The 1st National Conference on Recent Advances in Engineering and Modern Sciences
09 May 2018 / Tehran - Iran
IRIB International Conference Center
کنفرانس ملی پیشرفت‌های اخیر در مهندسی و علوم نوین

تحلیل امنیت یک طرح امضا انبوه فاقد گواهینامه

نصراله پاک‌نیت

پژوهشکده علوم اطلاعات، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، تهران، ایران

pakniat@irandoc.ac.ir

بهنام عباسی وندا

دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران

behnam_abasi@vu.iust.ac.ir

چکیده:

در سیستم‌های رمزنگاری مبتنی بر شناسه، مرکز تولید کلید به کلید خصوصی تمام کاربران دسترسی داشته و قادر است اعمالی مانند امضا و رمزگشایی را از طرف کاربران انجام دهد که به این مساله، مساله key escrow گویند. سیستم‌های رمزنگاری فاقد گواهینامه به عنوان راه‌حلی برای حل مساله key escrow ارائه شده‌اند. در این سیستم‌ها، مرکز تولید کلید تنها بخشی از کلید خصوصی کاربر را ایجاد کرده و تنها خود کاربر به کلید خصوصی کامل خود دسترسی دارد. اخیرا، Baoyuan وهمکاران یک طرح امضا انبوه بسیار کارا در زمینه رمزنگاری فاقد گواهینامه ارائه کرده و ادعا کرده‌اند که طرح آن‌ها تمام نیازمندی‌های امنیتی موردنیاز را تامین می‌کند. در این مقاله نشان می‌دهیم که ادعای فوق اشتباه بوده و طرح Baoyuan و همکاران از مساله key escrow رنج می‌برد. به عبارتی دیگر، نشان می‌دهیم که در این طرح مرکز تولید کلید بدون نیاز به دسترسی به کلید خصوصی کامل کاربران قادر است امضا آن‌ها را جعل کند.

واژه‌های کلیدی : امضا دیجیتال، امضا انبوه، رمزنگاری فاقد گواهینامه، جعل‌پذیری.

1. مقدمه:

در سیستم‌های رمزنگاری کلید عمومی سنتی(PKI)، کلید عمومی هر کاربر مقداری تصادفی است. در این سیستم‌ها، از گواهینامه‌های دیجیتال برای اطمینان از تعلق یک کلید عمومی به یک کاربر استفاده می‌شود. صدور و بررسی اعتبار گواهینامه‌ها در سیستم‌های PKI مساله‌ای هزینه‌بر بوده که از آن به عنوان مساله مدیریت گواهینامه‌ها یاد می‌شود. برای حل مساله مدیریت گواهینامه‌ها، در (Shamir,1984) ، مفهوم رمزنگاری مبتنی بر شناسه ارائه شد. در یک سیستم رمزنگاری مبتنی بر شناسه، کلید عمومی هر کاربر اطلاعی عمومی و یکتا از او (مانند شماره تلفن، آدرس ایمیل، آدرس IP و غیره) بوده و کلید خصوصی متناظر توسط مرکزی مورد اعتماد به نام مرکز تولید کلید ایجاد شده و به صورت محرمانه به کاربر ارسال می‌شود. با توجه به استفاده از شناسه به عنوان کلید عمومی و اعتماد به مرکز تولید کلید برای ارسال کلید خصوصی متناظر با یک شناسه به صاحب واقعی آن، در سیستم‌های مبتنی بر شناسه گواهینامه‌ای وجود نداشته و در نتیجه مساله مدیریت گواهینامه‌ها حل شده است. با این وجود، در این سیستم‌ها، مرکز تولید کلید به کلید خصوصی تمام کاربران دسترسی داشته و در نتیجه قادر است اعمال رمزنگاری مانند رمزگشایی و امضا دیجیتال را از طرف آن‌ها انجام دهد که به این مساله، مساله key escrowگویند. برای حل همزمان مسائل مدیریت گواهینامه‌ها وkey escrow ، در (Al-Riyami and Paterson, 2003) مفهوم رمزنگاری فاقد گواهینامه معرفی شده است. همانند سیستم‌های رمزنگاری مبتنی بر شناسه، در سیستم‌های رمزنگاری فاقد گواهینامه نیز مرکز تولید کلید (KGC) وجود داشته اما در اینجا این مرکز تنها بخشی از کلید خصوصی کامل کاربر به نام کلید خصوصی جزئی را با توجه به شناسه او تولید کرده و در اختیار او قرار می‌دهد. قسمت دیگر از کلید خصوصی کاربر توسط خود او انتخاب و محرمانه نگهداری می‌شود. در این سیستم‌ها، هر کاربر علاوه بر شناسه دارای یک کلید عمومی نیز بوده که با استفاده از قسمت دوم از کلید خصوصی او و مقادیری عمومی محاسبه شده و بدون نیاز به گواهینامه اعلام عمومی می‌شود. مفهوم امضا انبوه برای اولین بار در (Boneh et al, 2003) توسط Boneh و همکارانش ارائه شده است. با استفاده از یک طرح امضا انبوه، می‌توان n امضا ایجاد شده بر روی n پیام از طرف n کاربر را در یک امضا تجمیع و ارسال کرد و بدین طریق هم حجم داده‌های ارسالی و هم بار محاسباتی مورد نیاز برای تصدیق درستی امضاها را کاهش داد. این ویژگی امضاهای انبوه، آن‌ها را به ابزاری کاربردی مخصوصا در محیط‌های با محدودیت در حجم ارسال داده‌ها یا محدودیت در محاسبات تبدیل می‌کند. پس از ارائه اولین طرح امضا انبوه در (Boneh et al, 2003)، طرح‌های امضا انبوه زیادی در زمینه‌های رمزنگاری PKI و مبتنی بر شناسه ارائه شده که علاقمندان می‌توانند برای اطلاعات بیشتر به [4-10] مراجعه کنند. در سالیان گذشته، با توجه به مزیت‌های رمزنگاری فاقد گواهینامه، چندین طرح امضا انبوه فاقد گواهینامه (CLAS) ارائه شده است [11-20] . علی‌رغم کاهش هزینه‌های محاسباتی در تصدیق امضاهای انبوه، اغلب طرح‌های امضا انبوه فاقد گواهینامه ارائه شده تا به امروز همچنان ناکارا بوده و یا دارای مشکل امنیتی هستند. درسال2017، Baoyuan و همکاران(Baoyuan et al, 2017) یک طرح امضا انبوه فاقد گواهینامه جدید ارائه کرده‌اند که بنا بر ادعای نویسندگان از سایر طرح‌های موجود در این زمینه کاراتر می‌باشد. علاوه بر این، نویسندگان ادعا کرده‌اند که طرح ارائه شده در برابر هر دو نوع متخاصم در نظر گرفته شده در سیستم‌های رمزنگاری فاقد گواهینامه تامین کننده سطح امنیت جعل‌ناپذیری وجودی در برابر حمله انتخاب متن آگاهانه می‌باشد. در این مقاله نشان خواهیم داد که ادعای Baoyuan و همکاران در مورد امنیت طرح ارائه شده در (Baoyuan et al, 2017) اشتباه بوده و طرح

ارائه شده توسط آن‌ها در برابر مرکز تولید کلید بداندیش ناامن است. به بیان دقیق‌تر، در این مقاله نشان خواهیم داد که با دسترسی به یک امضا ایجاد شده توسط یک کاربر، مرکز تولید کلید بداندیش قادر است امضا او را روی هر پیام دلخواهی جعل کند. در ادامه این مقاله، در بخش 2 شمای کلی و مدل امنیتی یک طرح امضا انبوه فاقدگواهینامه را بررسی خواهیم کرد. در بخش 3، طرحCLAS پیشنهاد شده Baoyuan و همکاران را بررسی می‌کنیم. حمله پیشنهاد شده بر روی طرح Baoyuan و همکاران در بخش 4 ارائه شده و در نهایت نتیجه‌گیری‌های این مقاله در بخش 5 ارائه خواهد شد.

2.طرح‌های امضا انبوه فاقد گواهینامه(CLAS)

1.2 شمای کلی یک طرح CLAS

افراد موجود در یک طرح امضا انبوه فاقد گواهینامه عبارتند از مرکز تولید کلید(KGC) ، مجموعه فرستنده ها$(u_1, u_2, \cdots, u_n)$، دریافت‌کننده (u_R) و تولیدکننده امضا انبوه. یک طرح امضا انبوه فاقد گواهینامه از شش الگوریتم راه‌اندازی، تولید کلید خصوصی جزیی، تولید کلید کاربر، امضا، انبوه‌سازی و تایید اصالت انبوه تشکیل شده است. در ادامه هریک از این الگوریتم‌ها را بررسی خواهیم کرد.

1. **راه‌اندازی**: این الگوریتم توسط KGC انجام شده و با دریافت پارامتر امنیت k به عنوان ورودی، پارامترهای عمومی سیستم params و یک کلید مخفی اصلی MSK که به صورت تصادفی انتخاب شده است را بازمی‌گرداند.
2. **تولید کلید خصوصی جزیی**: این الگوریتم توسط KGC انجام شده و با دریافتparams ، کلید مخفی اصلی MSK و شناسه ID_i متناظر با کاربر u_i به عنوان ورودی، کلید خصوصی جزیی D_i متناظر با شناسه ID_i را تولید کرده و از طریق یک کانال امن به کاربر u_i بازمی‌گرداند.
3. **تولید کلید کاربر**: این الگوریتم توسط هر کاربر دلخواه u_i انجام شده و با ورودی params و شناسه u_i ، مقدار مخفی تصادفی x_i و کلید عمومی متناظر با این مقدار P_i را بازمی‌گرداند. x_i به صورت محرمانه نزد u_i نگهداری شده و P_i به عنوان کلید عمومی متناظر، بدون نیاز به گواهینامه، منتشر می‌شود.
4. **امضا**: این الگوریتم توسط هرامضاکنندهu_i (i=1,…,n) با شناسه ID_i اجرا شده و با ورودی params ،اطلاعات وضعیتw، پیام $m_i \in \{0,1\}^*$ و کلید خصوصی(D_i , x_i) ،امضا σ_i را به عنوان خروجی بازمی‌گرداند.
5. **انبوه‌سازی**: این الگوریتم n امضا متمایز $\sigma_1, \sigma_2, \cdots, \sigma_n$ تولید شده توسط کاربران $u_1, u_2, \cdots, u_n$ را به عنوان ورودی دریافت کرده و امضا انبوه σ بر روی پیام‌های$(m_1, m_2, \cdots, m_n)$ را به عنوان خروجی بازمی‌گرداند.
6. **تایید اصالت انبوه**: این الگوریتم پارامترهای عمومی سیستم params، اطلاعات وضعیتw، شناسه‌های امضاکنندگان $ID_1, ID_2, \cdots, ID_n$، کلیدهای عمومی امضاکنندگان $P_1, P_2, \cdots, P_n$ ، پیام‌های $(m_1, m_2, \cdots, m_n)$ و امضا انبوه σ را به عنوان ورودی دریافت کرده و اگر امضا انبوه معتبر باشد صحیح و در غیر این صورت غلط را بازمی‌گرداند .

2.2 مدل امنیتی طرح‌هایCLAS

به طور معمول، در بررسی امنیت سیستم‌های رمزنگاری فاقد گواهینامه دو نوع متخاصم در نظر گرفته می‌شود. متخاصم نوع I (A_1) که به کلید مخفی اصلی دسترسی نداشته اما قادر به تعویض کلید عمومی کاربران است. این نوع متخاصم، کاربران بداندیش بیرونی را شبیه‌سازی می‌کند.متخاصم نوع II (A_2) که به کلید مخفی اصلی دسترسی داشته اما قادر به تعویض کلید عمومی کاربران نیست. این نوع متخاصم شبیه‌ساز مرکز تولید کلید بداندیش است که قصد دارد از اطلاعاتی که در اختیار دارد سوء استفاده کند. به طور معمول، امنیت یک طرح CLAS با استفاده از دو بازی بین چالشگر C و متخاصمین نوع اول A_1 یا دوم A_2 مدل‌سازی می‌شود. در ادامه این بخش، از آن‌جا که هدف ما در این مقاله نشان دادن ناامنی طرح CLAS ارائه شده توسط Baoyuan و همکاران (Baoyuan et al, 2017) در برابر متخاصم نوع II است، تنها بازی متناظر با متخاصم نوع II را مرور می‌کنیم. در [21] این بازی به صورت زیر تعریف شده است.

بازی:II

فاز راه‌اندازی:در این فاز، C با دریافت پارامتر امنیت k به عنوان ورودی، الگوریتم آماده‌سازی را اجرا کرده، پارامترهای عمومی سیستم params و کلید مخفی اصلی MSK را تولید کرده و در اختیار (A_2) قرار می‌دهد.

فاز درخواست‌ها: در این فاز A_2 قادر است به صورت سازگارپذیر تعدادی درخواست (محدود به چندجمله‌ای) به C ارائه کند و C پاسخ‌های مناسب را به A_2 بازمی‌گرداند. درخواست‌های قابل انجام از طرف متخاصم عبارتند از:

- **درخواست چکیده**: از طریق این درخواست A_2 می‌تواند مقدار چکیده متناظر با هر ورودی را درخواست کند. C در پاسخ به این درخواست با استفاده از تابع درهم‌ساز مورد نظر مقدار چکیده متناظر با ورودی را محاسبه کرده و به A_2 بازمی‌گرداند.
- **درخواست کلید عمومی**: از طریق این درخواست A_2 قادر است کلید عمومی متناظر با هر امضاکننده‌ای با شناسه دلخواه را درخواست کند. C در پاسخ به این درخواست، با اجرا کردن الگوریتم تولید کلید کاربر،کلید عمومی متناظر یعنی P_i را بازمی‌گرداند.
- **درخواست مقدار مخفی**: از طریق این درخواست A_2می‌تواند مقدار مخفی متناظر با هر امضاکننده‌ای باشناسه دلخواه را درخواست کند. C در پاسخ به این درخواست، با اجرا کردن الگوریتم تولید کلید کاربر، مقدار مخفی متناظر را بازمی‌گرداند.
- **درخواست امضا**: از طریق این درخواست A_2 می‌تواند امضا یک کاربر دلخواه U_i بر روی پیام m_i تحت اطلاعات وضعیت w را درخواست کند. C در پاسخ به این درخواست با اجرا کردن الگوریتم امضا، امضا σ_i را بازمی‌گرداند.

فاز جعل: پس از پایان فاز درخواست‌ها، A_2 چهارتایی $(m^*, w^*, ID^*, \sigma^*)$ را خروجی می‌دهد که $m^* = (m_1^*, m_2^*, \cdots, m_n^*)$ مجموعه پیام‌ها، w^* اطلاعات وضعیت، $ID^* = (ID_1^*, ID_2^*, \cdots, ID_n^*)$ مجموعه شناسه‌های متناظر با امضاکنندگان و σ^* و امضا انبوه جعل شده می‌باشد. A_2 برنده این بازی است اگر:

1) σ^* یک امضا انبوه معتبر بر روی پیام‌های $(m_1^*, m_2^*, \cdots, m_n^*)$ تحت اطلاعات وضعیت w^* ، از طرف کاربرانی با شناسه‌های $(ID_1^*, ID_2^*, \cdots, ID_n^*)$ و کلید عمومی‌های متناظر $(pk_1^*, pk_2^*, \cdots, pk_n^*)$ باشد.

2) به ازای حداقل یکی از شناسه‌ها، که بدون از دست رفتن کلیت مساله فرض می‌کنیم این شناسه $ID_1^* \in ID^*$ باشد، در فاز درخواست‌ها "درخواست مقدار مخفی" متناظر با ID_1^* و درخواست امضا با ورودی (w^*, m_1^*, ID_1^*) صورت نگرفته باشد.

تعریف 1. یک طرح امضا انبوه فاقد گواهینامه را در برابر متخاصم نوع II (مرکز تولید کلید بداندیش) امن گویند هرگاه هیچ متخاصم احتمالاتی محدود به زمان چندجمله‌ای A_2 ای وجود نداشته باشد که بتواند با احتمالی غیرقابل چشم‌پوشی در بازی II پیروز شود.

3. مرور طرح CLAS ارائه شده توسط Baoyuan و همکاران

در این بخش، جزئیات طرح CLAS ارائه شده توسط Baoyuan و همکاران در (Baoyuan et al, 2017) را بررسی می‌کنیم. فرض کنید که KGC مرکز تولید کلید بوده و $U_1, U_2, \cdots, U_n$ مجموعه‌ای شامل n امضاکننده باشد. با توجه به این مفروضات، الگوریتم‌های تشکیل‌دهنده طرحCLAS ارائه شده توسط Baoyuan و همکاران به شرح زیر است:

- **آماده‌سازی**: در این الگوریتم، KGC با دریافت پارامتر امنیت k به عنوان ورودی، گروه جمعی G_1 و گروه ضربی G_2 هر دو از مرتبه q که q عددی اول است را انتخاب می‌کند. سپس، KGC مولد P در گروه G_1 و نگاشت دو خطی $e: G_1 \times G_1 \to G_2$ را انتخاب می‌کند. در ادامه، او عدد تصادفی $s \in Z_q^*$ را به عنوان کلید مخفی اصلی انتخاب کرده و مقدار $P_{pub} = sP$ را به عنوان کلید عمومی سیستم محاسبه می‌کند. سپس، KGC توابع درهم‌ساز $H_1, H_3, H_4: \{0,1\}^* \to G_1$ و $H_2: \{0,1\}^* \times \{0,1\}^* \times G_1 \times G_1 \to Z_q^*$ را انتخاب می‌کند. در انتها، KGC، s را به عنوان کلید مخفی اصلی محرمانه نزد خود نگهداری کرده و $params = (G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3, H_4)$ را به عنوان پارامترهای عمومی سیستم اعلام عمومی می‌کند.
- **تولید کلید خصوصی جزیی**: در این الگوریتم، KGC با ورودی کلید خصوصی اصلی s ، پارامترهای عمومی سیستم params و ID_i به عنوان شناسه یک کاربر U_i، ابتدا مقدار $Q_i = H_1(ID_i)$ را محاسبه کرده و سپس با استفاده از آن $D_i = sQ_i$ را به عنوان کلید خصوصی جزئی کاربر U_i محاسبه کرده و از طریق کانال امن به کاربر موردنظر ارسال می‌کند.

- **تولید کلید کاربر**: در این الگوریتم، کاربر U_i عدد تصادفی $x_i \in Z_q^*$ را به عنوان مقدار مخفی خود انتخاب کرده $P_i = x_i P$ را محاسبه کرده و اعلام عمومی می‌کند.
- **امضا**: در این الگوریتم، کاربر U_i با شناسه ID_i و کلید عمومی P_i ، اطلاعات وضعیت w و پیام m_i را به عنوان ورودی دریافت کرده و طی مراحل زیر امضا σ_i را بر روی آن تولید می‌کند.
  1) عدد تصادفی $r_i \in Z_q^*$ را انتخاب کرده و $R_i = r_i P$ را محاسبه می‌کند.
  2) $h_i = H_2(m_i, ID_i, P_i, R_i)$، $Z = H_3(w)$ و $F = H_4(w)$ را محاسبه می‌کند.
  3) $T_i = h_i D_i + x_i Z + r_i F$ را محاسبه می‌کند.
  4) σ_i را برابر با زوج (R_i, T_i) قرار می‌دهد.
- **انبوه‌سازی**: در این الگوریتم، انبوه‌ساز (که می‌تواند هر کاربری من جمله هر یک از امضاکنندگان) با دریافتn پیام و امضاهای روی این پیام‌ها یعنی $((m_1, \sigma_1 = (R_1, T_1)), \dots, (m_n, \sigma_n = (R_n, T_n)))$ امضا شده توسط n کاربر $U_1, \cdots, U_n$ (با استفاده از اطلاعات وضعیت یکسانw) به عنوان ورودی، $T = \sum_{i=1}^{n} T_i$ را محاسبه کرده و $\sigma = (R_1, \dots, R_n, T)$را به عنوان امضا انبوه نهایی محاسبه می‌کند.
- **تایید اصالت انبوه**: در این الگوریتم، دریافت‌کننده با ورودی امضا انبوه$\sigma = (R_1, \dots, R_n, T)$، پیام‌های $m_1, \cdots, m_n$ ، شناسه‌های $ID_1 \cdots, ID_n$ و کلیدهای عمومی $P_1, \cdots, P_n$ متناظر با n کاربر $U_1, \cdots, U_n$ و اطلاعات وضعیت w ، اعتبار امضا انبوه دریافتی را به صورت زیر بررسی می‌کند.

  1) $Q_i = H_1(ID_i)$ و $h_i = H_2(m_i, ID_i, P_i, R_i)$ را برای $1 \le i \le n$! $Z = H_3(w)$ و $F = H_4(w)$ را محاسبه می‌کند.
  2) $h_i = e(T, P) = e(P_{pub}, \sum_{i=1}^{n} h_i Q_i) e(Z, \sum_{i=1}^{n} P_i) e(F, \sum_{i=1}^{n} R_i)$ را محاسبه می‌کند.
  3) اگر معادله فوق برقرار باشد امضا معتبر بوده و صحیح را به عنوان خروجی بازمی‌گرداند و در غیر این صورت غلط را.

4. تحلیل امنیت طرح Baoyuan و همکاران

Baoyuan و همکاران ادعا کردند که طرح آن‌ها دارای سطح امنیت جعل‌ناپذیری وجودی در برابر حمله انتخاب متن سازگارپذیر است. در این بخش، نشان می‌دهیم که این ادعا اشتباه بوده و یک مرکز تولید کلید بداندیش به راحتی قادر است تا یک امضا معتبر را از طرف هر کاربری و بر روی هر پیام دلخواهی در این طرح ایجاد کند. جزئیات انجام کار و جعل امضا توسط مرکز تولید کلید بداندیش در طرح Baoyuan و همکاران در قضیه زیر و به صورت دقیق بیان شده است.

قضیه 1: **با توجه به تعریف 1**، طرح امضا انبوه فاقد گواهینامه ارائه شده توسط Baoyuan و همکاران جعل‌پذیر است. به عبارت دیگر، در این طرح، متخاصم نوع دوم (A_2، یعنی مرکز تولید کلید بداندیش) به راحتی می‌تواند در طول بازی II یک امضا انبوه جعل شده ایجاد کند.

اثبات:

برای سادگی فرض می‌کنیم n برابر با یک باشد. فرض کنید u_i کاربری با شناسه ID_i و کلید عمومی P_i در طرح Baoyuan و همکاران باشد. برای ایجاد یک امضا جعل شده معتبر σ' بر روی پیام m' با توجه به اطلاعات وضعیت w از طرف u_i ، A_2 در طول بازی II و در مقابل C به صورت زیر عمل می‌کند .

1) به C اجازه می‌دهد تا الگوریتم راه‌اندازی را اجرا کرده و پارامترهای عمومی سیستم params و کلید خصوصی اصلی را به او ارسال کند.
2) درخواست امضا با ورودی (m,ID_i,w) که $m\neq m'$ را صادر کرده و در پاسخ $\sigma=(R,S)$ را به عنوان امضا u_i روی پیام m با توجه به اطلاعات وضعیت w دریافت می‌کند.
3) با استفاده از کلید خصوصی اصلی، کلید خصوصی جزئی متناظر با u_i را به صورت $D_i = sH(ID_i)$ محاسبه می‌کند.
4) مقدار $H_i = h_i D_i$ را محاسبه می‌کندکه $h_i = H_2(m, ID_i, P_i, R)$.
5) مقدار $X_i = T_i - H_i$ را محاسبه می‌کند. بنابراین مقدار X_i برابر است با $x_iZ + rF$ که x_i مقدار مخفی متناظر با u_i و r مقدار تصادفی استفاده شده در تولید σ بوده که C از آن‌ها اطلاعی ندارد و $Z = H_3(w)$ و $F = H_4(w)$.
6) مقدار $h' = H_2(m', ID_i, P_i, R)$ و سپس مقدار $T' = X_i + h'D_i$ را محاسبه می‌کند.
7) $\sigma' = (R', S'')$ را به عنوان امضا جعل شده u_i روی پیام m' و تحت اطلاعات وضعیت w خروجی می‌دهد.

به راحتی می‌توان نشان داد که امضا ایجاد شده یک امضا معتبر از طرف u_i روی پیام m' و تحت اطلاعات وضعیت w است.لازم به ذکر است که در اثبات فوق تنها یک امضاکننده در نظر گرفته شده است. اما گسترش آن به حالت‌هایی با بیش از یک امضا کننده به راحتی قابل انجام است. در این راستا، ابتدا یک امضا تکی جعل شده ایجاد کرده و به راحتی و با جمع کردن آن را در امضا انبوه جایگذاری کرده و امضا انبوهی جعل شده با تعداد کاربر بیشتر ایجاد می‌شود.

5. نتیجه‌گیری

در این مقاله، ما امنیت یک طرح امضا انبوه فاقد گواهینامه که اخیرا توسط Baoyuan و همکاران ارائه شده بود را مورد بررسی قرار دادیم و اثبات کردیم که این طرح در برابر دشمن نوع دوم در نظر گرفته شده در سیستم‌های رمزنگاری فاقد گواهینامه (مرکز تولید کلید بداندیش) ناامن است. به عبارتی دقیق‌تر، نشان دادیم که در طرح ارائه شده توسطBaoyuan و همکاران، مرکز تولید کلید بداندیش قادر است با دسترسی به یک پیام و امضا روی آن، امضا معتبر روی هر پیام دیگری از طرف امضاکننده موردنظر جعل و ایجاد کند.

مراجع

[1] Shamir, A. (1984). Identity based cryptosystems and signature schemes, in: G.R. Blakley,D. Chaum (Eds.), Crypto-84, LNCS 196, Springer-Verlag, Santa Barbara, California, USA, 47–53.
[2] Al-Riyami, S. S., Paterson, K. G. (2003). Certificateless public key cryptography.Proceedings of the Asiacrypt'03. LNCS, vol. 2894. Springer-Verlag, 452–473.
[3] Boneh D, Gentry C, Shacham H, et al (2003). Aggregate and verifiably encrypted signatures from bilinear maps EUROCRPYT'03, LNCS 2656. Heidelberg: Springer-Verlag, 416-432.
[4] Cheng X, Liu J, Wang X. (2005). Identity-based aggregate and verifiably encrypted signatures from bilinear pairingICCSA'05, LNCS 3483. Heidelberg: Springer-Verlag, 1046-1054.
[5] Cheng Gentry C, Ramzan Z. (2006). Identity-based aggregate signature, PKC'06, LNCS3958. Heidelberg: Springer-Verlag, 257-273.
[6] Lu S, Ostrovsky R, Sahai A, et al. (2006). Sequential aggregate signatures and multisignatures without random oracles, EUROCRPYT'06, LNCS 4004. Heidelberg: Springer-Verlag, 465-485.
[7] Ruckert M, Schrode D. (2009). Aggregate and verifiably encrypted signatures from multilinear maps without random oracles, ISA'09, LNCS 5576. Heidelberg: Springer-Verlag, 750-759.
[8] Shao Z. (2005). Enhanced aggregate signature from pairings, CISC'05, LNCS 3822. Heidelberg: Springer-Verlag, 140-149.
[9] Shim K. (2010). An Id-based aggregate signature scheme with constant pairing computations, The Journal of System and Software, 83: 1873-1880.
[10] Kang B Y. (2012). ID-based aggregate signature scheme with constant pairing computations: attack and new construction, Journal of Computational Information Systems, 16 :6611- 6618.
[11] Gong Z, Long Y, Hong X, et al. (2007). Two certificateless aggregate signatures from bilinear maps, Eighth ACIS International Conference on Software Engineering, Artificial Intelligence,Networking, and Parallel Distributed Computing,ACIS.
[12] Xing H, Guan Z, Chen Z, et al. (2013). An efficient certificateless aggregate signature with constant pairing computations. Information Sciences, 10: 225-235.
[13] Yanai N, Tso R, Mambo M, et al. (2011). Certificateless orderedsequential aggregate signature scheme.Third International Conference on Intelligent Networking and Collaborative Systems, INCos 2011. Washington DC: IEEE Press: 662-667.
[14] Zhang L, Zhang F. (2009). A new certificateless aggregate signature scheme. Computer Communication, 32: 1079-1085.
[15] Cheng L, Wen Q, Jin Z, et al. (2015). Cryptanalysis and improvement of a certificateless aggregate signature scheme. Information Sciences, 295: 337-346.
[16] Zhang F, Shen L, Wu G. (2014). Notes on the security of certificateless aggregate signature schemes. Information Sciences, 287: 32-37.
[17] Horng S, Tzeng S, Huang P, et al. (2015). An efficient certificateless aggregate signature with conditional privacy-preserving forvehicular sensor networks. Information Sciences,317: 48-66.
[18] Du H, Huang M, Wen Q. (2013). Efficient and provably-secure certificateless aggregate signature scheme. ActaElectronicaSinica , 41(1): 72-76.
[19] Chen H, Wei S, Zhu C, et al. (2015). Secure certificateless aggregate signature scheme. Journal of Software, 26(5):1173-1180.
[20] Kang B Y, Xu D. (2016). A Secure certificateless aggregate signature scheme. International Journal of Security and ItsApplications, 10(3): 55- 68.
[21] Nie, H., Li, Y., Chen, W. and Ding, Y., (2016).. NCLAS: a novel and efficient certificateless aggregate signature scheme. Security and Communication Networks, in press.
[22] Baoyuan K., Wang M, and Jing Y. (2017). "An efficient certificateless aggregate signature scheme." Wuhan University Journal of Natural Sciences 22.2: 165-170.