A New (t,n) Designated Verifier Threshold Proxy Signature Scheme in the Standard Model

Mohammad Beheshti Atashgah[1*], Mahmoud Gardeshi[2], Mohammad Reza Aref[3]
1,2- Imam Hossein University, Tehran, Iran 3- Information Systems and Security Lab (ISSL), EE Department, Sharif University of Technology, Tehran, Iran
(Reccive: 2013/07/10, Accept: 2014/02/17)

Abstract

In a designated verifier threshold proxy signature scheme, an original signer can delegate his\her signing power to proxy signers such that any or more out of proxy signers can sign messages on behalf of the original signer but or less of the proxy signers cannot generate a valid proxy signature. Of course, the signature is issued for a designated receiver and therefore only the designated receiver can validate the proxy signature. In this paper, we propose a new designated verifier threshold proxy signature scheme and also show that our proposed scheme has provable security in the standard model. The security of proposed scheme is based on the assumption.

Keywords:

Proxy signature scheme, Threshold proxy signature scheme, Provable security, Standard model, Bilinear pairing.

***Corresponding Author Email:** M.Beheshti.A@gmail.com

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال دوم، شماره ۱، بهار۱۳۹۳، ص ۳۵-۲۵

یک (t , n) طرح امضای وکالتی آستانه با تأییدکننده مشخص جدید و اثبات امنیتی آن در مدل استاندارد

محمد بهشتی آتشگاه[1*]، محمود گردشی[2]، محمدرضا عارف[3]

۱- کارشناس ارشد، آزمایشگاه تئوری اطلاعات و مخابرات امن (ISSL)، دانشکده مهندسی برق، دانشگاه صنعتی شریف

۲- مربی، دانشگاه جامع امام حسین (ع)

۳- استاد، آزمایشگاه تئوری اطلاعات و مخابرات امن(ISSL)، دانشکده مهندسی برق، دانشگاه صنعتی شریف

(دریافت: ۹۲/٤/۱۹ ، پذیرش: ۹۲/۱۱/۲۸)

چکیده

در یک (t , n) طرح امضای وکالتی آستانه با تأییدکننده مشخص، صاحب امضاء، قابلیت امضای خود را به گروه n نفره از نمایندگان خود اعطاء می‌نماید تا در صورت توافق حداقل t نفر، بتوانند روی متن موردنظر امضای وکالتی صورت دهند. البته، این امضاء برای یک گیرنده مشخص صادر می‌شود و بنابراین، تنها او می‌تواند اعتبار امضاء را بررسی نماید. در این مقاله، یک (t , n) طرح امضای وکالتی آستانه با تأییدکننده مشخص جدید، ارائه شده و نیز نشان داده می‌شود که طرح ارائه‌شده، در مدل استاندارد دارای امنیت اثبات‌پذیر است. امنیت طرح ارائه‌شده، بر اساس فرض سختی مسئله دیفی- هِلمن دوخطی گپ GDBH استوار است.

واژه‌های کلیدی: طرح امضای وکالتی، طرح امضای وکالتی آستانه، امنیت اثبات‌پذیر، مدل استاندارد، زوج‌سازی دوخطی

۱. مقدمه

مفهوم امضای وکالتی، اولین بار در سال ۱۹۹۶ توسط مامبو[1] و همکارانش مطرح گردید[۱]. در یک امضای وکالتی، صاحب امضاء توانایی امضای خود را به نماینده‌اش اعطاء می‌نماید و بنابراین، او می‌تواند از جانب صاحب امضاء، روی متن مورد نظر امضاء صادر نماید. تاکنون طرح‌های امضای وکالتی بسیاری ارائه شده‌اند که [۲ و ۳] از این نمونه می‌باشند. کیم و ژانگ[2] به‌طور مستقل و به‌ترتیب، اولین طرح‌های امضای وکالتی آستانه بر اساس امضاهای وکالتی و طرح‌های تسهیم راز را مطرح نمودند[۴و ۵].

در یک (t , n) طرح امضای وکالتی آستانه، صاحب امضاء، قابلیت امضای خود را به گروه n نفره نمایندگان خود اعطاء می‌نماید تا در صورت توافق حداقل t نفر، بتوانند به نمایندگی از صاحب اصلی امضا، روی متن مورد نظر امضاء صورت دهند. از زمان ارائه اولین طرح امضای وکالتی آستانه تاکنون، طرح‌های زیادی ارائه شده که برای نمونه می‌توان به طرح‌های [۶ و ۷] اشاره نمود.

طرح‌های امضای وکالتی آستانه، دارای کاربردهای بسیاری است که از آن جمله، می‌توان به این مورد اشاره نمود: فرض نمایید که در یک شرکت، مدیرعامل (صاحب امضاء) قابلیت امضای خود را به هیئت مدیره (گروه نمایندگان) اعطاء نماید، به نحوی که هر سند قبل از آنکه رسمی گردد، باید توسط تعداد مشخصی از نمایندگان (که همان آستانه تعیین‌شده می‌باشد) امضاء شود. همچنین، طرح‌های امضاهای وکالتی آستانه در تجارت الکترونیک، شبکه‌های اقتضایی و در آژانس‌های سیار[3] کاربرد دارند.

1. Mambo
2. Kim and Zhang (et al.)
3. Mobile agents

* رایانامه نویسنده پاسخگو: M.Beheshti.A@gmail.com

یک طرح امضای وکالتی آستانه، باید ملزومات امنیتی زیر را داشته باشد [۸ و ۹]:

قابل تأیید بودن، غیرقابل جعل بودن، غیرقابل انکار بودن، قابل شناسائی بودن و جلوگیری از سوء استفاده.

اگرچه بسیاری از طرح‌های ارائه‌شده ادعا می‌کردند که تمامی ویژگی‌های بالا را برآورده می‌سازند، لیکن مفهوم امنیت آنها روشن و واضح نبود. اولین بار، بِلِیر و رُگاوِی[۴] مفهوم اثبات رسمی[۵] در مدل سروش تصادفی[۶] را برای پروتکل‌های توافق کلید ارائه کردند[۱۰]. پس از آنها، بولدیرِوا[۷] و همکارانش، امنیت امضای وکالتی را در مدل سروش تصادفی اثبات کردند و تاکنون، طرح‌های امضای وکالتی چون [۱۲ و ۱۳] ارائه شده‌اند که در این مدل، دارای امنیت قابل اثبات می‌باشند [۱۱].

مفهوم مدل استاندارد[۸] و اثبات امنیتی در این مدل نیز اولین بار توسط بونه و بوین[۹] برای یک طرح رمزنگاری مبتنی بر شناسه، ارائه شد که مدل ارائه‌شده آنها، مدل ID انتخابی[۱۰] بود [۱۴]. سپس، واترز[۱۱] در سال ۲۰۰۵ طی مقاله‌ای، یک طرح رمزنگاری مبتنی بر شناسه ارائه کرد و ثابت نمود که طرح او در مدل استاندارد، دارای امنیت قابل اثبات است [۱۵].

در حقیقت، مدل استانداردی که واترز ارائه نمود، کامل‌تر و کارآمدتر از مدل قبلی بود. هوآنگ[۱۲] و همکارانش در سال ۲۰۰۶، اولین طرح امضای وکالتی را در مدل استاندارد ارائه کردند [۱۶] و به تبع از آنان، طرح‌های دیگری مثل طرح امضای وکالتی با تأییدکننده مشخص یو و همکارانش[۱۳] در سال ۲۰۰۹ و طرح‌های دیگر، ارائه شدند [۱۷]. تا آنجا که اطلاع هست، هنوز طرح امضای وکالتی آستانه‌ای در مدل استاندارد، ارائه نشده است، بنابراین در این مقاله، اولین طرح امضای وکالتی آستانه با تأییدکننده مشخص به همراه اثبات امنیتی آن در مدل استاندارد، ارائه شده است. علاوه‌بر آن، نشان داده می‌شود که امنیت طرح ارائه‌شده، بر اساس فرض سختی مسئله GBDH استوار است.

ادامه مقاله، به این صورت سازمان‌دهی شده است: در قسمت بعد، مفاهیم پایه و مقدماتی مورد نیاز معرفی می‌شود. در بخش ۳، مدل رسمی برای یک طرح امضای وکالتی آستانه با تأییدکننده مشخص[۱۴] DVTPS بیان و طرح جدید در بخش ۴ ارائه می‌شود. در بخش ۵، طرح ارائه‌شده از لحاظ امنیتی، تحلیل و در نهایت، نتیجه‌گیری در قسمت ۶ بیان خواهد شد.

۲. مفاهیم پایه و مقدماتی

در این بخش، برخی از مفاهیم پایه‌ای شامل زوج‌سازی‌های دوخطی و فرض‌های پیچیدگی که در این مقاله استفاده خواهند شد، مرور می‌شود.

۱.۲. زوج‌سازی دوخطی

فرض کنید که G , G_T، دو گروه دوری ضربی از مرتبه p هستند که p، عدد اول بزرگی است و نیز g، مولد گروه G است.

نگاشت $e: G \times G \to G_T$ زوج‌سازی دوخطی پذیرفتنی نامیده می‌شود، اگر شرایط زیر را ارضا کند:

- دوخطی بودن: به ازای تمامی $a,b \in \mathbb{Z}_p$ شرط زیر برقرار باشد. $e(g^a, g^b) = e(g,g)^{ab}$
- زوال‌ناپذیری: $e(P,P) \neq 1_{G_T}$
- محاسبه‌پذیری: به‌ازای همه $g,h \in G$ یک الگوریتم کارآمد برای محاسبه $e(g,h)$ وجود دارد.

۲.۲. فرض‌های پیچیدگی

- **تعریف ۱** (مسئله دیفی- هِلمن دوخطی محاسباتی یا CBDH): به ازای پارامترهای نامعلوم $a,b,c \in \mathbb{Z}_p$، مقادیر $(g, g^a, g^b, g^c \in G)$ معلوم هستند و هدف، یافتن مقدار $e(g,g)^{abc}$ است.
- **تعریف ۲** (مسئله دیفی- هِلمن دوخطی تصمیمی یا DBDH): به‌ازای پارامترهای نامعلوم $a,b,c \in \mathbb{Z}_p$ و $w \in G_T$ مقادیر $(g, g^a, g^b, g^c \in G)$ معلوم هستند و قصد داریم تا تصمیم بگیریم که آیا $w = e(g,g)^{abc}$ ، است یا نه؟

یک پیشگوی DBDH[15] یعنی O_{DBDH}، پیشگویی است که پارامترهای $(g, g^a, g^b, g^c \in G)$ و $w \in G_T$ را به‌عنوان ورودی می‌گیرد و خروجی آن ۱ است، اگر $w = e(g,g)^{abc}$ و در غیر این صورت، خروجی آن صفر است.

4. Bellare & Rogaway
5. Formal proof
6. Random oracle
7. Boldyreva
8. Standard model
9. Boneh&Boyen
10. Selective-ID model
11. Waters
12. Huang
13. Yu et al.
14. Designated Verifier Threshold Proxy Signature Scheme
15. Oracle

- **تعریف ۳** (مسئله دیفی- هلمن دوخطی گپ یا GBDH): به ازای پارامترهای نامعلوم $a,b,c \in \mathbb{Z}_p$ مقادیر زیر معلوم هستند $(g, g^a, g^b, g^c \in G)$ و عبارت زیر با کمک پیشگوی DBDH یعنی ODBDH محاسبه می‌شود.

$$w = e(g,g)^{abc} \in G_T$$

احتمال موفقیت مهاجم A برای حل مسئله GBDH، به‌صورت زیر تعریف می‌شود:

$$Succ_{\mathcal{A}}^{GBDH} = \Pr[e(g,g)^{abc} \leftarrow \mathcal{A}(G, G_T, g, g^a, g^b, g^c, O_{DBDH})]$$

۳. مدل رسمی برای یک طرح DVTPS

در این بخش قصد داریم تا ابتدا مدل رسمی یک طرح امضای وکالتی آستانه با تأییدکننده مشخص را در مدل استاندارد بیان کرده و سپس مدل و ملزومات امنیتی آن را تعریف نماییم.

۱.۳. طرح اصلی

در یک طرح امضای وکالتی آستانه با تأییدکننده مشخص، سه نوع شرکت‌کننده به نام‌های صاحب امضاء (آلیس)، گروه نمایندگی $A = \{P_1, P_2, \cdots, P_n\}$ و تأییدکننده مشخص(سیندی) وجود دارند که از الگوریتم‌های زیر تشکیل شده است:

- **برپایی**: به ازای یک پارامتر امنیتی داده‌شده k، این الگوریتم پارامترهای سیستم را به عنوان خروجی می‌دهد.
- **تولید کلید**: این الگوریتم، پارامتر امنیتی k را به‌عنوان ورودی گرفته و زوج کلید عمومی/ خصوصی (sk_i, pk_i)، را که $i \in \{a, \{1,2,\cdots,n\}, c\}$ است، برای آلیس، گروه نمایندگی و سیندی تولید و به‌صورت خروجی بیرون می‌دهد.
- **تولید وکالت**: این الگوریتم، پارامترهای سیستم، کلید خصوصی صاحب امضاء و گواهینامه ω (که قرار است امضاء شود) را به‌صورت ورودی دریافت کرده و سهم وکالتی گروه نمایندگان را به‌صورت $\sigma_{\omega_{P_i}}$ تولید و به عنوان خروجی می‌دهد که $i = 1,2,\cdots,n$
- **تأیید وکالت**: به محض اینکه هر نماینده در گروه نمایندگی A، سهم وکالتی خود یعنی $(\omega, R_{a_i}, \sigma_{\omega_{P_i}})$ را دریافت نمود، اعتبار آن را بررسی و تأیید می‌نماید.
- **تولید امضای وکالتی**: این الگوریتم، ورودی‌هایی شامل: کلیدهای خصوصی نمایندگان امضاءکننده، $sk_i(i = 1,2,\cdots,t)$ سهم‌های وکالتی آنان، $\sigma_{\omega_{P_i}}(i = 1,2,\cdots,t)$ کلید عمومی تأییدکننده مشخص pk_c و متن مورد نظر m را برای تولید امضای وکالتی σ_p دریافت می‌کند.
- **تأیید امضای وکالتی**: یک الگوریتم معین که یک متن m، گواهینامه ω، یک امضای وکالتی، کلیدهای عمومی صاحب - امضاء و نمایندگان (pk_a, pk_{P_i}) و کلید مخصوص تأییدکننده مشخص sk_c را به‌عنوان ورودی گرفته و اگر امضاء معتبر باشد؛ خروجی $\top$ را می‌دهد، و در غیر این صورت (اگر امضاء معتبر نباشد)، خروجی $\perp$ را می‌دهد.
- **شبیه‌سازی رونوشت**: این الگوریتم پارامترهای متن m، گواهینامه ω و کلید خصوصی تأییدکننده مشخص sk_c را به‌عنوان ورودی گرفته و یک رونوشت با توزیع دقیقاً یکسان σ_P^* را به‌گونه‌ای تولید می‌نماید که از امضای وکالتی اصلی σ_p ، تمایزناپذیر است.

۲.۳. مدل امنیتی

به‌طور کلی، چهار نوع مهاجم بالقوه در این سیستم موجود است:

- **نوع I (A_I)**: مهاجم A_I، تنها کلیدهای عمومی صاحب امضاء، نمایندگان و تأییدکننده مشخص را دارد.
- **نوع II (A_{II})**: مهاجم A_{II}، کلیدهای عمومی صاحب امضاء، نمایندگان و تأییدکننده مشخص را دارد. به‌علاوه، کلید خصوصی صاحب امضاء (آلیس) را نیز در اختیار دارد.
- **نوع III (A_{III})**: مهاجم A_{III} کلیدهای عمومی صاحب امضا، نمایندگان و تأییدکننده مشخص را دارد. به‌علاوه، کلید خصوصی یکی از نمایندگان را نیز در اختیار دارد.
- **نوع IV (A_{IV})**: مهاجم A_{IV}، کلیدهای عمومی صاحب امضاء، نمایندگان و تأییدکننده مشخص را دارد. به‌علاوه، t-1 نفر از نمایندگان را تحت کنترل دارد و یا به عبارت دقیق‌تر، کلیدهای خصوصی آنان را می‌داند.

اگر طرح ارائه‌شده در مقابل مهاجمان نوع II و نوع III امن باشد، قطعاً در مقابل مهاجم نوع I نیز امن خواهد بود. همچنین، واضح است که مهاجم نوع IV، حالت قوی‌تری از مهاجم نوع III است و در نتیجه، اگر طرح در مقابل مهاجم نوع IV امن باشد؛ در مقابل مهاجم نوع III نیز امن خواهد بود.

غیرقابل جعل بودن در مقابل مهاجم A_{II}

غیرقابل جعل بودن در مقابل مهاجم نوع II، به این معنی است که صاحب امضاء نباید قادر باشد به جای نمایندگانش، روی متنی مثل M^* و با گواهینامه ω^*، امضای معتبری را صورت دهد. این مطلب، در بازی زیر که بین مهاجم نوع II و چالش‌گر C است، تعریف می‌شود.

برپایی: C، این الگوریتم را اجرا کرده و پارامترهای سیستم را به‌دست می‌آورد و نیز با اجرای الگوریتم تولید کلید، می‌تواند کلید کلید عمومی/خصوصی صاحب امضاء (آلیس)، تأییدکننده مشخص (سیندی) و نمایندگان زیر را به دست آورد:

$$(sk_i, pk_i) i = 1, \cdots, n \quad \text{و} \quad (sk_c, pk_c), (sk_a, pk_a)$$

پس C مقادیر sk_a, pk_a, pk_c, pk_i را برای مهاجم A_{II} ارسال می‌کند.

پرسمان‌های[1] امضای وکالتی: A_{II} می‌تواند امضای وکالتی را روی متن M و تحت گواهینامه ω درخواست کند. C الگوریتم تولید امضای وکالتی را برای به‌دست آوردن امضای وکالتی σ_p اجرا کرده و آن را به مهاجم A_{II} می‌دهد.

پرسمان‌های تأیید امضای وکالتی: مهاجم A_{II}، یک تأیید امضاء روی (M, ω, σ_P) را درخواست می‌کند. اگر σ_p معتبر باشد، C خروجی $\top$ و اگر σ_p معتبر نباشد، C خروجی $\perp$ را می‌دهد.

خروجی: در نهایت، A_{II} یک امضای σ_P^* با مجوز ω^* و یک متن M^* را به عنوان خروجی می‌دهد که:

- به‌عنوان یکی از پرسمان‌های امضای وکالتی، درخواست نشده باشد.
- (M^*, ω^*) تحت گواهینامه ω^*، یک امضای معتبر روی متن M^* باشد.

امتیاز یک مهاجم A_{II} در بازی بالا، به‌صورت زیر تعریف می‌شود:

$$\mathrm{Adv}_{\mathcal{A}_{II}} = \Pr[\mathcal{A}_{II} \text{ succeeds}]$$

تعریف۴: یک مهاجم A_{II} یک $(\epsilon, t, q_{PS}, q_v)$ – جعل‌کننده امضای وکالتی به تأییدکننده مشخص گفته می‌شود اگر A_{II} در بازی بالا: دارای امتیاز حداقل ε باشد، عملیات را حداکثر در زمان t انجام دهد و از پرسمان‌های امضای وکالتی، حداکثر q_{ps} و از پرسمان‌های تأیید امضاء، حداکثر q_v پرسمان نماید.

غیرقابل جعل بودن در مقابل مهاجم A_{II}

مشابه مهاجم قبل، بازی زیر که بین مهاجم نوع IV و چالش‌گر C است، تعریف می‌شود. این بازی شبیه حالت II است، با این تفاوت که در این حالت، به‌جای یک نماینده، t-1 نماینده شرکت دارند.

برپایی: C، این الگوریتم را اجرا کرده و پارامترهای سیستم را به دست می‌آورد و نیز با اجرای الگوریتم تولید کلید، می‌تواند کلید عمومی/خصوصی صاحب‌امضاء (آلیس)، تأییدکننده مشخص (سیندی) و نمایندگان $(sk_c, pk_c), (sk_a, pk_a)$ و $(sk_i, pk_i) i = 1, \cdots, n$ را به‌دست آورد. سپس C، مقادیر t-1، ...، i=1، pk_i، pk_c، pk_a، sk_i، را برای A_{IV} ارسال می‌کند. توجه شود که شبیه‌ساز باید نمایندگان تحت کنترل مهاجم را حدس زده و حدس او باید درست باشد؛ در غیر این‌صورت، بازی متوقف خواهد شد.

پرسمان‌های وکالت: A_{IV}، سهم وکالتی t-1 نماینده تحت کنترل خود را روی ω درخواست می‌کند. C، الگوریتم تولید وکالت را اجرا کرده و سهم وکالت نمایندگان $\sigma_{\omega_{P_i}}, i = 1, \cdots, t-1$ را به‌دست آورده و سپس آن را به مهاجم ارسال می‌کند.

پرسمان‌های امضای وکالتی: A_{IV}، می‌تواند امضای وکالتی انفرادی نمایندگان تحت کنترل خود را روی متن M درخواست کند. C، الگوریتم تولید امضای وکالتی را برای به‌دست آوردن امضاهای انفرادی و امضای وکالتی σ_p اجرا کرده و آنها را به مهاجم A_{IV} می‌دهد.

پرسمان‌های تأیید امضاء: مهاجم A_{IV}، یک تأیید امضاء روی (M, ω, σ_P) را درخواست می‌کند. اگر σ_p معتبر باشد، Cخروجی $\top$ و اگر σ_p معتبر نباشد، C خروجی $\perp$ را می‌دهد.

خروجی: در نهایت، A_{IV} یک امضای σ_P^*با مجوز ω^* و یک متن M^* را به‌عنوان خروجی می‌دهد که:

- ω^* در پرسمان‌های وکالت درخواست نشده باشد.
- (M^*, ω^*) به‌عنوان یکی از پرسمان‌های امضای وکالتی، درخواست نشده باشد.
- σ_P^* تحت گواهینامه ω^*، یک امضای معتبر روی متن M^* باشد. اکنون امتیاز یک مهاجم A_{IV} در بازی بالا، به‌صورت زیر تعریف می‌شود:

$$\mathrm{Adv}_{\mathcal{A}_{IV}} = \Pr[\mathcal{A}_{IV} \text{ succeeds}]$$

1. Query

تعریف۵: مهاجم A_{IV} یک $(\epsilon, t, q_\omega, q_{PS}, q_v)$ - جعل‌کننده امضای وکالتی با ابطال سریع گفته می‌شود اگر A_{IV} در بازی بالا: دارای امتیاز حداقل ε باشد، عملیات را حداکثر در زمان t انجام دهد، از پرسمان‌های وکالت حداکثر q_ω، از پرسمان‌های امضای وکالتی حداکثر q_{PS} و از پرسمان‌های تأیید امضاء حداکثر q_v پرسمان نماید.

۳.۳. ملزومات امنیتی

- **قابل تأیید بودن**: فرد تأییدکننده، باید از توافق صاحب امضاء روی متن امضاءشده اطمینان حاصل نماید.
- **قابل تشخیص بودن قوی**: یک فرد، باید بتواند هویت نمایندگان متناظر را از روی یک امضای وکالتی معتبر تعیین کند.
- **غیرقابل انکار بودن قوی**: گروه نمایندگان نباید با تولید امضاء قادر باشند تا خودشان را به جای صاحب امضاء معرفی نمایند. این ویژگی، برخی از اوقات تحت عنوان "انکارناپذیری[1]" به‌کار می‌رود.
- **جلوگیری از سوءاستفاده**: یک کلید امضای وکالتی، نباید بتواند برای اهدافی غیر از تولید امضای وکالتی معتبر استفاده شود. در حالت سوءاستفاده، مسئولیت نمایندگان امضاءکننده باید به‌طور آشکار تعیین شود.

۴. طرح DVTPS ارائه‌شده در مدل استاندارد

در این بخش، طرح ارائه‌شده توصیف می‌شود. در طرح ذکرشده، سه نوع شرکت‌کننده وجود دارند: صاحب امضاء که با آلیس نشان داده می‌شود، گروه نمایندگی $A = \{P_1, P_2, \cdots, P_n\}$ و تأییدکننده مشخص که با سیندی نشان داده خواهد شد. در ادامه، تمامی متن‌هایی که قرار است امضاء شوند، به‌صورت رشته بیت‌هایی با طول n نمایش داده می‌شود.

ممکن است سوال شود که اگر متن‌های ورودی همگی از طول n بیت باشند؛ پس عملاً برای متن‌های با طول بیت بیشتر، چه می‌توان کرد؟ لذا، برای انعطاف‌پذیرتر شدن طرح، می‌توان از یک تابع چکیده‌ساز مقاوم در برابر تصادم مثل $H: \{0,1\}^* \to \{0,1\}^n$ در ابتدای طرح استفاده کرد. به این نحو که قبل از اینکه متن با طول دلخواه (مثلاً بیشتر از n بیت) امضاء شود، به یک تابع چکیده‌ساز با طول خروجی n اعمال شده و خروجی تابع چکیده‌ساز، به‌عنوان ورودی طرح ارائه‌شده استفاده می‌شود. طرح ارائه‌شده، دارای الگوریتم‌های زیر است:

تولید کلید: آلیس، زوج کلید خصوصی خود را به‌صورت $sk_a = (x_a, y_a) \in \mathbb{Z}_p^2$ قرار می‌دهد و زوج کلید عمومی متناظر را به صورت $pk_a = (g^{x_a}, g^{y_a})$ محاسبه می‌نماید. هر نماینده $P_i \in A, i = 1,2,\cdots,n$ نیز به‌طور مشابه، زوج کلید خصوصی و عمومی خود را به‌ترتیب $sk_i = (x_i, y_i) \in \mathbb{Z}_p^2$ و $pk_i = (g^{x_i}, g^{y_i})$ قرارمی‌دهد. زوج کلید خصوصی و عمومی تأییدکننده مشخص (سیندی) نیز به‌ترتیب $sk_c = (x_c, y_c) \in \mathbb{Z}_p^2$ و $pk_c = (g^{x_c}, g^{y_c})$ خواهد بود.

تولید وکالت: ω_j، به عنوان j-اُمین بیت ω در نظر گرفته می‌شود که ω، گواهینامه‌ای است که از طرف صاحب امضاء صادر می‌شود و نیز، $\mathcal{W} \subseteq \{1,2,\cdots,n\}$ مجموعه jها برای $\omega_j = 1$ است. آلیس (صاحب امضاء)، مقادیر $r_{a_i} \in_R \mathbb{Z}_p, i = 1,\cdots,n$ را به طور تصادفی انتخاب کرده و گواهی نماینده P_i را به‌صورت زیر محاسبه و علاوه بر آن، R_{ai} را نیز منتشر می‌کند.

$$\sigma_{\omega_{P_i}} = e\left(\sigma_{\omega_{P_{i_1}}}, \sigma_{\omega_{P_{i_2}}}\right) = e\left(g^{x_a y_a}\left(u'\prod_{j\in\mathcal{W}} u_j\right)^{r_{a_i}}, pk_{ix}\right)$$

$$R_{a_i} = g^{r_{a_i}} \qquad (۱)$$

سپس، $(\omega, R_{a_i}, \sigma_{\omega_{P_i}})$ آلیس را برای هر نماینده P_i می‌فرستد که $i = 1,2,\cdots,n$؛ در ضمن، صاحب امضاء پارامتر $\sigma_{\omega_{P_{i_1}}}$ را منتشر می‌نماید. در رابطه (۱)، منظور از pk_{ix}، بخش اول از کلید خصوصی نماینده P_i یعنی g^{x_i} می‌باشد.

تأیید وکالت: برای تأیید صحت سهم دریافتی $(\omega, R_{a_i}, \sigma_{\omega_{P_i}})$ هر نماینده P_i، بررسی می‌کند که آیا معادله زیر برقرار است یا نه؟

$$\sigma_{\omega_{P_i}} = e(g^{x_a}, g^{y_a})^{x_i} \cdot e\left(u'\prod_{j\in\mathcal{W}} u_j, R_{a_i}\right)^{x_i} \qquad (۲)$$

تولید امضای وکالتی: فرض کنید متن M به طول n- بیت و M_j نشان‌دهنده j-اُمین بیت M است که $M_j = 1$ و نیز $\mathcal{M} \subseteq \{1,2,\cdots,n\}$، مجموعه jها برای $M_j = 1$ است.

- تولید امضای انفرادی: هر نماینده، اعداد تصادفی $r'_{a_i}, r_{b_i} \in_R \mathbb{Z}_p$ را انتخاب کرده و عبارات $R'_{a_i} = g^{r'_{a_i}}$ و $R_{b_i} = g^{r_{b_i}}$

1. Non-Repudiation

را محاسبه و منتشر می‌کند. در نهایت، هر نماینده P_i امضای انفرادی خود را به‌صورت زیر تولید می‌نماید:

$$\sigma_{i_1} = \left(\sigma_{\omega_{P_{i_1}}} \left(u' \prod_{j\in\mathcal{W}} u_j\right)^{r'_{a_i}} g^{x_i y_i} \left(m' \prod_{j\in\mathcal{M}} m_j\right)^{r_{b_i}}\right) \qquad (۳)$$

$$\sigma_{i_2} = R_{a_i} g^{r'_{a_i}} = R_{a_i} R'_{a_i} \qquad \sigma_{i_3} = g^{r_{b_i}} = R_{b_i}$$

هر نماینده P_i امضای انفرادی خود $\sigma_i = (\sigma_{i_1}, \sigma_{i_2}, \sigma_{i_3})$ را به منشی ارسال می‌کند. توجه شود که منشی می‌تواند یکی از نمایندگان یا فردی غیر از آنها باشد. منشی نیز از طریق بررسی رابطه زیر، از اعتبار امضاهای انفرادی اطمینان حاصل می‌نماید:

$$e(\sigma_{i_1}, g) \qquad (۴)$$
$$= e(pk_{ax}, pk_{ay}) e\left(u' \prod_{j\in\mathcal{W}} u_j, R_{a_i} R'_{a_i}\right) e(pk_{ix}, pk_{iy}) e\left(m' \prod_{j\in\mathcal{M}} m_j, R_{b_i}\right)$$

- تولید امضای نهایی: منشی پس از کسب اطمینان از اعتبار امضاهای انفرادی نمایندگان، امضای نهایی را به‌صورت زیر تولید می‌نماید:

$$\sigma_{P_1} = \prod_{i=1}^{t} e(\sigma_{i_1}, pk_{cx}) \;, \sigma_2 = \sum_{i=1}^{t} R_{a_i} R'_{a_i} = R_a \;, \sigma_3 = \sum_{i=1}^{t} R_{b_i} = R_b, \sigma_3 = \sum_{i=1}^{t} R_{b_i} = R_b \qquad (۵)$$

در نهایت، سه‌تایی $\sigma_P = (\sigma_{P_1}, \sigma_{P_2}, \sigma_{P_3})$ به‌عنوان امضای نهایی خواهد بود و برای گیرنده مشخص (سیندی) ارسال خواهد شد.

تأیید امضای وکالتی: تأییدکننده مشخص یا همان سیندی، از طریق کنترل رابطه زیر، تأیید می‌کند که آیا امضای وکالتی زیر روی متن معتبر است یا نه: $\sigma_P = (\sigma_{P_1}, \sigma_{P_2}, \sigma_{P_3})$

$$\sigma_{P_1} \qquad (۶)$$
$$= e(pk_{ax}, pk_{ay})^{x_c} e(pk_{txy}, g)^{x_c} . e\left(u' \prod_{j\in\mathcal{W}} u_j, \sigma_{P_2}\right)^{x_c} e\left(m' \prod_{j\in\mathcal{M}} m_j, \sigma_{P_3}\right)^{x_c}$$

توجه شودکه در رابطه بالا، از یکی از خصوصیات زوج‌سازی‌های دوخطی استفاده شده که این خاصیت در زیر آمده است:

$$\prod_{i=1}^{t} e(P_i, Q) = e\left(\prod_{i=1}^{t} P_i, Q\right)$$

همچنین، در روابط بالا، کلید عمومی گروهی به‌صورت رابطه $pk_{txy} = \prod_{i=1}^{t} g^{x_i y_i}$ است که هر نماینده امضاءکننده در مرحله تولید امضای انفرادی خود، از آن استفاده کرده است $g^{x_i y_i}$ و بنابراین، به‌صورت عمومی است.

شبیه‌سازی رونوشت: سیندی می‌تواند با استفاده از کلید خصوصی خود، روی یک متن دلخواه، M^* تحت گواهینامه ω^* تولید نماید. او دو عدد تصادفی $r_1, r_2 \in \mathbb{Z}_p^*$ را انتخاب کرده و $\sigma_P^* = (\sigma_{P_1}^*, \sigma_{P_2}^*, \sigma_{P_3}^*)$ را محاسبه می‌کند که $\sigma_{P_2}^* = g^{r_1}$ و $\sigma_{P_3}^* = g^{r_2}$ است.

$$\sigma_{P_1}^* \qquad (۷)$$
$$= e(pk_{ax}, pk_{ay})^{x_c} e(pk_{txy}, g)^{x_c} . e\left(u' \prod_{j\in\mathcal{W}} u_j, \sigma_{P_2}^*\right)^{x_c} e\left(m' \prod_{j\in\mathcal{M}} m_j, \sigma_{P_3}^*\right)^{x_c}$$

۵. تحلیل طرح ارائه‌شده

۱.۵.غیرقابل جعل بودن

غیرقابل جعل بودن در مقابل مهاجم نوع II

قضیه ۱. اگر یک مهاجم A_{IV} وجود داشته باشد که بتواند با $(\epsilon, t, q_{PS}, q_v)$ طرح ارائه‌شده را بشکند، آن‌گاه، الگوریتم دیگری به نام B وجود دارد که می‌تواند مهاجم A_{IV} را برای حل یک نمونه از مسئله GBDH در (G, G_T) با احتمال $Succ_B^{GBDH} \geq \frac{\epsilon}{8(n+1)q_{PS}}$ و در زمان

$$t' \leq \big((2n+6)q_{PS} + nq_v + 2\big)t_1 + (5q_v)t_2 + (3n + 12q_{PS} + q_v + 5)T_1 + (3q_v)T_2 + (q_{PS} + 4q_v)t_e$$

به‌کار گیرد؛ که t_1 , t_2 به ترتیب زمان لازم برای محاسبه یک ضرب در گروه‌های G و G_T می‌باشد. همچنین T_1 و T_2 به‌ترتیب زمان لازم برای محاسبه یک رابطه نمایی در گروه‌های G , G_T و t_B زمان لازم برای محاسبه یک زوج‌سازی در (G, G_T) است.

اثبات. برای اثبات قضیه۱، لطفاً به‌مرجع [۱۷] رجوع نمایید.

غیرقابل جعل بودن در برابر مهاجم IV

قضیه ۲. اگر یک مهاجم A_{IV} وجود داشته باشد که بتواند با $(\epsilon, t, q_\omega, q_{PS}, q_v)$ طرح ارائه‌شده را بشکند، آن‌گاه، الگوریتم دیگری به نام B وجود دارد که می‌تواند مهاجم A_{IV} را برای حل یک نمونه از مسئله GDBH در (G, G_T) با احتمال

$$Succ_B^{GBDH} \geq \frac{(t-1)!\,(n-t+1)!\,\epsilon}{3(n+1)^3 n! \left(3(q_\omega + q_{ps})\right)^{q_v+2}}$$

و در زمان

$$t' \le \big((2n+6)q_{PS} + (n+4)q_v + (n+4)q_\omega\big)t_1 + (3q_v)t_2 + (8q_\omega + 12q_{PS} + 4q_v)T_1 + (4q_v)T_2 + (q_{PS} + 6q_v)t_e$$

به‌کار گیرد؛ t_2, t_1 که به ترتیب زمان لازم برای محاسبه یک ضرب در گروه‌های T_2, T_1, G_T, G می‌باشد به ترتیب زمان لازم برای محاسبه یک رابطه نمایی در گروه‌های G_T, G و t_B زمان لازم برای محاسبه یک زوج‌سازی در (G, G_T) است.

اثبات. فرض کنید که شبیه‌ساز B ، یک نمونه از مسئله GBDH را به‌صورت (g, g^a, g^b, g^c) از یک گروه دوخطی (G, G_T) که از مرتبه اول P می‌باشد، دریافت می‌کند. هدف او این است که $e(g,g)^{abc}$ را با کمک O_{DBDH} یا همان پیشگوی DBDH به دست آورد. B مهاجم A_{IV} را راه‌اندازی کرده و خود نیز نقش چالش‌گر را برای مهاجم ایفا می‌کند. B، پرسمان‌های A_{IV} را به طریق زیر پاسخ می‌دهد:

برپایی: B، دو عدد صحیح l_a و l_b نیز دو عدد صحیح دیگر k_a و k_b را به‌طور تصادفی و دارای توزیع یکنواخت در $[0, n]$ انتخاب می‌نماید. سپس B، دو مقدار x'_a, x'_b و دو بردار n-تایی را طبق رابطه $\vec{x}_b = (x_{bi}), \vec{x}_a = (x_{ai})$ به طور تصادفی انتخاب می‌کند که $x'_b, x_{bi} \in \mathbb{Z}_{l_b}$ و $x'_a, x_{ai} \in \mathbb{Z}_{l_a}$

به‌علاوه، دو مقدار y'_a, y'_b و دو بردار n-تایی $y_a = (y_{ai})$ و $\vec{y}_b = (y_{bi})$ را به‌طور تصادفی انتخاب می‌کند که طبق $y'_a, y'_b, y_{ai}, y_{bi} \in \mathbb{Z}_p$ همه این مقادیر، توسط B به صورت داخلی نگه داشته می‌شود.

برای یک متن M و یک گواهی ω، $\mathcal{M} \subset \{1,2,\cdots,n\}$ و $\mathcal{W} \subset \{1,2,\cdots,n\}$ مجموعه‌ای از تمامی‌های i در نظر گرفته می‌شود که $\omega_i = 1$ و $M_i = 1$ برای راحتی تحلیل، شش تابع F_a (ω)، J_a(ω)، K_a(ω)، F_b(M)، J_b(M) و K_b(M) درست به همان صورتی که در طرح واترز بیان شده است، تعریف می‌شود[۱۵].

$$(1) F_a(\omega) = (p - l_a k_a) + x'_a + \sum_{i\in\mathcal{W}} x_{ai}, J_a(\omega) = y'_a + \sum_{i\in\mathcal{W}} y_{ai}$$

$$K_a(\omega) = \begin{cases} 0 & if\ x'_a + \sum_{i\in\mathcal{W}} x_{ai} = 0\ (mod\ l_a) \\ 1 & Otherwise. \end{cases} \quad (۸)$$

$$(2) F_b(M) = (p - l_b k_b) + x'_b + \sum_{i\in\mathcal{M}} x_{bi}, J_b(M) = y'_b + \sum_{i\in\mathcal{W}} y_{bi}$$

$$K_b(M) = \begin{cases} 0 & if\ x'_b + \sum_{i\in\mathcal{M}} x_{bi} = 0\ (mod\ l_b) \\ 1 & Otherwise. \end{cases}$$

در گام بعد، شبیه‌ساز B پارامترهای زیر را تولید می‌کند.

- B، زوج کلید عمومی صاحب امضاء را به‌صورت $(pk_{ax}, pk_{ay}) = (g^a, g^b)$ و کلید عمومی تأییدکننده مشخص را به‌صورت $pk_{cx} = g^c$ اختصاص می‌دهد که ورودی‌های مسئله GDBH هستند g^a, g^b, g^c.
- B، اعداد تصادفی $x_i, y_i \in Z_p^*, i = 1,2,\cdots,t-1$ را انتخاب کرده و زوج کلید عمومی t-1 نماینده را به‌صورت زیر اختصاص می‌دهد. $(pk_{ix}, pk_{iy}) = (g^{x_i}, g^{y_i})$

توجه شود که شبیه‌ساز باید حدس بزند که نماینده تحت کنترل مهاجم، چه کسانی هستند. اگر شبیه‌ساز درست حدس بزند، بازی ادامه می‌یابد و در غیر این صورت، بازی متوقف می‌شود. احتمال حدس درست شبیه‌ساز برای t-1 نماینده تحت کنترل مهاجم، برابر است با:

$$\frac{1}{\binom{n}{t-1}} = \frac{(t-1)!\ (n-t+1)!}{n!}$$

- B، عبارات $u' = pk_{ay}^{p-l_a k_a + x'_a} g^{y'_a}$ ، $u_i = pk_{ay}^{x_{ai}} g^{y_{ai}}$ و $\vec{u} = (u_1, u_2, \cdots, u)$ را قرار می‌دهد.
- B، عبارات $m' = pk_{ay}^{p-l_b k_b + x'_b} g^{y'_b}$، $m_i = pk_{ay}^{x_{bi}} g^{y_{bi}}$ و $\vec{m} = (m_1, m_2, \cdots, m_n)$ را قرار می‌دهد.

توجه شود که:

$$m' \prod_{i\in\mathcal{M}} m_i = pk_{ay}^{F_b(M)} g^{J_b(M)}, u' \prod_{i\in\mathcal{W}} u_i = pk_{ay}^{F_a(\omega)} g^{J_a(\omega)}$$

در نهایت، B چندتایی‌های $(G, G_T, e, p, g, u', \vec{u}, m', \vec{m})$ و $(pk_{ax}, pk_{ay}, pk_{ix}, pk_{iy}, pk_{cx}, x_i, y_i)$ را به مهاجم A_{IV} می‌دهد.

در اینجا لازم به ذکر است که بدون از دست دادن کلیت مسئله، فرض می‌شود که t-1 نماینده تحت کنترل مهاجم، همگی عیناً در تولید امضای وکالتی نقش دارند و یا به‌عبارت بهتر، جزء نماینده امضاءکننده می‌باشند.

تولید وکالت: شامل مراحل زیر است:

- اگر $K_a(\omega) = 0$ باشد، شبیه‌ساز B، بازی را متوقف و از ادامه آن انصراف می‌دهد.
- اگر $K_a(\omega) \neq 0$ باشد، این بدین معنی است که $F_a(\omega) \neq 0\ (mod\ p)$ است؛ در این حالت، برای تولید وکالت برای تک‌تک نمایندگان، شبیه‌ساز B، عدد تصادفی

$r_{a_i} \in \mathbb{Z}_p^*$ را انتخاب و سهم وکالتی نماینده i-اُم را به صورت زیر محاسبه می‌کند:

$$\sigma_{\omega_{P_i}} = e\left(pk_{ax}^{-\frac{J_a(\omega)}{F_a(\omega)}}\left(u'\prod_{j\in\mathcal{W}}u_j\right)^{r_{a_i}}, pk_{ix}\right), R_{a_i} = g^{r_{a_i}}$$

پرسمان‌های تولید امضای وکالتی: در حین این مرحله، مهاجم A_{IV} می‌تواند امضای انفرادی نمایندگان تحت کنترل خود (t-1 نماینده) را به اضافه امضای نهایی پرسمان کند.

- اگر $K_a(\omega) = 0, K_b(M) = 0$ باشد، شبیه‌ساز B، از بازی انصراف می‌دهد.
- اگر $K_a(\omega) = 0, K_b(M) \neq 0$ باشد، شبیه‌ساز B، با انتخاب عدد تصادفی $r_{a_i}, r_{b_i} \in \mathbb{Z}_p^*$ را انتخاب و سهم وکالتی نماینده i-اُم را به صورت زیر تولید می‌کند:

$$\sigma_{i_1} = pk_{ax}^{-\frac{J_b(M)}{F_b(M)}}\left(u'\prod_{j\in\mathcal{W}}u_j\right)^{r_{a_i}} g^{x_i y_i}\left(m'\prod_{j\in\mathcal{M}}m_j\right)^{r_{b_i}}$$

$$\sigma_{i_2} = g^{r_{a_i}} = R_{a_i}, \sigma_{i_3} = g^{r_{b_i} - \frac{a}{F_b(M)}} = g^{\hat{r}_{b_i}}$$

که در آن، $\hat{r}_{b_i} = r_{b_i} - \frac{a}{F_b(M)}$ است.

- توجه شودکه در مرحله شبیه‌سازی امضا، باید $K_a(\omega) = 0$ برقرار باشد. اگر $K_a(\omega) \neq 0$ بود، شبیه‌ساز باید به مرحله شبیه‌سازی وکالت برگشته و مجدداً مراحل را طوری اجرا نماید که شرط مذکور برآورده شود.

پرسمان‌های تأیید امضای وکالتی: فرض کنید که مهاجم A_{IV}، یک پرسمان تأیید برای متن و امضای روی آن یعنی رابطه $(M, \omega, \sigma_{P_1}, \sigma_{P_2}, \sigma_{P_3})$ صادر می‌کند.

- اگر $F_a(\omega) \neq 0$ و $F_b(M) \neq 0$ باشد، B روند شبیه‌سازی را متوقف می‌کند.
- اگر $F_a(\omega) = 0$ و $F_b(M) = 0$ باشد، B چندتایی

$$\left(g, g^a, g^b, g^c, \frac{\sigma_{P_1}}{e(\prod_{i=1}^t g^{x_i y_i}, g)^c e\left(g^c, \sigma_{P_2}\right)^{J_a(\omega)} e\left(g^c, \sigma_{P_3}\right)^{J_b(M)}}\right) \quad (۱۱)$$

را به پیشگوی DBDH یعنی O_{DBDH} می‌دهد. اگر خروجی O_{DBDH} برابر ۱ باشد، B، خروجی "معتبر بودن" را می‌دهد و در غیر این‌صورت، خروجی "عدم اعتبار" را می‌دهد.

- اگر $F_a(\omega) = 0$ و $F_b(M) \neq 0$ باشد، B می‌تواند یک امضای وکالتی معتبر را تحت گواهی ω روی متن M را محاسبه و به‌جای پاسخ پرسمان‌های امضای وکالتی استفاده نماید. فرض کنید که $(M, \omega, \sigma'_{P_1}, \sigma'_{P_2}, \sigma'_{P_3})$ امضایی باشد که توسط B محاسبه شده است؛ سپس B چندتایی

$$\left((g^b)^{F_b(M)} g^{J_b(M)}, \frac{\sigma_{P_3}}{\sigma'_{P_3}}, g^c, \left(\frac{\sigma_{P_1}}{\sigma'_{P_1}}\right) e\left(g^c, \frac{\sigma'_{P_2}}{\sigma_{P_2}}\right)^{J_b(M)}\right) \quad (۱۲)$$

را به پیشگوی DBDH یعنی O_{DBDH} می‌دهد. اگر خروجی O_{DBDH} برابر ۱ باشد، B خروجی "معتبر بودن" را می‌دهد و در غیر این صورت، خروجی "عدم اعتبار" را می‌دهد.

اگر $F_a(\omega) \neq 0$ و $F_b(M) = 0$ باشد، مشابه حالت قبل، B می‌تواند یک امضای وکالتی معتبر را تحت گواهی ω روی متن M را محاسبه و به‌جای پاسخ پرسمان‌های امضای وکالتی استفاده نماید. فرض کنید که، $(M, \omega, \sigma'_{P_1}, \sigma'_{P_2}, \sigma'_{P_3})$ امضایی باشد که توسط B محاسبه شده است؛ سپس B چندتایی

$$\left((g^b)^{F_a(\omega)} g^{J_a(\omega)}, \frac{\sigma_{P_2}}{\sigma'_{P_2}}, g^c, \left(\frac{\sigma_{P_1}}{\sigma'_{P_1}}\right) e\left(g^c, \frac{\sigma'_{P_3}}{\sigma_{P_3}}\right)^{J_b(M)}\right) \quad (۱۳)$$

را به پیشگوی DBDH یعنی O_{DBDH} می‌دهد. اگر خروجی O_{DBDH} برابر ۱ باشد، B، خروجی "معتبر بودن" را می‌دهد و در غیر این‌صورت، خروجی "عدم اعتبار" را می‌دهد.

اگر شبیه‌ساز B در حین شبیه‌سازی انصراف ندهد، مهاجم A_{IV} می‌تواند یک امضای وکالتی با تأییدکننده مشخص را به‌صورت $\sigma_P^* = (\sigma_{P_1}^*, \sigma_{P_2}^*, \sigma_{P_3}^*)$ روی متن M^* و تحت گواهی ω^* با احتمال موفقیت ε ارائه نماید.

- اگر $F_b(M^*) \neq 0, F_a(\omega^*) \neq 0$ باشد، شبیه‌ساز B انصراف می‌دهد.
- در غیر این صورت، $F_b(M^*) = 0, F_a(\omega^*) = 0$ و شبیه‌ساز B، رابطه زیر را محاسبه و به عنوان خروجی می‌دهد:

$$\frac{\sigma_{P_1}^*}{e(\prod_{i=1}^t g^{x_i y_i}, g)^c e\left(g^c, \sigma_{P_2}^*\right)^{J_a(\omega^*)} e\left(g^c, \sigma_{P_3}^*\right)^{J_b(M^*)}}$$

که در واقع، همان $e(g,g)^{abc}$ است که این مطلب روند شبیه‌سازی را تکمیل می‌کند. اکنون باید احتمال موفقیت B محاسبه شود.

تنها در صورتی B انصراف نمی‌دهد یا به‌عبارت بهتر، بازی را تا انتها ادامه می‌دهد که تمام شرایط زیر برقرار باشد:

G: شبیه‌ساز باید t-1 نفری را که در اختیار مهاجم می‌باشند، درست حدس بزند.

A: در حین پرسمان‌های وکالت، $K_a(\omega) \neq 0 \ (mod\ l_a)$ باشد.

B: حین پرسمان‌های امضای وکالتی، $K_a(\omega) \neq 0 \ (mod\ l_a)$ یا $K_b(M) \neq 0 \ (mod\ l_b)$ باشد.

C: در حین پرسمان‌های تأیید امضاء، $F_a(\omega) = 0 \ (mod\ p)$ یا $F_b(M) = 0 \ (mod\ p)$ باشد.

D: در فاز خروجی، $F_a(\omega^*) = 0 \ (mod\ p)$ و یا به صورت $F_b(M^*) = 0 \ (mod\ p)$ باشد.

در نهایت، احتمال موفقیت شبیه‌ساز B برابر است با .

$$Succ_{\mathcal{B}}^{GBDH} = \Pr[G \wedge A \wedge B \wedge C \wedge D]\epsilon$$

اکنون با تکنیک‌های استفاده‌شده توسط واترز، این احتمال محاسبه می‌شود [۱۵]. توجه شودکه احتمال حدس $\Pr[G]$ مستقل از بقیه احتمالات می‌باشد.

بنابراین $Succ_{\mathcal{B}}^{GBDH} \geq \frac{(t-1)!\ (n-t+1)!}{(n+1)^3 n!\ l_a^{q_v+1} l_b}\left(1 - \frac{2(q_\omega + q_{ps})}{l_a}\right)\epsilon$

می‌توان با قرار دادن $l_a = l_a = 3(q_\omega + q_{ps})$ ، به یک نتیجه ساده و بهینه دست یافت. بنابراین:

$$Succ_{\mathcal{B}}^{GBDH} \geq \frac{(t-1)!\ (n-t+1)!\ \epsilon}{3(n+1)^3 n! \left(3(q_\omega + q_{ps})\right)^{q_v+2}} \cdot \blacksquare$$

$$\Pr[G \wedge A \wedge B \wedge C \wedge D] = \Pr[G] \cdot \Pr[A \wedge B \wedge C \wedge D] = \frac{(t-1)!\ (n-t+1)!}{n!} \cdot \Pr[A \wedge B \wedge C \wedge D]$$

$$\text{But } \Pr[A \wedge B \wedge C \wedge D] = \Pr\left[\bigcap_{i=1}^{q_\omega} K_a(\omega_i) \neq 0 \bigcap_{i=1}^{q_{ps}} \left(K_a(\omega_i) \neq 0 \bigcup K_b(M_i) \neq 0\right)\right.$$

$$\left.\bigcap_{i=1}^{q_v} \left(F_a(\omega_i) = 0 (mod\ p) \bigcup F_b(M) = 0 (mod\ p)\right) \bigcap \left(F_a(\omega^*) = 0 (mod\ p) \bigcap F_b(M^*) = 0 (mod\ p)\right)\right]$$

$$\geq \Pr\left[\bigcap_{i=1}^{q_\omega + q_{ps}} K_a(\omega_i) \neq 0 \bigcap_{i=1}^{q_v} F_a(\omega_i) = 0 (mod\ p) \bigcap F_a(\omega^*) = 0 (mod\ p) \bigcap F_b(M^*) = 0 (mod\ p)\right]$$

$$= \Pr\left[\bigcap_{i=1}^{q_\omega + q_{ps}} K_a(\omega_i) \neq 0\right] \Pr\left[\bigcap_{i=1}^{q_v} F_a(\omega_i) = 0 (mod\ p) \bigcap F_a(\omega^*) = 0 (mod\ p) \bigcap F_b(M^*) = 0 (mod\ p) \mid \bigcap_{i=1}^{q_\omega + q_{ps}} K_a(\omega_i) \neq 0\right]$$

$$\geq \frac{1}{(n+1)^3}\left(1 - \frac{q_\omega + q_{ps}}{l_a}\right) \Pr\left[\bigcap_{i=1}^{q_v} K_a(\omega_i) = 0 \bigcap K_a(\omega^*) = 0 \bigcap K_b(M^*) = 0 \mid \bigcap_{i=1}^{q_\omega + q_{ps}} K_a(\omega_i) \neq 0\right]$$

$$= \frac{1}{(n+1)^3}\left(1 - \frac{q_\omega + q_{ps}}{l_a}\right) \frac{\Pr\left[\bigcap_{i=1}^{q_v} K_a(\omega_i) = 0 \cap K_a(\omega^*) = 0 \cap K_b(M^*) = 0\right]}{\Pr\left[\bigcap_{i=1}^{q_\omega + q_{ps}} K_a(\omega_i) \neq 0\right]}$$

$$\Pr\left[\bigcap_{i=1}^{q_\omega + q_{ps}} K_a(\omega_i) \neq 0 \mid \bigcap_{i=1}^{q_v} K_a(\omega_i) = 0 \bigcap K_a(\omega^*) = 0 \bigcap K_b(M^*) = 0\right]$$

$$\geq \frac{1}{(n+1)^3 l_a^{q_v+1} l_b}\left(1 - \frac{q_\omega + q_{ps}}{l_a}\right) \times \left(1 - \Pr\left[\bigcup_{i=1}^{q_\omega + q_{ps}} K_a(\omega_i) \neq 0 \mid \bigcap_{i=1}^{q_v} K_a(\omega_i) = 0 \bigcap K_a(\omega^*) = 0 \bigcap K_b(M^*) = 0\right]\right)$$

$$\geq \frac{1}{(n+1)^3 l_a^{q_v+1} l_b}\left(1 - \frac{q_\omega + q_{ps}}{l_a}\right)^2 \geq \frac{1}{(n+1)^3 l_a^{q_v+1} l_b}\left(1 - \frac{2(q_\omega + q_{ps})}{l_a}\right)$$

۲.۵. ملزومات امنیتی دیگر

غیرقابل جعل بودن، در زیربخش(۱.۵) بحث شد و در اینجا، نیز سایر ملزومات امنیتی مورد ارزیابی قرار می‌گیرد.

- **قابل تأیید بودن**: در طرح ارائه‌شده، چون کلید عمومی صاحب امضاء برای تأیید امضاء مورد نیاز است، بنابراین تأییدکننده مشخص می‌تواند از توافق صاحب امضاء روی متن امضاء شده اطمینان حاصل نماید.
- **غیرقابل انکار بودن**: به‌خاطر سختی مسئله لگاریتم گسسته (DLP)، هیچ فردی نمی‌تواند کلید خصوصی نمایندگان را بیابد. درنتیجه، تنها هر نماینده کلید خصوصی خود را می‌داند. بنابراین، زمانی که نمایندگان یک امضای وکالتی معتبر تولید می‌نمایند، نمی‌توانند خود را به‌جای دیگران معرفی و متعاقباً سوءاستفاده نمایند؛ چرا که آنها در تولید امضاء باید از کلیدهای خصوصی خود استفاده نمایند.
- **قابل شناسائی بودن**: در طرح ارائه‌شده، شناسه‌های نمایندگان امضاءکننده، هم در گواهینامه ω و هم در یک امضای وکالتی معتبر به‌طور مجزا و در قالب کلید عمومی آنان ظاهر می‌شود. بنابراین، هر فردی می‌تواند هویت نمایندگان امضاءکننده را از روی امضای تولیدشده توسط آن‌ها، شناسائی کرده و با کمک گواهینامه ω، این مطلب را تأیید نماید.
- **جلوگیری از سوءاستفاده**: تنها نمایندگان مجاز می‌توانند یک امضای وکالتی معتبر خلق نمایند؛ چرا که فقط آن‌ها از کلید خصوصی خود اطلاع دارند. بنابراین، اگر نمایندگان سهم‌های وکالتی خود را برای اهداف دیگری استفاده کنند، مسئولیت این امر با خود آنها است. از طرف دیگر، احتمال سوءاستفاده صاحب امضاء نیز منتفی است؛ چرا که او قادر نیست امضاهای انفرادی نمایندگان را خلق نماید و دلیل این امر آن است که صاحب امضاء، کلید خصوصی نمایندگان خود را نمی‌داند.

۶. نتیجه‌گیری

امروزه، طرح‌های امضاهای وکالتی در مدل استاندارد (طرح‌های بدون توابع چکیده‌ساز) بسیار مورد توجه قرار گرفته‌اند، در حالی که توجه چندانی به طرح‌های امضای وکالتی آستانه در این مدل نشده است. این در حالی است که امضاهای وکالتی آستانه، دارای کاربردهای فراوانی می‌باشند و وجود اثبات امنیتی یک طرح می تواند تضمین بهتری برای امنیت آن باشد. در این مقاله، اولین طرح امضای وکالتی آستانه به‌همراه تعریف انواع مهاجمان بالقوه آن در مدل استاندارد ارائه شد. طرح ارائه‌شده در مدل استاندارد، بر اساس فرض GDHP دارای امنیت قابل اثبات بوده و دیگر ملزومات امنیتی یک طرح امضای وکالتی آستانه را نیز برآورده می‌سازد.

۷. مراجع

[1] M. Mambo, K. Usuda, E. Okamoto, "Proxy signature: Delegation of the power to sign messages", IEICE Transactions on Fundamentals, E79-A 9 (1996), pp. 1338–1353.

[2] J. Y. Lee, J.H. Cheon, S. Kim, "An analysis of proxy signatures: Is a secure channel necessary? ", in: CT-RSA 2003, in: LNCS, vol. 2612, Springer-Verlag, Berlin, 2003, pp. 68–79.

[3] B. Lee, H. Kim, K. Kim, "Secure mobile agent using strong nondesignated proxy signature", in: ACISP01, in: LNCS, vol. 2119, Springer-Verlag, Berlin, 2001, pp. 474–486.

[4] S. J. Kim, S. J. Park, D. H. Won, "Proxy Signatures, revisited." ICICS'97, LNCS 1334, Springer-Verlag, 1997, pp. 223-232.

[5] K. Zhang, "Threshold proxy signature schemes," Information Security Workshop, Japan, 1997, pp. 191-197.

[6] J. Hu & J. Zhang, "Cryptanalysis & improvement of a threshold proxy signature scheme", Computer Standards & Interfaces, 2009, pp.169–173.

[7] Z. Tan, "Improvement on C.-L Hsu et al's threshold proxy signature scheme with known signers", international Conference on ConvergenceInformation Technology, 2007, pp. 1463–1467.

[8] F. kong, J. Yu, B. Qin, M. Li, D. Li, "Security Analysis and Improvement of a (t,n) Threshold Proxy Signature Scheme" 8th ACIS International Conference on Engineering, Artificial Intelligent, Networking and Parallel\Distributed Computing, 2007, pp. 923–926.

[9] S. H. Seo, K. A. Shim, S. H. Lee. "A mediated proxy signature scheme with fast revocation for electronic transactions". Proceedings of the 2nd International Conference on Trust, Privacy and Security in Digital Business, Aug 22-26, 2005, Copenhagen, Denmark. LNCS 3592.Berlin, German: Springer-Verlag, 2005,pp. 216–225.

[10] M. Bellare, P. Rogaway, Random Oracles are Practical: "A Paradigm for Designing Efficient Protocols", Proceeding of the First ACM Conference on Computer and Communications Security, 1993, pp. 62–73.

[11] Boldyreva, A. Palacio and B. Warinschi, "SecureProxy Signature Schemes for Delegation of Signing Rights", http://eprint.iacr.org/2003/096.

[12] Gu, Y. Zhu, "Provable Security of ID-Based Proxy Signature Schemes", ICCNMC 2005, LNCS 3619, Springer-Verlag Heidelberg, 2005, pp. 1277–1286.

[13] H. Ji, W. Han, L. Zhao and Y. Wang, "AnIdentity-Based Proxy Signature from Bilinear Pairings", WASE International Conference on Information Engineering, 2009, pp. 14–17.

[14] D. Boneh, X. Boyen, "Efficient selective-id secure identity based encryption without random oracles", In Proceeding of the International Conference on Advances in Cryptology (EUROCRYPT'04), Lecture Notes in Computer Science. Springer-Verlag, 2004.

[15] B. Waters. "Efficient identity based encryption without random oracles". Proceedings of Advances in Cryptology-Eurocrypt 2005, May 22–26, 2005, Aarhus, Denmark. LNCS 3494. Berlin, German: Springer-Verlag, 2005, pp. 114–127.

[16] X. Huang, W. Susilo, Y. Mu and W.Wu, "Proxy Signature without Random Oracles", in: MSN 2006, in: LNCS, vol. 4325, Springer-Verlag, Berlin, 2006, pp. 473–484.

[17] Y. Yu, C. Xu, X. Zhang, Y. Liao, "Designated verifier proxy signature scheme without random oracles", computers and Mathematics with Applications 57 (2009), pp.1352 –136