub})^b K_i$$
$$= e(Q_{IDB}, asP)^b K_i$$
$$= e(Q_{IDB}, P)^{bas} K_i \quad .$$

۴- پیچیدگی محاسباتی:

اکنون محاسبات لازم برای هریک از مراحل پروتکل فوق را بطور خلاصه در جدول ۲ بیان می‌کنیم.

T_p: محاسبه تابع زوج سازی

T_e: محاسبه توان رسانی در G_2

T_m: محاسبه ضرب در G_2

T_a: محاسبه جمع در G_2

T_M: محاسبه ضرب اسکالر G_1

T_A: محاسبه جمع در G_1

T_H: محاسبه تابع درهم

آماده سازی	T_M					
استخراج کلید	تولید کلید توسط کاربر	تولید کلید توسط KGC		تصدیق کلید		
	T_M	$T_M + T_H$		۲ T_M		
توافق کلید	تعهد	چالش	واکنش	تصدیق توسط آلیس	تصدیق توسط باب	توافق کلید
	T_M	$T_M + T_p + T_e + T_H$	$T_m + T_a + T_M + T_H$	$3T_p + T_m + T_e + 2T_H$	$T_p + T_e + T_H$	$T_{K_1,K_2} = 2(2T_p + 2T_e + T_m)$
						$T_{K_3-K_3} = 2(11T_p + 9T_e + 11T_m)$

نکته۲: اگر در این طرح طرف آلیس را مرکز (سرور[1]) و طرف باب را کاربر در نظر بگیریم در اینصورت طرف آلیس نیازمند ارسال مقدار D در مرحلهٔ چالش نمی‌باشد. در نتیجه طرف باب نیز نیازمند بررسی رابطه تصدیق متناظر نمی‌باشد. در اینصورت پیچیدگی محاسباتی و حجم مقادیر ارسالی کاهش یافته و کارایی طرح نیز افزایش می‌یابد.

۵- بررسی‌های امنیتی:

اکنون در این بخش به بررسی نکات امنیتی طرح فوق می‌پردازیم.

نکته۳: در مرحلهٔ تعهد مقدار m و در مرحله چالش مقدار n بطور تصادفی انتخاب می‌شوند بنابراین مقادیر

[1] *Server*

$$M = mQ_{IDB}$$

$$،S = e\left(S_{IDA}, M\right)^n ،N = nQ_{IDA} ،$$

$$f = H\left(N \| IDA \| IDB\right) \quad و \quad D = H\left(S \| IDA \| IDB\right)$$

که به آنها وابسته هستند نیز تصادفی می‌باشند.

قضیه۴: رابطهٔ تصدیق معرفی شده در مرحلهٔ استخراج کلید طرح فوق که سبب می‌شود کاربر کلید خصوصی خود را که از سوی مرکز تولید کلید صادر شده تأیید کند، کامل می‌باشد.

اثبات: کاربر دارای $\{Q_{ID}, S_{ID}\}$ برای تأیید کلید خصوصی خود از رابطهٔ زیر استفاده می‌کند:

$$\begin{aligned} e\left(P, S_{ID}\right) &= e\left(P, sQ_{ID}\right) \\ &= e\left(sP, Q_{ID}\right) \\ &= e\left(P_{pub}, Q_{ID}\right). \end{aligned}$$

قضیه۵: طرح ارائه شده در این مقاله کامل[1] می‌باشد. بدین معنی که یک تصدیق‌کننده راستگو بعد از اجرای مرحلهٔ تصدیق هویت ثابت کننده حقیقی (کاربر واقعی) را تأیید می‌کند.

اثبات: از آنجا که در این طرح در حالت کلی دو رابطهٔ تصدیق وجود دارد بنابراین ابتدا به اثبات اولین رابطهٔ تصدیق می‌پردازیم. این رابطه در مرحلهٔ ۴ طرح استفاده شده است:

$$\begin{aligned} e\left(P, Y\right) &= e\left(P, \left(m + fb\right) S_{IDB}\right) \\ &= e\left(P, \left(m + fb\right) s\, Q_{IDB}\right) \\ &= e\left(sP, mQ_{IDB} + fbQ_{IDB}\right) \\ &= e\left(P_{pub}, mQ_{IDB}\right) e(P_{pub}, fbQ_{IDB}\left.\right) \\ &= e\left(P_{pub}, M\right) e(bP_{pub}, fQ_{IDB}\left.\right) \\ &= e\left(P_{pub}, M\right) e\left(P_{B,pub}, Q_{IDB}\right)^f. \end{aligned}$$

بنابراین این رابطه تصدیق کامل می‌باشد. حال به بررسی رابطهٔ تصدیق دوم که در مرحلهٔ ۵ توسط طرف باب اجرا می‌شود می‌پردازیم:

$$\begin{aligned} S &= e(S_{IDA}, M)^n \\ &= e(sQ_{IDA}, mQ_{IDB})^n \\ &= e(Q_{IDA}, Q_{IDB})^{mns} \\ &= e(nQ_{IDA}, sQ_{IDB})^m \\ &= e(N, sQ_{IDB})^m = e(N, S_{IDB})^m, \end{aligned}$$

$$\begin{aligned} \Rightarrow D &= H\left(e(S_{IDA}, M)^n \| IDA \| IDB\right) \\ &= H\left(e(N, S_{IDB})^m \| IDA \| IDB\right). \end{aligned}$$

و در نتیجه رابطهٔ تصدیق دوم نیز کامل می‌باشد.

قضیه۶: طراح ارائه شده در این مقاله دارای خاصیت درستی[2] می‌باشد.

اثبات: برای اثبات وجود ویژگی درستی کافی است نشان دهیم که جعل هویت یک شخص معادل با داشتن پارامترهای خصوصی او (و یا توانایی محاسبه آنها) توسط جاعل می‌باشد. حال فرض کنیم شخص جاعل قادر به جعل هویت طرف باب باشد. بنابراین او حداقل دوبار با مقادیر $(Y_1, f_1), (Y_2, f_2)$ موفق به فریب طرف آلیس در رابطهٔ تصدیق شده است. بنابراین داریم:

$$\begin{aligned} Y_1 &= \left(m + f_1 b\right) S_{IDB} \\ Y_2 &= \left(m + f_2 b\right) S_{IDB} \\ \Rightarrow Y_2 - Y_1 &= mS_{IDB} + f_2 bS_{IDB} - mS_{IDB} - f_1 bS_{IDB} \\ \Rightarrow Y_2 - Y_1 &= \left(f_2 - f_1\right) bS_{IDB} \\ \Rightarrow bS_{IDB} &= \left(f_2 - f_1\right)^{-1} \left(Y_2 - Y_1\right). \end{aligned}$$

. با توجه به رابطه زیر

$$\begin{aligned} e\left(P, Y\right) &= e\left(P, \left(m + fb\right) S_{IDB}\right) \\ &= e\left(P, mS_{IDB} + fbS_{IDB}\right) \\ &= e\left(P, msQ_{IDB}\right) e(P, fbS_{IDB}\left.\right) \\ &= e\left(sP, M\right) e(P, bS_{IDB}\left.\right)^f \\ &= e\left(P_{pub}, M\right) e(P, bS_{IDB}\left.\right)^f. \end{aligned}$$

کاملا واضح است که هر شخصی با داشتن مقدار bS_{IDB} می‌تواند هویت کاربر را جعل و موفق به فریب تصدیق کننده در رابطه تصدیق شود. در نتیجه شخصی که قادر به دو بار جعل هویت طرف باب می‌باشد می‌تواند به محاسبه کلید خصوصی او می‌باشد. برای طرف دیگر نیز همین گونه عمل می‌کنیم. عکس مطالب فوق کاملاً بدیهی است بدین معنی است که هر کس با داشتن پارامتر خصوصی طرف آلیس و طرف باب قادر به جعل هویت آنها می‌باشد.

قضیه۷: طرح ارائه شده در این مقاله دارای ویژگی *اثبات با اطلاع صفر*[3] می‌باشد. بدین معنی که شخص اثبات‌کننده موفق به اثبات هویت خود به شخص تصدیق‌کننده می‌شود بدون اینکه هیچ یک از اطلاعات مخفی خود را افشا کند.

[1] Completeness

[2] Soundness

[3] Zero-Knowledge Proof

اثبات: طرف آلیس (طرف باب) دارای اطلاعات $\left(\{Q_{IDA}, N, D, P_{A,pub}\}\right)\{Q_{IDB}, M, Y, P_{B,pub}\}$ از طرف مقابل می‌باشد. بدست آوردن کلید خصوصی طرف باب (طرف آلیس) یعنی $(S_{IDA})S_{IDB}$ از رابطهٔ $Y=(m+fb)S_{IDB}$ به علت $\left(D=H\left(e(S_{IDA},M)^n \| IDA \| IDB\right)\right)$ ندانستن مقادیر m,b (یک طرفه بودن H و سخت بودن مسئله لگاریتم گسته) غیرممکن می‌باشد. از طرفی بدست آوردن مقادیر m,b (n,a) از روابط $P_{B,pub}=bP_{pub}=bsP$ و $M=mQ_{IDB}$ ($N=nQ_{IDA}, P_{A,pub}=aP_{pub}=asP$) مستلزم حل مسئله لگاریتم گسته می‌باشد که این امر نیز غیرممکن است. بنابراین این طرح دارای خاصیت اثبات با اطلاع صفر می‌باشد.

قضیه۸: در طرح ارائه شده در این مقاله باب نباید از مقدار ثابت m استفاده کند، زیرا در غیر این‌صورت مقادیر لازم برای جعل هویت وی در اختیار تصدیق کننده قرار می‌گیرد.

اثبات: اگر باب در مرحله تعهد مقدار ثابت m استفاده کند آنگاه شخص تصدیق کننده با ارسال دو مقدار f_1, f_2 و تفریق مقادیر ارسالی از سوی کاربر مقادیر مخفی او را بیابد:

$$Y_1=(m+f_1b)S_{IDB}$$
$$Y_2=(m+f_2b)S_{IDB}$$
$$\Rightarrow Y_2-Y_1=mS_{IDB}+f_2bS_{IDB}-mS_{IDB}-f_1bS_{IDB}$$
$$\Rightarrow Y_2-Y_1=(f_2-f_1)bS_{IDB}$$
$$\Rightarrow bS_{IDB}=(f_2-f_1)^{-1}(Y_2-Y_1).$$

بنابراین شخص تصدیق کننده مقدار bS_{IDB} را می‌یابد. مطابق آنچه در بالا ذکر شد با داشتن مقدار bS_{IDB} می‌توان هویت کاربر را جعل و موفق به فریب تصدیق کننده در رابطه تصدیق شده و در نتیجه پروتکل خاصیت اثبات با اطلاع صفر بودن خود را از دست می‌دهد.

قضیه۹: طرح ارائه شده در این مقاله دارای ویژگی *امنیت در مقابل جعل هویت طرف آغازگر پروتکل با کلید آشکار شده*[1] می‌باشد. بدین معنی که در صورت آشکار شدن کلید خصوصی طولانی مدت طرف آلیس مهاجمی که این کلید را در اختیار دارد نتواند خود را به جای طرف باب به طرف آلیس معرفی کند.

اثبات: از آنجا که در مقدار ارسالی طرف باب (امضا یا جواب $Y=(m+fb)S_{IDB}$) کلید خصوصی طرف آلیس تأثیر ندارد. بنابراین مهاجم با داشتن کلید خصوصی طرف آلیس نمی‌تواند هویت طرف باب را جعل کند. اما برای طرف مقابل چنین امنیتی وجود ندارد. بدین معنی که در صورت افشای کلید خصوصی طولانی مدت طرف باب شخص جاعل می‌تواند خود را بجای آلیس به باب معرفی نماید. با استفاده از رابطه زیر

$$S=e(S_{IDA},M)^n=e(N,S_{IDB})^m,$$
$$\Rightarrow D=H(e(S_{IDA},M)^n \| IDA \| IDB)$$
$$=H(e(N,S_{IDB})^m \| IDA \| IDB).$$

مشخص است که باب اشتباها هویت جاعل را تصدیق می‌کند. برای مقابله با این مشکل باب می‌تواند از روش چالش- واکنش برای تصدیق آلیس استفاده نماید.

قضیه۱۰: طرح ارائه شده در این مقاله ویژگی *امنیت کلید شناخته شده*[2] را برآورده می‌کند. بدین معنی که در صورت دستیابی مهاجم به کلید یک نشست او توانایی محاسبه کلیدهای نشست بعدی را نداشته باشد.

اثبات: از آنجا که کلیدهای نشست بعدی به کلید خصوصی و مقدار تصادفی تولیدی هر دو طرف پروتکل وابسته می‌باشند بنابراین مهاجم توانایی محاسبه کلیدهای نشست بعدی را ندارد.

قضیه۱۱: طرح ارائه شده در این مقاله دارای ویژگی *امنیت کلید ناشناخته*[3] بوده و نیز در برابر «مردی در میانه[4]» مقاوم می‌باشد.

اثبات: ویژگی امنیت کلید ناشناخته بدین معنی است که فرض کنیم آلیس و باب در حال اجرای پروتکل توافق کلید هستند. یک مهاجم فعال (اسکار) نباید بتواند به نحوی در اجرای پروتکل دخالت کند تا بعد از اتمام پروتکل، طرف آلیس بر این باور باشد که با طرف باب توافق کلید انجام داده اما طرف باب معتقد است با اسکار (مهاجم) کلید محرمانه مشترک ساخته است. حمله «مردی در میانه» بدین ترتیب است که فرض کنیم آلیس و باب در حال اجرای پروتکل توافق کلید هستند. در این حمله مهاجم فعال (اسکار) به نحوی در اجرای پروتکل دخالت می‌کند تا سبب شود طرفین پروتکل روی کلیدهای متفاوتی توافق کنند. حال در طرح ارائه شده در این مقاله قبل از مرحلهٔ توافق کلید طرفین با استفاده از برخی روشهای احراز اصالت از هویت طرف مقابل مطمئن می‌شوند. بنابراین این طرح در برابر حملات فوق امن می‌باشد.

قضیه۱۲: طرح ارائه شده در این مقاله دارای امنیت پیشرو کامل[5] می‌باشد. بدین معنی که در صورت افشای کلیدهای خصوصی هر دو طرف آلیس و باب امنیت کلیدهای مخفی

[1] Key-Compromise Impersonation

[2] Known-Key Security

[3] Unknown Key Security

[4] Man-In-The-Middle Attack

[5] Perfect Forward Secrecy

مشترک قبلی آنها به خطر نمی‌افتد و هیچ مهاجمی قادر به محاسبه کلیدهای نشست‌های قبلی نمی‌باشد.

اثبات: نشان می‌دهیم اگر مهاجمی دارای کلیدهای خصوصی هر دو طرف باب و آلیس باشد او برای محاسبه کلیدهای نشست قبلی نیازمند دانستن حداقل یکی از مقادیر تصادفی تولید شده در آن نشست می‌باشد.

فرض کنیم فرد مهاجم دارای مقادیر

$$\{a,b,S_{IDA},S_{IDB},Q_{IDA},Q_{IDB},M,N,P_{A,pub},P_{B,pub}\}$$

باشد. با توجه به روابط زیر

$$\begin{aligned}K_1 &= e(M,S_{IDA})^n e\left(P_{A,pub},P_{B,pub}\right)^a \\ &= e(S_{IDB},N)^m e(P_{A,pub},P_{A,pub})^b, \\ K_2 &= e(M,S_{IDA})^n e\left(P_{B,pub},P_{B,pub}\right)^a \\ &= e(S_{IDB},N)^m e(P_{A,pub},P_{B,pub})^b.\end{aligned}$$

کاملاً واضح است که شخص مهاجم برای محاسبه K_i به ازای $(i=1,2)$ نیازمند داشتن یکی از مقادیر تصادفی m یا n می‌باشد. بنابراین عدم توانایی او در محاسبه مقدار K_i سبب عدم بدست آوردن کلیدهای نشست قبل توسط مهاجم می‌شود. بنابراین این طرح دارای امنیت پیشرو کامل می‌باشد.

قضیه۱۳: طرح ارائه شده در این مقاله دارای ویژگی *امنیت قوی*[1] می‌باشد. بدین معنی که در صورت افشا هر یک از جفت‌های (کلید خصوصی طرف آلیس، مقدار تصادفی تولیدی طرف باب) یا (مقدار تصادفی تولیدی طرف آلیس، کلید خصوصی طرف باب) یا (مقدار تصادفی تولیدی طرف آلیس، مقدار تصادفی طرف باب) امنیت پروتکل به خطر نمی‌افتد.

اثبات: این طرح به گونه‌ای طراحی شده است که در صورت افشای هر یک از جفت‌های $((b,S_{IDB}),(a,S_{IDA}))$ یا $(n,(b,S_{IDB}))$ یا $(m,(a,S_{IDA}))$ یا (m,n) نمی‌توان مقادیر K_i را به ازای $(i=1,2)$ محاسبه کرد. همان‌طور که قبلاً اشاره شد با توجه به روابط

$$\begin{aligned}K_1 &= e(M,S_{IDA})^n e\left(P_{A,pub},P_{B,pub}\right)^a \\ &= e(S_{IDB},N)^m e(P_{A,pub},P_{A,pub})^b, \\ K_2 &= e(M,S_{IDA})^n e\left(P_{B,pub},P_{B,pub}\right)^a \\ &= e(S_{IDB},N)^m e(P_{A,pub},P_{\mathbf{B},pub})^b.\end{aligned}$$

تنها زمانی می‌توانیم K_i را به ازای $(i=1,2)$ محاسبه کنیم که فقط یکی از جفت‌های $(n,(a,S_{IDA}))$ یا $((m,(b,S_{IDB}))$ را در اختیار داشته باشیم. بنابراین کلیدهای K_i به ازای $(i=1,2)$ دارای ویژگی امنیت قوی می‌باشد و بنابراین بقیه کلیدها که با استفاده از آنها حاصل می‌شوند نیز دارای این ویژگی می‌باشند.

قضیه۱۴: طرحی که در این مقاله ارائه شده است در برابر بازیابی قانونی کلید و جعل هویت توسط مرکز تولید کلید مقاوم می‌باشد.

اثبات: نشان می‌دهیم مرکز تولید کلید با در اختیار داشتن همه مقادیر

$$\{s,S_{IDA},S_{IDB},Q_{IDA},Q_{IDB},M,N,P_{A,pub},P_{B,pub}\}$$

نمی‌تواند کلیدهای یک نشست را محاسبه کند. با توجه به روابط زیر

$$\begin{aligned}K_1 &= e(S_{IDB},N)^m e(P_{A,pub},P_{A,pub})^b \\ &= e(sQ_{IDB},N)^m e(P_{A,pub},aP_{pub})^b \\ &= e(mQ_{IDB},N)^s e(P_{A,pub},bP_{pub})^a \\ &= e(M,N)^s e(P_{A,pub},P_{B,pub})^a \ ,\end{aligned}$$

$$\begin{aligned}K_2 &= e(S_{IDB},N)^m e(P_{A,pub},P_{B,pub})^b \\ &= e(sQ_{IDB},N)^m e(aP_{pub},P_{B,pub})^b \\ &= e(mQ_{IDB},N)^s e(bP_{pub},P_{B,pub})^a \\ &= e(M,N)^s e(P_{B,pub},P_{B,pub})^a,\end{aligned}$$

تنها زمانی مرکز تولید کلید می‌تواند K_i به ازای $(i=1,2)$ را محاسبه کند که حداقل یکی از a یا b را در اختیار داشته باشد. بنابراین طرحی که در این مقاله ارائه شده در برابر بازیابی قانونی کلید مقاوم می‌باشد.

۶- مقایسه:

طرحی که در این مقاله ارائه شده است یک طرح توافق کلید چندتایی از نوع کلید عمومی بدون گواهی می‌باشد. این طرح از روش تعیین هویت مبتنی بر چالش واکنش استفاده می‌کند بنابراین می‌توان آن‌را با برخی طرح‌های تعیین هویت مقایسه کرد. از طرفی این طرح نقطه ضعف اساسی سیستم‌های رمز-نگاری مبتنی بر شناسه یعنی بازیابی قانونی کلید برطرف می-کند. بدین معنی که در این طرح کاربر با تولید یک کلید خصوصی موقت می‌تواند در برابر بازیابی قانونی کلید و جعل هویت توسط مرکز تولید کلید مقاومت کند. بنابراین در مقایسه با بسیاری از طرح‌های مبتنی بر شناسه دارای برتری می‌باشد. در پروتکل ارائه شده در این مقاله هر یک از طرفین تنها یک عدد تصادفی تولید و یک مضرب اسکالر محاسبه و در کل طرح

[1] *Strong Security*

دو عدد تصادفی و مضارب اسکالر متناظر با آن‌ها تولید می‌شود. کلیدهای مشترک تولید شده به ازای تولید این ۲ عدد تصادفی در مقایسه با بسیاری از طرح‌های توافق کلید بیشتر می‌باشد که این مورد نیز برای کارایی این طرح می‌افزاید. ضمناً همان‌گونه که در بالا اثبات شد این طرح موارد امنیتی مهم مانند اثبات اطلاع صفر، امنیت پیشرو کامل و ویژگی امنیت قوی را برآورده می‌کند. حال در ادامه برخی از مقایسات انجام شده را بیشتر توضیح می‌دهیم و در نهایت خلاصه این بررسی‌ها را در جدول ۳ نمایش می‌دهیم. پروتکل‌های تعیین هویت چالش – واکنش مبتنی بر کلید عمومی مانند [22-14-10-9-7-6] دارای سه مرحله کلی (تعهد، چالش، واکنش) همانند طرح ارائه شده در این مقاله می‌باشد و به ازای اندکی عملیات اضافه شده در این مراحل از طرح ارائه شده در این مقاله توانایی توافق کلید چندتایی اضافه شده به این طرح برتری محسوسی نسبت به طرح‌های مفروض می‌بخشد. اولین طرح توافق کلید بوسیله [8] Diffie – Hellman در سال ۱۹۷۶ ارائه شد که امنیت آن بر مبنای سختی محاسبه مسئله لگاریتم گسسته بوده در این طرح دو طرف پروتکل موفق به ساخت یک کلید مخفی مشترک می‌شوند. متأسفانه طرح دیفی – هلمن به علت عدم بررسی هویت طرف مقابل در برابر *حمله «مردی در میانه»* ناامن بوده و یک مهاجم قادر به فریب هر کاربری می‌باشد. طرح ارائه شده در این مقاله برای تصدیق هویت کاربران از روش تعیین هویت چالش – واکنش استفاده می‌کند. در سال ۲۰۰۲، [29] Smart با ترکیب ایده Boneh – Franklin و پروتکل سه قسمتی [12]Joux اولین پروتکل توافق کلید مبتنی بر شناسه ارائه نمود. [27-23] Shim نشان داد که طرح Smart دارای امنیت پیشرو نمی‌باشد و برای اصلاح آن یک پروتکل توافق کلید مبتنی بر شناسه ارائه داد. بعد از آن [30] Sun-Hiseh نشان دادند که طرح Shim در برابر حملهٔ مردی در میانه ناامن می‌باشد. طرح‌های توافق کلید مبتنی بر شناسه دیگر مانند [4-5-13-16-21-23-31-32-35-36] نیز قادر به ساخت یک کلید می‌باشند. در سال ۱۹۹۸ اولین بار [11] Haran - Lin پروتکل‌های توافق کلید چندتایی را ارائه نمودند. این نوع پروتکل‌ها نسبت به سایر پروتکل‌های توافق کلید تک کلیدی بسیار کاراتر می‌باشند. [20] Oh et.al یک طرح توافق کلید مبتنی بر شناسه ارائه نمودند که موفق به تولید ۲ کلید نشست در پایان اجرای پروتکل می‌شد ولی در [18] نشان داده شد که این طرح نیز نا امن می‌باشد. پروتکل مبتنی بر شناسه ارائه شده توسط [15] Kim et.al قادر ساخت ۴ کلید مشترک بود ولی [28]Shim نشان داد که این طرح نیز ناامن می‌باشد. همانگونه که گفته شد [1]Al-Riyami-Paterson یک پروتکل توافق کلید با استفاده از رمزنگاری کلید عمومی بدون گواهی ارائه دادند که کلید عمومی تولیدی هر یک از طرفین پروتکل شامل دو مضرب اسکالر می‌باشد. این طرح شامل ۲ مرحله ارسالی اطلاعات می‌باشد و در پایان پروتکل طرفین موفق به تولید یک کلید مشترک می‌شوند. [19] Mandt و همکارانش با استفاده از ایده Al-Riyami-Paterson موفق به ارائه پروتکلی شدند که در آن محاسبات طرح [1] کاهش داده شده و در نتیجه کارایی بیشتری حاصل می‌کرد. این طرح شامل ۳ مرحله ارسال اطلاعات بوده و کلید عمومی تولیدی هریک از طرفین شامل یک مضرب اسکالر می‌باشد. این طرح نیز از نوع تک کلیدی می‌باشد. [33] Wang و همکارانش موفق به ارائه طرحی شدند که شامل ۲ مرحله ارسال اطلاعات بوده و کلید عمومی تولید طرفین پروتکل شامل یک مضرب اسکالر می‌باشد. این طرح تک کلیدی در برابر حمله جعل هویت با کلید آشکار شده نا امن بودن و دارای امنیت پیشرو جزئی می‌باشد. [34] Wang-Zhang پروتکل توافق کلیدی ارائه دادند که دارای ۲ مرحله ارسال اطلاعات بوده و کلید عمومی تولیدی هر یک از طرفین پروتکل نیز شامل ۲ ضرب اسکالر می‌باشد. این پروتکل نیز از نوع تک کلیدی بوده و در برابر حمله مردی در میانه ناامن می‌باشد. طرح‌های توافق کلید مبتنی بر شناسه مانند [4-5-21-23-31-32-35-36] به ازای ۲ مقدار تصادفی انتخاب شده در پروتکل قادر به ساخت یک کلید می‌باشند. طرحهای [13-16] به ازای ۴ مقدار تصادفی تولید شده تنها یک کلید مشترک می‌سازند و طرح [20] Oh et.al به ازای ۲ نقطه تصادفی قادر به ساخت ۲ کلید مشترک می‌باشد. ضمنا باید بگوییم که هر یک از طرح‌های توافق کلید چندتایی موجود مانند [11-15-20] برخی از موارد امنیتی مطرح شده در بالا را برآورده نمی‌کنند. تعداد کلیدهای مشترک تولید شده در پروتکل‌های [11-15] حداکثر ۴ کلید مشترک به ازای تولید ۴ عدد تصادفی در این پروتکل‌ها می‌باشد. همچنین در بسیاری از طرح‌های توافق کلید چندتایی مانند[10-14] تعداد مقادیر تصادفی تولید شده توسط هر یک از طرفین برابر ۲ می‌باشد یعنی در مجموع پروتکل ۴ عدد تصادفی تولید می‌شود و برای هر یک از این مقادیر تصادفی یک مضرب اسکالر محاسبه می‌شود.

شماره طرح	نوع طرح	مبتنی بر شناسه	مقاوم در برابر بازیابی قانونی کلید	تعداد نقاط تصادفی	تعداد کلید مشترک
6-7-9-10-22	تعیین هویت	×	×	2	_
14	تعیین هویت	✓	×	2	_
2	تعیین هویت -توافق کلید	×	×	1	1
4-5-21-23-31-32-35-36	توافق کلید	✓	×	2	1
19	توافق کلید	✓	×	2	2
13-16	توافق کلید	✓	×	4	1
11-15	توافق کلید	✓	×	4	4
1-19-33-34	توافق کلید	✓	✓	2	1
طرح ارائه شده	تعیین هویت -توافق کلید	✓	✓	2	24

جدول ۳

۷- نتیجه گیری:

طرح ارائه شده در این مقاله یک طرح توافق کلید چندتایی از نوع بدون گواهی می‌باشد. این طرح در مقایسه با بسیاری از طرح‌های موجود تعداد کلید بیشتری تولید کرده و نسبت به این طرح‌ها بسیار کاراتر می‌باشد. علاوه بر این طرح دارای ویژگی‌های امنیتی مهم مانند اثبات اطلاع صفر، امنیت پیشرو کامل و امنیت قوی را دارا می‌باشد.

مراجع

[1] S.-S. Al-Riyami, K. Paterson, *Certificateless Public Key Cryptography*. In: ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003). full version in Cryptology ePrint Archive, Report 2003/126, 2003. http://eprint.iacr.org/.

[2] A. M Allam, I. I. Ibrahim, I. A. Ali, A.H. Elsawy, Efficient Zero-Knowledge Identification Scheme with Secret Key Exchange, 2004 IEEE.

[3] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing. In Advances in Cryptology - CRYPTO '01, LNCS 2139, pages 213-229, Springer-Verlag, 2001.

[4] Y.-J. Choie, E. Jeong and E. Lee, Efficient identity based authenticated key agreement protocol from pairings. Journal of Applied Mathematics and Computation,162(1), pp. 179-188, 2005.

[5] S.S.M. Chow and K.-K.R. Choo, Strongly-Secure Identity-Based Key Agreement and Anonymous Extension, In ISC 2007, LNCS 4779, pp. 203–220, Springer, 2007

[6] M. H. Dehkordi, , R. Alimoradi, Zero-Knowledge Identification Scheme Based on Weil Pairing, Lobachevskii Journal of Mathematics, Vol. 30, No. 3, 203–207. 2009.

[7] M. H. Dehkordi, , R. Alimoradi, A NEW BATCH IDENTIFICATION SCHEME, Discrete Mathematics, Algorithms and Applications, Vol. 1, No. 3, 369–376, 2009.

[8] W. Diffiee, M. Hellman. New Directions in Cryptography. In IEEE Transaction on Information Theory, IT-22 (6), pp. 644-654, 1976.

[9] U.Feige, A. Fiat,A. Shamir, Zero- Knowledge Proofs of Identity,Journal of Cryptology, vol.1, 1988, 77-94.

[10] A. Fiat, A. Shamir. How To Prove Yourself: practical solutions of identification and signature problems. In Odlyzko A.M, editor, Advances in Cryptology - Proceedings of CRYPTO' 86, volume 263 of Lecture Notes in Computer Science, 186-194, Santa- Barbara, California, 1987, Springer- verlag.

[11] L. Harn, H.-Y. Lin, An authenticated key agreement protocol without using one-way function. In: Proceedings of eighth information security conference, Taiwan, May 1998; 155–60.

[12] A. Joux,A One Round Protocol for Tripartite Diffie-Hellman, in:Proceedings of Algorithmic Number Theory Symposium, LNCS 1838, Springer-Verlag, (2000), 385-394.

[13] S. Kim, H. Lee, H. Oh, Enhanced ID-Based Authenticated Key Agreement Protocols for a Multiple Independent PKG Environment, ICICS 2005, LNCS 3783, pp. 323–335, Springer, 2005.

[14] M. Kim and K. Kim. A New Identification Scheme Based on the Bilinear Diffie- Hellman Problem. In The 7th Australian Conference on Information Security and Privacy, ACISP 02, 362-378. Springer-Verlag, 2002.

[15] K. Kim, E. Ryu and K. Yoo, ID-based authenticated multiple-key agreement protocol from pairing, International Conference on Computational Science and Its Applications, ICCSA'04, LNCS 3046, Springer-Verlag, pp. 672-680, 2004.

[16] H. Lee, D. Kim, S. Kim, H. Oh, Identity-based Key Agreement Protocols in a Multiple PKG Environment. Proc. of the Int. Conf. on Computational Science and Its

Applications, ICCSA 2005. Lecture Notes in Computer Science, Vol. 3483. Springer (2005) 877–886.
[18] N.-Y. Lee, C.-N. Wu, C.-C. Wang, Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings, In: Computers and Electrical Engineering 34 (2008), 12–20.
[19] M.-H. Lim, S. Lee and H. Lee, Cryptanalytic Flaws in Oh et al.'s ID-Based Authenticated Key Agreement Protocol, Cryptology ePrint Archive: Report,(2007).
[20] T.-K. Mandt and C.-H. Tan, *Certificateless Authenticated Two-Party Key Agreement Protocols*, In: ASIAN 2006, LNCS, vol. 4435, pp. 37–44. Springer, Heidelberg (2007).
[21] J.-B. Oh, E.-J. Yoon and K.-Y. Yoo, An Efficient ID Based Authenticated Key Agreement Protocol with Pairings, Parallel and Distributed Processing and Applications, In Proceeding of 5th International Symposium, ISPA 2007, LNCS, vol. 4742, 2007, pp. 446-456.
[22] E.-K. Ryu, E.-J. Yoon, and K.-Y. Yoo. An Efficient ID-Based Authenticated Key Agreement Protocol from Pairings. In 3rd International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols – NETWORKING 2004, pages 1464–1469. Springer-Verlag, 2004. Vol. 3042/2004 of LNCS.
[23] C. P. Schnorr ,Efficient signature generation by smart cards. Journal of Cryptology, 4(1991), 161-174.
[24] M. Scott, Authenticated ID-based key exchange and remote log-in with insecure token and PIN number. Cryptology ePrint Archive, Report 2002/164, http://eprint.iacr.org/2002/164/.
[25] A. Shamir, *Identity-based cryptosystems and signature schemes*. In Advances in Cryptology - CRYPTO '84, LNCS 196, pages 47-53, Springer-Verlag, 1984.
[26] J. Shao, R. Lu, and Z. Cao. A New Efficient Identification Scheme Based on the Strong Diffie-Hellman Assumption. In International Symposium on Future Software Technology, 2004.
[27] K. Shim and S. Woo, "Weakness in ID-based one round authenticated tripartite multiple-key agreement protocol with pairings", Applied Mathematics and Computation, Volume: 166, Issue: 3, July 26, 2005, pp. 523-530.
[28] K. Shim, Efficient ID-based authenticated key agreement protocol based on the Weil pairing. In Electron Lett 39, 653–654, 2003.
[29] K-A. Shim and S-H. Seo, Cryptanalysis of ID-Based Authenticated Key Agreement Protocols from Bilinear Pairings. In ICICS 2006, LNCS 4307, pp. 410–419, 2006. Springer-Verlag (2006).
[30] N. Smart, An identity based authenticated key agreement protocol based on the Weil pairing. In Electronics Letters, 38:630-632, 2002.
[31] H. Sun, B. Hsieh, Security analysis of Shim's authenticated key agreement protocols from pairings. Cryptology ePrint Archive, Report 2003/113.
[32] Y. Wang. Efficient Identity-Based and Authenticated Key Agreement Protocol. Cryptology ePrint Archive, Report 2005/108, 2005. http://eprint.iacr.org/2005/108/.
[33] S. Wang, Z. Cao, Z. Cheng, K.-K. R. Choo, Perfect Forward Secure Identity-Based Authenticated Key Agreement Protocol in the Escrow Mode, ePrint Archive, Report 2007.
[34] S. Wang, Z. Cao, L. Wang. *Efficient Certificateless Authenticated Key Agreement Protocol from Pairings*. In:
Wuhan University Journal of Natural Sciences (WUJNS) Vol. 11, No. 5, 2006, pp. 1278-1282.
[35] F. Wang, Y. Zhang, *A New Provably Secure Authentication and Key greement Mechanism for SIP Using Certificateless Public-key Cryptography*, In: International Conference on Computational Intelligence and Security (CIS.2007.113), IEEE Computer Society, pp. 809-814, 2007.
[36] Y. Xun, Efficient ID-based key agreement from Weil pairing. In Electronics Letters 23th, 206-208, 2003.
[37] Q. Yuan and S.-P. Li, A New Efficient ID-Based Authenticated Key Agreement Protocol, Cryptology ePrint Archive: Report, (309)(2005).