رمزنگاری مبتنی بر شناسه در شبکه‌های حس‌گر بی‌سیم

رضا علیمرادی[1]

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

چکیده

در سال‌های اخیر برای حل مشکل توزیع کلید و تعداد زیاد کلیدهای ذخیره‌شده در شبکه‌های حس‌گر بی‌سیم از رمزنگاری کلید عمومی استفاده و در این شبکه‌ها از این نوع رمزنگاری برای انجام احراز اصالت و توافق کلید بهره گرفته شده است. پر کاربردترین رمزنگاری کلید عمومی که مبتنی بر گواهی است، از زیرساخت کلید عمومی (PKI) استفاده می‌کند. همان‌طورکه می‌دانیم برای پیاده‌سازی PKI نیازمند میزان قابل توجهی حافظه، حجم محاسبات و ارتباطات می‌باشیم که برای پیاده‌سازی بر روی شبکه‌های حس‌گر غیرعملی است. برای حل این مشکل می‌توانیم از رمزنگاری مبتنی بر شناسه (IBC) استفاده کنیم. در این نوع رمزنگاری، شناسه‌های عمومی کاربران مانند نشانی رایانامه و یا IP به‌عنوان کلید عمومی افراد استفاده می‌شود و بنابراین دیگر نیازی به PKI نیست. این نوع رمزنگاری بعد از پیدایش رمزنگاری مبتنی بر توابع زوج‌سازی، به‌صورت عملی مورد استفاده قرار گرفت. در این مقاله به بررسی نحوه استفاده از توابع زوج‌سازی در شبکه‌های حس‌گر بی‌سیم می‌پردازیم.

واژگان کلیدی: رمزنگاری، رمزنگاری مبتنی بر شناسه، منحنی‌های بیضوی، ضرب اسکالر، توابع زوج‌سازی.

۱- مقدمه

شبکه‌های حس‌گر بی‌سیم[1] (WSN) شبکه‌های موردی[2] هستند که شامل تعداد زیادی حس‌گر کوچک و یک یا چند ایستگاه اصلی[3] است. این حس‌گرها به‌علت وجود محدودیت در اندازه و هزینه محدودیت‌هایی در میزان انرژی مصرفی، حافظه، سرعت محاسبات و پهنای باند دارند. این شبکه‌ها به‌منظور جمع‌آوری اطلاعات و کنترل محیط به کار می‌روند. شبکه‌های حس‌گر بی‌سیم کاربردهای فراوانی در ساختارهای نظامی و غیرنظامی دارند. نظارت میدان جنگ، مراقبت از طبیعت، کنترل ترافیک و کنترل وضعیت سلامتی از جملهٔ این کاربردها هستند. این حس‌گرها شامل باتری شارژشده، ریزپردازنده و مدار فرکانس رادیویی هستند. در سال‌های اخیر برای حفظ امنیت در WSN از سامانه‌های رمزنگاری متقارن مانند Skipjack و RC5 به‌منظور انجام احراز اصالت و تأمین محرمانگی استفاده می‌شد. سامانه‌های رمزنگاری متقارن به‌دلیل اینکه در میزان انرژی مصرفی و حافظه مورد نیاز نسبت به سامانه‌های رمزنگاری کلید عمومی کاراتر هستند، برای استفاده در WSN مناسب‌ترند. با این حال توزیع کلید و تعداد کلیدهای ذخیره‌شده دو مشکل اساسی استفاده از سامانه‌های رمزنگاری متقارند. زمانی‌که کلیدهای منحصر به‌فرد در WSN با n گره به‌کار می‌روند آن‌گاه هر گره باید (n-1) کلید را ذخیره کند. به‌طورکامل واضح است که این امر برای شبکه‌های بزرگ مناسب نیست. به‌هرحال امنیت پیشرو کامل بعد از افشای کلید یک گره وجود نخواهد داشت. درصورتی‌که از یک کلید متقارن استفاده کنیم، آن‌گاه میزان حافظه مورد نیاز به‌شدت کاهش می‌یابد؛ ولی درصورت افشای کلید در یک

[1] Wireless Sensor Networks
[2] Ad hoc
[3] Base station (BS)

گره امنیت کل شبکه به خطر می‌افتد. برای غلبه بر این مشکل طرح‌های توزیع کلید احتمالی زیادی برای الگوریتم متقارن ارائه شده است. در حالت کلی همهٔ این طرح‌ها نیازمند کلیدهای از پیش توزیع‌شده‌اند که این امر سبب افزایش فعالیت‌ها قبل از توسعه شبکه می‌شود. بنابراین الگوریتم‌های نامتقارن (کلید عمومی) برای انجام توافق کلید و احراز اصالت در WSN بسیار ارزشمند هستند. در ادامه سه نوع از طرح‌های توافق کلید را که به‌طورمعمول برای شبکه‌های عمومی مورد استفاده قرار می‌گیرند، بیان می‌کنیم. یکی طرح‌های مبتنی بر سرور امن[1] است که در آن ها نیازمند وجود یک مرکز اصلی امین برای توافق کلید بین گره‌ها هستیم. این نوع از طرح‌ها برای WSN که دارای محدودیت انرژی و توان محاسباتی می‌باشد، مناسب نیست. دیگری طرح‌های مبتنی بر پیش توزیع کلید می‌باشند که در آن‌ها اطلاعات کلیدی قبل از توسعه و ایجاد شبکه در همهٔ گره‌ها توزیع می‌شود و در آخر طرح‌های مبتنی بر کلید عمومی که از رمزنگاری مبتنی بر کلید عمومی در آن‌ها استفاده می‌شود. در گذشته رمزنگاری کلید عمومی برای پیاده‌سازی بر روی سامانه‌های کم‌توان مانند شبکه‌های حس‌گر که از ریزپردازنده‌ها استفاده می‌کنند و دارای محدودیت‌های عملیاتی زیادی هستند، بسیار بعید به نظر می‌رسید. امروزه با کاراترکردن الگوریتم‌های کلید عمومی و نیز افزایش توان محاسباتی ریزپردازنده‌ها امکان استفادهٔ رمزنگاری کلید عمومی فراهم شده است. در سال‌های اخیر پژوهش‌های زیادی برای عملی‌کردن رمزنگاری کلید عمومی بر روی WSN انجام شده است[۱۳]. به‌عنوان مثال نتایج ارائه‌شده در [۲۸،۲۷،۲۵،۱۹،۱۳،۱۲،۸] نشان می‌دهد که رمزنگاری مبتنی بر منحنی‌های بیضوی (ECC) بر روی WSN قابل پیاده‌سازی است. هم‌اکنون منحنی‌های بیضوی در بسیاری از سامانه‌های قابل حمل مانند PDAها، کارت‌های هوشمند، موبایل‌ها و خبردهنده‌ها[2] مورد استفاده قرار می‌گیرند. حس‌گرهای خانواده TELOSB [۵]،[۴] MICAz، MICA2 و[۳] Imot2 برای پیاده‌سازی رمزنگاری کلید عمومی مناسب هستند. به‌منظور استفاده از ECC بر روی WSN باید از انجام حملات مردی در میانه به‌وسیلهٔ انجام احراز اصالت مبتنی بر کلید عمومی جلوگیری کرد. رمزنگاری کلید عمومی برای دستیابی به این منظور از زیرساخت کلید عمومی (PKI) استفاده می‌کنند. همان طور که می‌دانیم برای پیاده‌سازی PKI نیازمند میزان قابل توجهی حافظه، حجم محاسبات و ارتباطات هستیم که برای پیاده‌سازی برروی WSN غیرعملی است. برای حل این مشکل می‌توانیم از رمزنگاری مبتنی بر شناسه (IBE) استفاده کنیم. در این نوع رمزنگاری شناسه‌های عمومی کاربران مانند نشانی رایانامه و یا IP به‌عنوان کلید عمومی افراد استفاده می‌شود و بنابراین دیگری نیازی به PKI نیست. این نوع رمزنگاری بعد از پیدایش رمزنگاری مبتنی بر توابع زوج‌سازی به‌صورت عملی مورد استفاده قرار گرفت. درحقیقت به‌نظر می‌رسد IBE تنها راه حل عملی برای به‌کاربردن رمزنگاری کلید عمومی برروی WSN است. نمونه‌هایی از رمزنگاری مبتنی بر شناسه (IBC) ارائه‌شده برای MANET[3] در[۳۱،۳۰،۱۷،۹،۶] آورده شده است. نمونه‌هایی از رمزنگاری مبتنی بر توابع زوج‌سازی به‌کاررفته در سامانه‌های دارای محدودیت، مانند WSN در [۲۹،۲۲،۲۰،۱۵،۱۴] آورده شده است. در سامانه IBE شناسهٔ عمومی هر گره (حس‌گر) عضو WSN یعنی ID هر گره برابر کلید عمومی آن گره محسوب می‌شود.همان‌طورکه می‌دانیم در سامانه IBE نیازمند وجود مرکزی مطمئن برای تولید کید خصوصی برای کاربران هستیم که از طریق کانال امن و محرمانه کلید را برای کاربران ارسال کند. در WSN ایستگاه اصلی (BS) وظیفه تولید کلید را می‌تواند برعهده داشته باشد. درضمن کلید خصوصی هر گره می‌تواند قبل از ایجاد توسعه شبکه در درون هر حس‌گر بارگذاری شود. از آنجا که IBE پیچیده‌تر از سامانه‌های رمزنگاری متقارن است، بنابراین از IBE فقط برای تولید کلید مشترک بین دو گره (و یا گره‌ها) استفاده می‌شود. در[۲۶] پروتکل‌های مبتنی بر کلید عمومی برای WSN ارائه شده است. این پروتکل‌ها شامل طرح‌های توافق کلید و احراز اصالت مبتنی بر RSA می‌باشند که با Tiny PK نام‌گذاری شده‌اند. Tiny PK تحت NesC بر روی ریزپردازنده‌های ۸ بیتی MICAz پیاده‌سازی شده است. از آنجا که یک توان‌رسانی RSA با طول کلید ۱۰۲۴ بیتی در ۱۴،۵ ثانیه قابل انجام است، بنابراین ساختارهای مبتنی بر RSA به‌طورتقریبی برای بسیاری از کاربردها غیرقابل قبول هستند. رمزنگاری مبتنی بر منحنی‌های بیضوی (ECC) در مقایسه با RSA دارای طول کلید کمتری هستند (۱۶۰بیت در برابر ۱۰۲۴ بیت) بنابراین با توجه به محدودیت‌های ذکرشده برای حس‌گرهای مبتنی بر ریزپردازنده‌های ۸ بیتی، به‌نظر می‌رسد استفاده از

[1] Trusted Server
[2] Pager
[3] Mobile Ad Hoc Network

EEC به جای RSA بسیار کاراتر باشد[۸]. اصلی‌ترین عمل در ECC عمل ضرب اسکالر است. در[۱۲] کتابخانه نرم‌افزاری رایگانی تحت نام Tiny ECC ارائه شده که یکی از سریع‌ترین کتابخانه‌های نرم‌افزاری برای اجرای ECC بر روی WSN است و همه منحنی‌های ۱۲۸، ۱۶۰، ۱۹۲ بیتی استاندارد SECG [۱۸] را پشتیبانی می‌کند. البته بسته نرم‌افزاری ارائه‌شده توسط شرکت SUN Microsystem که تهیه آن مستلزم پرداخت هزینه می‌باشد، برای این منظور سریع‌ترین است.

۲- بررسی کارایی کتابخانهٔ نرم‌افزاری Tiny Pairing بر روی حس‌گر MICAz

همان‌طورکه درقبل گفته شده بسته نرم‌افزاری موسوم به Tiny ECC یکی از سریع‌ترین کتابخانه‌های نرم‌افزاری موجود است. بنابراین بسیاری از پژوهش‌گران نتایج حاصل پیاده‌سازی‌های نرم‌افزاری خود را با آن مقایسه می‌کنند. به‌عنوان مثال کتابخانهٔ نرم‌افزاری موسوم به Tiny Pairing [۲۹] که توابع زوج‌سازی را پشتیبانی کرده و بنابراین برای رمزنگاری مبتنی بر توابع زوج‌سازی (PBC) مناسب است. در جدول زیر کارایی کتابخانهٔ Tiny Pairing [۲۴] بر روی حس‌گر MICAz بیان شده است. بدین ترتیب که به‌ازای هر عمل ده ورودی تصادفی انتخاب سپس میانگین زمان اجرا محاسبه شده است.

(جدول۱): زمان اجرای محاسبات در PBC برروی حسگر MICAz با استفاده از Tiny Pairing [۲۲]

زمان(sec)	
0.89	تبدیل یک رشته بیت به یک نقطه بر روی منحنی به کمک تابع درهم
0.38	فشرده کردن نقطه
0.38	تبدیل نمایش فشرده نقطه به نمایش معمولی
7.75	ضرب اسکالر
2.50	ضرب اسکالر
2.45	ضرب اسکالر
5.32	محاسبه تابع زوج سازی n_T

حال با استفاده از نتایج بالا به مقایسهٔ نتایج حاصل از پیاده‌سازی برخی از طرح‌های مبتنی بر توابع زوج‌سازی توسط Tiny Pairing با برخی از طرح‌های مبتنی بر منحنی‌های بیضوی توسط Tiny ECC بر روی حس‌گر MICAz می‌پردازیم.

(جدول۲): پیاده‌سازی برخی از طرح‌های رمزنگاری بر روی MICAz [۲۹]

کتابخانه	Tiny ECC	Tiny Pairing
طرح	ECIES	BF IBE
آغازین(sec)	0	-
راه اندازی	-	3.22
بدست آوردن کلید(sec)	-	2.83
رمزکردن(sec)	61.40	10.61
رمزگشایی(sec)	31.87	5.35
RAM(bytes)	150	392
ROM(bytes)	12,442	22,598
اندازه کلید عمومی/ID	بیت بعد از فشرده سازی160	هر رشته بیت دلخواه

(جدول۳): پیاده‌سازی برخی از طرح‌های رمزنگاری بر روی MICAz [۲۹]

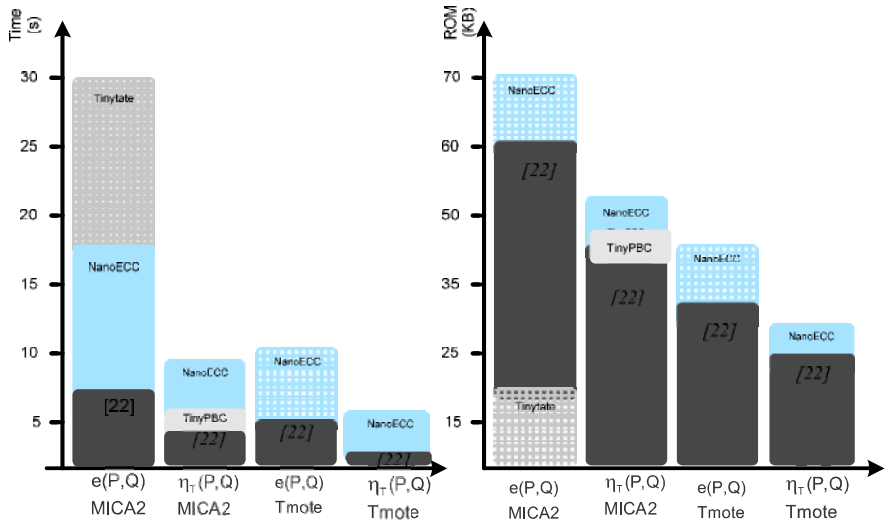
کتابخانه	Tiny ECC	Tiny Pairing	
طرح	ECDSA	BLS SS[1]	BBSS[2]
آغازین(sec)	0	-	-
تولید کلید(sec)	-	3.18	12.33
امضا(sec)	30.72	4.08	3.0
تصدیق(sec)	61.80	12. 62	11.03
RAM(bytes)	152	382	392
ROM(bytes)	10,180	22,632	19,742
اندازه امضا(بیت)	320	160	312

۳- مقایسه‌ای بین انواع مختلفی از حس‌گرها و بسته‌های نرم‌افزاری

اکنون مقایسه‌ای بین انواع مختلفی از حس‌گرها از قبیل MICA2 که از نوع MICAz است و Imote2 و Tmote SKY ارائه می‌شود. در این مقایسه دو نوع تابع زوج‌سازی $e(P,Q)$ و $n_T(P,Q)$ توسط بسته‌های نرم‌افزاری NanoECC [۲۱]، Tinytate [۱۴]، Tiny PBC [۱۵] و بسته ارائه شده در [۲۲] پیاده‌سازی شده‌اند.

(جدول۴): پیاده‌سازی توابع زوج‌سازی تعریف‌شده روی به‌ازای حس‌گرهای Imote2[۲۲]

	Imote2(13MHz)		Imote2(104MHz)	
	$n_T(P,Q)$	$e(P,Q)$	$n_T(P,Q)$	$e(P,Q)$
زمان	0.46s	0.62s	0.06s	0.08s
ROM	29.55KB	44.40KB	29.55KB	44.40B
انرژی مصرفی	12.12mJ	16.34mJ	3.76mJ	5.02mJ



(شکل۱): مقایسه بین پیاده‌سازی توابع زوج‌سازی مختلف بر روی برخی از انواع حس‌گرها [۲۲]

(جدول۵): پیاده‌سازی توابع زوج‌سازی تعریف‌شده روی بهازای حسگرهای MICA2 و TmoteSky[۲۲]

	MICA2		Tmote Sky	
	$n_T(P,Q)$	$e(P,Q)$	$n_T(P,Q)$	$e(P,Q)$
زمان	2.66s	7.43s	1.71s	4.61s
ROM	47.41KB	60.9KB	23.66KB	34.88B
انرژی مصرفی	62.73mJ	175.65mJ	17.70mJ	50.89mJ

(جدول۶): زمان اجرای ECDSA برروی MICAz بهازای w=4[۱۰]

منحنی	آغازین	امضا	تصدیق
secp 128r1	2.522	1.923	2.418
secp 128r2	2.518	2.069	2.674
secp 160k1	3.553	2.059	2.441
secp 160r 1	3.548	1.925	2.433
secp 160r2	3.543	2.066	2.615
secp 192k1	4.992	3.070	3.612
secp 192r1	4.992	2.991	3.776

۴- بررسی الگوریتم ECDSA حس‌گرهای MICAz، TelosB و Imote2

در این بررسی الگوریتم ECDSA با استفاده از منحنی‌های منتخب SecG تعریف‌شده بر روی میدان‌های نخست۱۲۸،۱۶۰،۱۹۲ بیتی پیاده‌سازی شده‌اند. حس‌گرهای مورد آزمایش شامل MICAz، TelosB و Imote2 هستند. در جداول زیر نتایج حاصل از پیاده‌سازی ECDSA برروی MICAz، TelosB و Imote2 ارائه شده است. همچنین طول قالب در روش ضرب اسکالر قالبی برابر w=4 است.

(جدول۷): زمان اجرای ECDSA بر روی TeloseB بهازای w=4[۱۰]

منحنی	آغازین	امضا	تصدیق
secp 128r1	3.861	4.059	5.056
secp 128r2	3.847	4.325	5.618
secp 160k1	5.208	4.433	5.209
secp 160r1	5.225	4.361	5.448
secp 160r2	5.197	4.457	5.609
secp 192k1	7.190	6.695	7.840
secp 192r1	7.204	6.651	8.331

(جدول۸): زمان اجرای ECDSA برروی Imote2 بهازای w=4[۱۰]

Curve	104MHz			416 MHz		
	آغازین	امضا	تصدیق	آغازین	امضا	تصدیق
secp 128r1	0.136	0.255	0.317	0.035	0.065	0.083
secp 128r2	0.136	0.255	0.360	0.035	0.069	0.095
secp 160k1	0.151	0.180	0.219	0.038	0.049	0.060
secp 160r1	0.148	0.167	0.205	0.037	0.042	0.054
secp 160r2	0.151	0.187	0.233	0.038	0.047	0.060
secp 192k1	0.190	0.265	0.308	0.050	0.067	0.079
secp 192r1	0.200	0.265	0.325	0.050	0.068	0.084

در جدول زیر انرژی مورد نیاز محاسبه ECDSA بر روی این سه نوع حس‌گر به‌ازای یک منحنی خاص و طول قالب‌های مختلف نشان داده شده است.

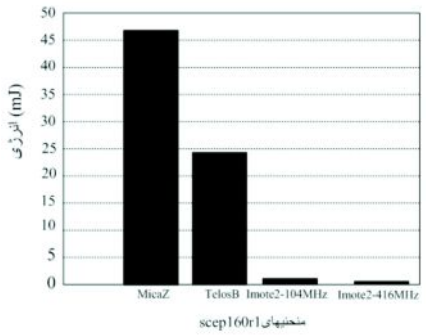
(جدول۹): انرژی مورد نیاز برای محاسبه ECDSA برحسب mj به‌ازای منحنی secp160r1[۱۰]

w	MICAz		TeloseB	
	امضا	تصدیق	امضا	تصدیق
2	52.9	58.4	27.5	29.4
4	46.2	58.4	23.5	29.4
8	-	-	-	-

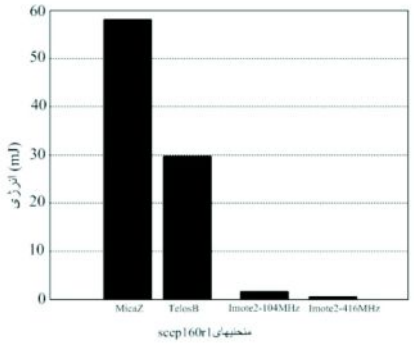
(جدول۱۰): انرژی مورد نیاز برای محاسبه ECDSA برحسب mj به‌ازای منحنی secp160r1[۱۰]

w	Imote2					
	13MHz		104MHz		416MHz	
	امضا	تصدیق	امضا	تصدیق	امضا	تصدیق
2	2.56	2.72	0.32	0.34	0.08	0.10
4	2.19	2.72	0.28	0.34	0.07	0.09
8	-	-	0.24	0.34	0.06	0.09

انرژی مورد نیاز مراحل امضا و تصدیق الگوریتم ECDSA به‌ازای منحنی‌های secp160r1 بر روی حس‌گرهای مختلف به‌طور خلاصه در نمودارهای زیر بیان شده‌اند.

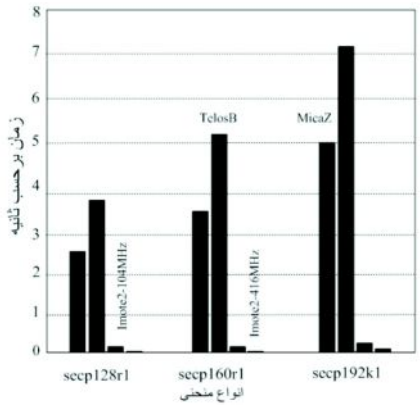


(شکل۲): انرژی مورد نیاز مرحلهٔ امضا ECDSA بر روی برخی از حس‌گرها[۱۰]

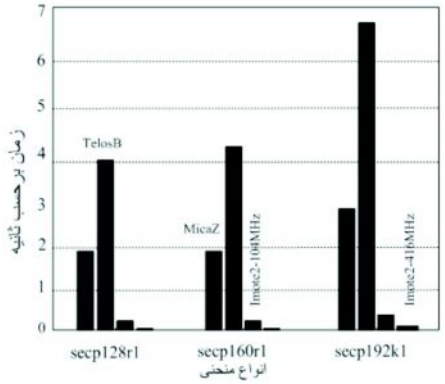


(شکل۳): انرژی مورد نیاز مرحلهٔ تصدیق ECDSA بر روی برخی از حس‌گرها[۱۰]

همچنین زمان مورد نیاز مراحل آغازین و امضای الگوریتم ECDSA به‌ازای منحنی‌های مختلف بر روی حس‌گرهای مختلف در زیر آورده شده است.



(شکل۴): زمان اجرای مرحلهٔ آغازین ECDSA بر روی برخی از حس‌گرها[۱۰]



(شکل۵): زمان اجرای مرحلهٔ امضا ECDSA بر روی برخی از حس‌گرها[۱۰]

با توجه به نتایج ارائه‌شده در بالا مشاهده می‌کنیم که حس‌گرهای مدرن نوع Imote2 برای پیاده‌سازی رمزنگاری مبتنی بر منحنی‌های بیضوی بسیار مناسب‌تر از حس‌گرهای MICAz و TeloseB است.

۵- پیاده‌سازی توابع زوج‌سازی بر روی حسگرهای MICAz، TelosB و Imote2

حال به بیان پیاده‌سازی توابع زوج‌سازی بر روی این حس‌گرهای MICAz، TelosB و Imote2 می‌پردازیم. از آنجا که محاسبه یک تابع زوج‌سازی مانند تابع تیت[1] همان‌طور که درقبل نیز ذکر شد، بسیار پرهزینه است، بنابراین حس‌گر پرتوان Imote2 نسبت به MICAz و TeloseB بسیار مناسب‌تر است. در این قسمت برخی از نتایج پژوهش‌های انجام‌شده را در جهت پیاده‌سازی تابع تیت بر روی Imote2 بیان می‌کنیم. در این بررسی اندازهٔ برنامهٔ نوشته‌شدهٔ زمان و انرژی لازم را برای پیاده‌سازی تابع تیت برروی Imote2 به‌ازای منحنی‌های بالای تکین[2] تعریف‌شده بر روی میدان متناهی نخست ۱۹۲ بیتی و ۵۱۲ بیتی نشان داده شده است. اندازهٔ برنامه نرم‌افزاری نوشته بر روی Imote2 برای محاسبه تابع تیت در جدول۱۱ آورده شده است. از آنجا که اندازهٔ حافظهٔ RAM حس‌گر Imote2 برابر 32MB است، بنابراین هر دو نوع منحنی اندازهٔ برنامه قابل قبول است. برای حافظه ROM نیز به همین ترتیب است.

(جدول۱۱): اندازهٔ برنامهٔ محاسبهٔ تیت بر روی Imote2[۱۰]

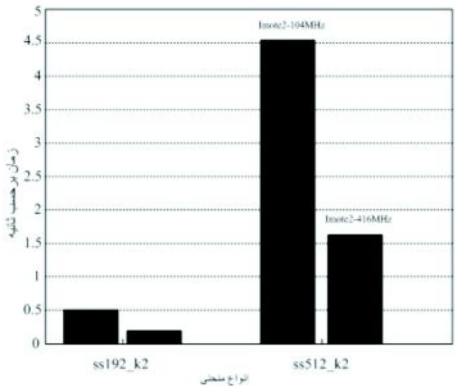
منحنی	ROM	RAM
ss192k2	13,512	434
ss512k2	13,844	1,034

(جدول۱۲): زمان اجرای الگوریتم تیت بر روی Imote2[۱۰]

منحنی	104MHz		
	میلر	توان رسانی آخر	مجموع
ss192k2	0.459	0.032	0.491
ss512k2	4.405	0.154	4.559

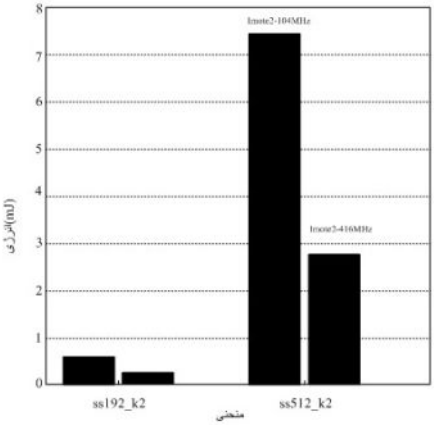
(جدول۱۳): زمان اجرای الگوریتم تیت بر روی Imote2[۱۰]

منحنی	416MHz		
	میلر	توان رسانی آخر	مجموع
ss192k2	0.115	0.008	0.123
ss512k2	1.575	0.055	1.629



(شکل۶): زمان اجرای الگوریتم تیت بر روی Imote2 [۱۰]

همان‌طورکه می‌دانیم، محاسبهٔ تابع تیت دارای دو قسمت اصلی است که یکی الگوریتم میلر و دیگری عمل توان‌رسانی در آخر الگوریتم تیت است. پرهزینه‌ترین عمل در الگوریتم تیت الگوریتم میلر است. زمان مورد نیاز برای اجرای الگوریتم تیت بر روی Imote2 را در جدول‌های(۱۲)و(۱۳) بیان می‌کنیم. با توجه به زمان اجرای الگوریتم تیت به‌ازای منحنی ۵۱۲ بیتی که برخلاف منحنی ۱۹۲ بیتی دارای سطح امنیتی مناسبی است، درمی‌یابیم که می‌توانیم از این الگوریتم در کاربردهای واقعی WSN استفاده شود؛ ولی ممکن است، حملات DoS بر روی حس‌گر مورد نظر قابل انجام باشد که برای جلوگیری از این امر می‌توانیم از مختصات تصویری استفاده کنیم که در این صورت می‌توانیم زمان محاسبه را تا ده برابر سریع‌تر کنیم. حال انرژی مورد نیاز را برای پیاده‌سازی الگوریتم تیت بر روی Imote2 با جدول و نمودار زیر بیان می‌کنیم.



(شکل۷): انرژی مصرفی الگوریتم تیت بر روی Imote2 [۱۰]

[1]Tate
[2]Super singular

(جدول۱۴): انرژی مصرفی الگوریتم تیت بر روی Imote2 [۱۰]

منحنی	104MHz	416MHz
ss192k2	0.80	0.20
ss512k2	7.47	2.67

از آنجا که انرژی مورد نیاز محاسبه الگوریتم تیت بر روی Imote2 بسیار کمتر از انرژی مورد نیاز برای اجرای مرحلهٔ تصدیق الگوریتم ECDSA بر روی TeloseB , MICAz است، بنابراین انرژی مصرفی الگوریتم تیت بر Imote2 قابل قبول می‌باشد.

۶- نتیجه‌گیری

محاسبهٔ یک تابع زوج‌سازی مانند تابع تیت بسیار پرهزینه است؛ بنابراین حس‌گر پرتوان Imote2 نسبت به حس‌گرهای MICAz و TeloseB بسیار مناسب‌تر است. بسته ارائه شده در [۲۲] نسبت به بسته‌های نرم‌افزاری NanoECC ، Tinytate، Tiny PBC در مجموع عملکرد بهتری دارد .

۷-مراجع

[1] D. Boneh, H. Shacham, and B. Lynn, “Short signatures from the Weil pairing,” in Advances in Cryptology – ASIACRYPT 2001, pp. 514-532, 2001.

[2] D. Boneh and X. Boyen, “Short signatures without random oracles and the SDH assumption in bilinear groups,” J. Cryptology, vol. 21(2), pp.149–177, 2008.

[3] Crossbow Technology Inc. Imote2{High-Performance Wireless Sensor Network Node. http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/Imote2_Datasheet.pdf.

[4] Crossbow Technology Inc. MICAz { Wireless Measurement System. Available at http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICAz_Datasheet.pdf.

[5] Crossbow Technology Inc. TELOSB { TELOSB Mote Platform. Available at http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf.

[6] H. Deng, A. Mukherjee, and D. Agrawal, Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), 107-111, 2004.

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

[8] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs, The 6th International Workshop on Cryptographic Hardware and Embedded Systems-CHES 2004, LNCS 3156, M. Joye and J.-J. Quisquater (eds.), Berlin, Germany: Springer-Verlag, 119-132, 2004.

[9] K. Hoeper and G. Gong, Identity-Based Key Exchange Protocols for Ad Hoc Networks", Proceedings of the Canadian Workshop on Information Theory (CWIT'05), 127-130, 2005.

[10] P. T. Kampanakis, Identity-Based Cryptography: Feasibility & Applications in Next Generation Sensor Networks, Master of Science thesis, North Carolina State University, 2007.

[11] A. Liu and P. Ning, TinyECC: A Con_gurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks, Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN 2008), SPOTS Track,. 245- 256, 2008.

[12] J. López, D. Aranha, D. Camara, R. Dahab, L. Oliveira, and C. Lopes, Fast Implementation of Elliptic Curve Cryptography and Pairing Computation for Sensor Networks, The 13th Workshop on Elliptic Curve Cryptography (ECC 2009), 2009, http://ecc.math.ucalgary.ca/sites/ecc.math.ucalgary.ca/files/u5/Lopez_ECC2009.pdf.

[13] D. J. Malan, M. Welsh, and M. D. Smith, Implementing Public-Key Infrastructure for Sensor Networks, ACM Transactions on Sensor Networks, vol. 4, no. 4,. 22:1-22:23, 2008.

[14] 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.

[15] L. B. Oliveira, M. Scott, J. López, and R. Dahab, TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks, Proceedings of the 5th International Conference on Networked Sensing Systems (INSS 2008), 173-180, 2008.

[16] E. Öztürk, B. Sunar, and E. Savascedil. Low-power elliptic curve cryptography using scaled modular arithmetic. In Proc. of CHES'04, volume 3156 of LNCS, 92–106. Springer-Verlag, 2004.

[17] N. Saxena, G. Tsudik, and J.H. Yi, Identity-Based Access Control for Ad Hoc Groups", The 7th International Conference on Information Security and Cryptology - ICISC 2004), LNCS 3506, C. Park, S. Chee (eds.), Berlin, Germany: Springer- Verlag, 362-379, 2004.

[18] Standards for Efficient Cryptography Group (SECG), http://www.secg.org.

[19] S. C. Seo, D.-G. Han, and S. Song, TinyECCK: Efficient Elliptic Curve Cryptography Implemenation over GF(2m) on 8-bit Micaz Mote", IEICE Transactions on Information and Systems, E91-D(5):1338-1347, 2008.

[20] M. Shirase, Y. Miyazaki, T. Takagi, D.-G. Han, and D. Choi, Efficient Implementation of Pairing Based Cryptography on a Sensor Node", IEICE Transactions on Information and Systems, E92-D(5):909-917, 2009.

[21] P. Szczechowiak, L. Oliviera, M. Scott, M. Collier, and R. Dahab. NanoECC: Testing the limits of Elliptic Curve Cryptography in Sensor Networks. In Wireless Sensor Networks – EWSN 2008, volume 4913 of Lecture Notes in Computer Science, 305–320. Springer-Verlag, 2008.

[22] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, On the Application of Pairing Based Cryptography to Wireless Sensor Networks", Proceedings of the Second ACM Conference on Wireless Network Security (WiSec'09), 1-12, 2009.

[23] TinyOS 2.1: a free and open source component-based operating system and platform targeting wireless sensor networks (WSNs).

[24] TinyPairing library for wireless sensor networks. Available: http://www.cs.cityu.edu.hk/_ecc/TinyPairing.

[25] H. Wang and Q. Li, Efficient Implementation of Public Key Cryptosystems on MICAz Motes", The 8th International Conference on Information and Communications Security-ICICS 2006, LNCS 4307, P. Ning, S. Qing, and N. Li (eds.), Berlin, Germany: Springer-Verlag, 519-528, 2006.

[26] R. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, and P. Kruus. TinyPK: Securing Sensor Networks with Public Key Technology. In SASN '04: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, 59–64, New York, NY, USA, ACM, 2004.

[27] 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.

[28] T. Wollinger, Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems.PhD thesis, Department of Electrical Engineering and Information Sciences, Ruhr-UniversitätBochum, Bochum, Germany, 2004.

[29] X. Xiong, D. C. Wong, and X. Deng, TinyPairing: Computing Tate Pairing on Sensor Nodes with Higher Speed and Less Memory", Proceedings of the Eighth IEEE International Symposium on Network Computing and Applications (NCA'09), 187-194, 2009.

[30] Y. Zhang, W. Liu, W. Lou, and Y. Fang, Securing Mobile Ad Hoc Networks with Certificateless

[31] Public Keys", IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, 386-399, 2006.

[32] Y. Zhang, W. Liu, W. Lou, and Y. Fang, Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, 247-260, 2006.

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.