

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

محمد بهشتی آتسگاه<sup>۱\*</sup>، محمود گردشی<sup>۲</sup>، محمدرضا عارف<sup>۳</sup>

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: ۹۲/۴/۱۹، 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-هیلمن دوخطی گپ GDBH استوار است.

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

### ۱. مقدمه

صاحب اصلی امضاء، 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 امضای وکالتی آستانه در تجارت الکترونیک، شبکه‌های اقتضایی و در آژانس‌های سیار<sup>۳</sup> کاربرد دارند.

مفهوم امضای وکالتی، اولین بار در سال ۱۹۹۶ توسط مامبو<sup>۱</sup> 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<sup>۲</sup> به‌طور مستقل و به‌ترتیب، اولین طرح‌های امضای وکالتی آستانه بر اساس امضاهای وکالتی و طرح‌های تسهیم راز را مطرح نمودند [۴ و 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

3. Mobile agents

1. Mambo  
2. Kim and Zhang (et al.)

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

در بخش ۵، طرح ارائه شده 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  $e: G \times G \rightarrow G_T$  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.  
$$e(g^a, g^b) = e(g, g)^{ab}$$
- زوال ناپذیری:  $e(P, P) \neq 1_{G_T}$
- محاسبه پذیری: به ازای همه  $g, h \in G$  یک الگوریتم کارآمد برای محاسبه  $e(g, h)$  وجود دارد.

### ۲.۲. فرض‌های پیچیدگی

- **تعریف ۱** (مسئله دیفی-هلمن دوخطی محاسباتی یا CBDH): به ازای پارامترهای  $a, b, c \in \mathbb{Z}_p$  نامعلوم، مقادیر  $(g, g^a, g^b, g^c \in G)$  معلوم هستند و هدف، یافتن مقدار است.
  - **تعریف ۲** (مسئله دیفی-هلمن دوخطی تصمیمی یا DBDH): به ازای 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 به عنوان ورودی می‌گیرد و خروجی آن ۱ است، اگر  $w = e(g, g)^{abc}$  و در غیر این صورت، خروجی آن صفر است.

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 شناسایی بودن و جلوگیری از سوء استفاده.

اگرچه بسیاری از طرح‌های ارائه شده ادعا می‌کردند که تمامی ویژگی‌های بالا را برآورده می‌سازند، لیکن مفهوم امنیت آنها روشن و واضح نبود. اولین بار، بلیر و رگاوی<sup>۴</sup> مفهوم اثبات رسمی<sup>۵</sup> در مدل سروش تصادفی<sup>۶</sup> را برای پروتکل‌های توافق کلید ارائه کردند [۱۰]. پس از آنها، بولدیروا<sup>۷</sup> 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<sup>۸</sup> و اثبات امنیتی در این مدل نیز اولین بار توسط بونه و بوین<sup>۹</sup> برای یک طرح رمزنگاری مبتنی بر شناسه، ارائه شد که مدل ارائه شده آنها، مدل ID انتخابی<sup>۱۰</sup> بود [۱۴]. سپس، واترز<sup>۱۱</sup> 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 استاندارد<sup>۸</sup> که واترز ارائه نمود، کامل‌تر و کارآمدتر از مدل قبلی بود. هوآنگ<sup>۱۲</sup> 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<sup>۱۳</sup> 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. علاوه بر آن، نشان داده می‌شود که امنیت طرح ارائه شده، 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<sup>۱۴</sup> DVTPS بیان و طرح جدید در بخش ۴ ارائه می‌شود.

10. Selective-ID model  
11. Waters  
12. Huang  
13. Yu et al.  
14. Designated Verifier Threshold Proxy Signature Scheme  
15. Oracle

4. Bellare & Rogaway  
5. Formal proof  
6. Random oracle  
7. Boldyreva  
8. Standard model  
9. Boneh & Boyen

$sk_i (i = 1, 2, \dots, t)$  سهم‌های وکالتی آنان،  
 $\sigma_{\omega p_i} (i = 1, 2, \dots, t)$  کلید عمومی تأییدکننده مشخص  
 $pk_c$  و متن مورد نظر  $m$  را برای تولید امضای وکالتی  $\sigma_p$   
 دریافت می‌کند.

• **تأیید امضای وکالتی:** یک الگوریتم معین که یک متن  $m$ ،  
 گواهینامه  $\omega$ ، 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  $\perp$  را می‌دهد، و در غیر این صورت (اگر امضاء  
 معتبر نباشد)، خروجی  $\perp$  را می‌دهد.

• **شبیه‌سازی رونوشت:** این الگوریتم پارامترهای متن  $m$ ،  
 گواهینامه  $\omega$  و کلید خصوصی تأییدکننده مشخص  $sk_c$  را  
 به‌عنوان ورودی گرفته و یک رونوشت با توزیع دقیقاً یکسان  
 $\sigma_p^*$  را به‌گونه‌ای تولید می‌نماید که از امضای وکالتی اصلی  $\sigma_p$ ،  
 تمایزناپذیر است.

### ۲.۲. مدل امنیتی

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

- **نوع I (A<sub>I</sub>):** مهاجم A<sub>I</sub>، تنها کلیدهای عمومی صاحب امضاء،  
 نمایندگان و تأییدکننده مشخص را دارد.
- **نوع II (A<sub>II</sub>):** مهاجم A<sub>II</sub>، کلیدهای عمومی صاحب امضاء،  
 نمایندگان و تأییدکننده مشخص را دارد. به‌علاوه، کلید  
 خصوصی صاحب امضاء (آلیس) را نیز در اختیار دارد.
- **نوع III (A<sub>III</sub>):** مهاجم A<sub>III</sub> کلیدهای عمومی صاحب امضاء،  
 نمایندگان و تأییدکننده مشخص را دارد. به‌علاوه، کلید  
 خصوصی یکی از نمایندگان را نیز در اختیار دارد.
- **نوع IV (A<sub>IV</sub>):** مهاجم A<sub>IV</sub>، 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.

• **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:

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

### 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  
 $A = \{P_1, P_2, \dots, P_n\}$  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  
 $i \in \{a, \{1, 2, \dots, n\}, c\}$  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  $\omega$  (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 می-  
 دهد که  $i = 1, 2, \dots, n$

• **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،

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، به جای 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 صاحب امضاء (آلیس)، تأییدکننده مشخص (سیندی) و نمایندگان  $(sk_i, pk_i), i=1, \dots, n$  و  $(sk_c, pk_c), (sk_a, pk_a)$  را به دست آورد. سپس C، مقادیر  $t-1, \dots, t$  را برای  $sk_i, pk_a, pk_c, pk_i$  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 این صورت، بازی متوقف خواهد شد.

**پرسمان‌های وکالت:**  $A_{IV}$ ، سهم وکالتی  $t-1$  نماینده تحت کنترل خود را روی  $\omega$  درخواست می‌کند. C، الگوریتم تولید وکالت را اجرا کرده و سهم وکالت نمایندگان  $t-1, \dots, t$  را  $\sigma_{\omega p_i}$  به دست 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 به دست آوردن امضای انفرادی و امضای وکالتی  $\sigma_p$  اجرا کرده و آنها را به مهاجم  $A_{IV}$  می‌دهد.

**پرسمان‌های تأیید امضاء:** مهاجم  $A_{IV}$ ، یک تأیید امضاء روی  $(M, \omega, \sigma_p)$  را درخواست می‌کند. اگر  $\sigma_p$  معتبر باشد، خروجی  $T$  و اگر  $\sigma_p$  معتبر نباشد، خروجی  $\perp$  را می‌دهد.

**خروجی:** در نهایت،  $A_{IV}$  یک امضای  $\sigma_p^*$  با مجوز  $\omega^*$  و یک متن  $M^*$  را به عنوان خروجی می‌دهد که:

- $\omega^*$  در پرسمان‌های وکالت درخواست نشده باشد.
- $(M^*, \omega^*)$  به عنوان یکی از پرسمان‌های امضای وکالتی، درخواست نشده باشد.
- $\sigma_p^*$  تحت گواهینامه  $\omega^*$  یک امضای معتبر روی متن  $M^*$  باشد. اکنون امتیاز یک مهاجم  $A_{IV}$  در بازی بالا، به صورت زیر تعریف می‌شود:

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

### 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  $\omega^*$  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 به دست می‌آورد و نیز با اجرای الگوریتم تولید کلید، می‌تواند کلید عمومی/خصوصی صاحب امضاء (آلیس)، تأییدکننده مشخص (سیندی) و نمایندگان زیر را به دست آورد:

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

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

**پرسمان‌های امضای وکالتی:**  $A_{II}$  می‌تواند امضای وکالتی را روی متن  $M$  و تحت گواهینامه  $\omega$  درخواست کند. C الگوریتم تولید امضای وکالتی را برای به دست آوردن امضای وکالتی  $\sigma_p$  اجرا کرده و آن را به مهاجم  $A_{II}$  می‌دهد.

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

**خروجی:** در نهایت،  $A_{II}$  یک امضای  $\sigma_p^*$  با مجوز  $\omega^*$  و یک متن  $M^*$  را به عنوان خروجی می‌دهد که:

- به عنوان یکی از پرسمان‌های امضای وکالتی، درخواست نشده باشد.
- $(M^*, \omega^*)$  تحت گواهینامه  $\omega^*$ ، یک امضای معتبر روی متن  $M^*$  باشد.

امتیاز یک مهاجم  $A_{II}$  در بازی بالا، به صورت زیر تعریف می‌شود:

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

**تعریف ۴:** یک مهاجم  $A_{II}$  یک  $(\epsilon, t, q_{ps}, q_v)$  - جعل کننده امضای وکالتی به تأییدکننده مشخص گفته می‌شود اگر  $A_{II}$  در بازی بالا: دارای امتیاز حداقل  $\epsilon$  باشد، عملیات را حداکثر در زمان  $t$  انجام دهد و از پرسمان‌های امضای وکالتی، حداکثر  $q_{ps}$  و از پرسمان‌های

ورودی طرح ارائه شده استفاده می شود. طرح ارائه شده، دارای الگوریتم های زیر است:

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

**تولید وکالت:**  $\omega_j$ ، به عنوان ز-آمین بیت  $\omega$  در نظر گرفته می شود که  $\omega$ ، گواهی نامه ای است که از طرف صاحب امضاء صادر می شود و نیز،  $\mathcal{W} \subseteq \{1, 2, \dots, n\}$  مجموعه  $\mathcal{W}$ ها برای  $\omega_j = 1$  است. آلیس (صاحب امضاء)، مقادیر  $r_{a_i} \in \mathbb{Z}_p, i = 1, \dots, n$  را به طور تصادفی انتخاب کرده و گواهی نماینده  $P_i$  را به صورت زیر محاسبه و علاوه بر آن،  $R_{a_i}$  را نیز منتشر می کند.

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

$$R_{a_i} = g^{r_{a_i}} \quad (1)$$

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

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

$$\sigma_{\omega P_i} = e(g^{x_a}, g^{y_a})^{x_i} \cdot e\left(u' \prod_{j \in \mathcal{W}} u_j, R_{a_i}\right)^{x_i} \quad (2)$$

**تولید امضای وکالتی:** فرض کنید متن  $M$  به طول  $n$ -بیت و  $M_j$  نشان دهنده ز-آمین بیت  $M$  است که  $M_j = 1$  و نیز  $\mathcal{M} \subseteq \{1, 2, \dots, n\}$ ، مجموعه  $\mathcal{M}$ ها برای  $M_j = 1$  است.

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

**تعریف ۵:** مهاجم  $A_{IV}$  یک  $(\epsilon, t, q_{\omega}, q_{PS}, q_v)$  - جعل کننده امضای وکالتی با ابطال سریع گفته می شود اگر  $A_{IV}$  در بازی بالا: دارای امتیاز حداقل  $\epsilon$  باشد، عملیات را حداکثر در زمان  $t$  انجام دهد، از پرسمان های وکالت حداکثر  $q_{\omega}$  از پرسمان های امضای وکالتی حداکثر  $q_{PS}$  و از پرسمان های تأیید امضاء حداکثر  $q_v$  پرسمان نماید.

### ۳.۳. ملزومات امنیتی

- **قابل تأیید بودن:** فرد تأییدکننده، باید از توافق صاحب امضاء روی متن امضاء شده اطمینان حاصل نماید.
- **قابل تشخیص بودن قوی:** یک فرد، باید بتواند هویت نمایندگان متناظر را از روی یک امضای وکالتی معتبر تعیین کند.
- **غیر قابل 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" به کار می رود.
- **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 به طور آشکار تعیین شود.

### ۴. طرح DVTPS ارائه شده در مدل استاندارد

در این بخش، طرح ارائه شده توصیف می شود. در طرح ذکر شده، سه نوع شرکت کننده وجود دارند: صاحب امضاء که با آلیس نشان داده می شود، گروه نمایندگی  $A = \{P_1, P_2, \dots, P_n\}$  و تأییدکننده مشخص که با سیندی نشان داده خواهد شد. در ادامه، تمامی متن هایی که قرار است امضاء شوند، به صورت رشته بیت هایی با طول  $n$  نمایش داده می شود.

ممکن است سوال شود که اگر متن های ورودی همگی از طول  $n$  بیت باشند؛ پس عملاً برای متن های با طول بیت بیشتر، چه می توان کرد؟ لذا، برای انعطاف پذیرتر شدن طرح، می توان از یک تابع چکیده ساز مقاوم در برابر تصادم مثل  $H: \{0, 1\}^* \rightarrow \{0, 1\}^n$  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 چکیده ساز با طول خروجی  $n$  اعمال شده و خروجی تابع چکیده ساز، به عنوان

امضای انفرادی خود، از آن استفاده کرده است  $g^{x_i y_i}$  و بنابراین، به صورت عمومی است.

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

$$\sigma_{P_1}^* = e(pk_{ax}, pk_{ay})^{x_c} e(pk_{txy}, g)^{x_c} \cdot e\left(u \prod_{j \in W} u_j, \sigma_{P_2}^*\right)^{x_c} e\left(m \prod_{j \in M} m_j, \sigma_{P_3}^*\right)^{x_c} \quad (7)$$

### ۵. تحلیل طرح ارائه شده

#### 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 ارائه شده 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  $\frac{\epsilon}{8(n+1)q_{PS}}$

و در زمان

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

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  $T_2$  به ترتیب 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 قضیه ۱، لطفاً به مرجع [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 ارائه شده 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

$$Succ_B^{GDBH} \geq \frac{(t-1)!(n-t+1)!\epsilon}{3(n+1)^3 n! (3(q_\omega + q_{PS}))^{q_V + 2}}$$

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

$$\sigma_{i_1} = \left( \sigma_{\omega P_{i_1}} \left( u \prod_{j \in W} u_j \right)^{r_{a_i}} g^{x_i y_i} \left( m \prod_{j \in M} m_j \right)^{r_{b_i}} \right) \quad (3)$$

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

هر نماینده  $P_i$  امضای انفرادی خود  $(\sigma_{i_1}, \sigma_{i_2}, \sigma_{i_3})$  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 امضای انفرادی اطمینان حاصل می‌نماید:

$$e(\sigma_{i_1}, g) = e(pk_{ax}, pk_{ay}) e\left(u \prod_{j \in W} u_j, R_{a_i} R'_{a_i}\right) e(pk_{ix}, pk_{iy}) e\left(m \prod_{j \in M} m_j, R_{b_i}\right) \quad (4)$$

• تولید امضای نهایی: منشی پس از کسب اطمینان از اعتبار امضای انفرادی نمایندگان، امضای نهایی را به صورت زیر تولید می‌نماید:

$$\sigma_{P_1} = \prod_{i=1}^t e(\sigma_{i_1}, pk_{cx}), \sigma_2 = \sum_{i=1}^t R_{a_i} R'_{a_i} = R_a, \sigma_3 = \sum_{i=1}^t R_{b_i} = R_b, \sigma_3 = \sum_{i=1}^t R_{b_i} = R_b \quad (5)$$

در نهایت، سه تایی  $\sigma_P = (\sigma_{P_1}, \sigma_{P_2}, \sigma_{P_3})$  به عنوان امضای نهایی خواهد بود و برای گیرنده مشخص (سیدی) ارسال خواهد شد.

**تأیید امضای و کالتی:** تأییدکننده مشخص یا همان سیدی، از طریق کنترل رابطه زیر، تأیید می‌کند که آیا امضای و کالتی زیر روی متن معتبر است یا نه:

$$\sigma_{P_1} = e(pk_{ax}, pk_{ay})^{x_c} e(pk_{txy}, g)^{x_c} \cdot e\left(u \prod_{j \in W} u_j, \sigma_{P_2}\right)^{x_c} e\left(m \prod_{j \in M} m_j, \sigma_{P_3}\right)^{x_c} \quad (6)$$

توجه شود که در رابطه بالا، از یکی از خصوصیات زوج‌سازی‌های دوطرفه 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 به صورت رابطه  $pk_{txy} = \prod_{i=1}^t g^{x_i y_i}$  است که هر نماینده امضاءکننده در مرحله تولید

و در زمان

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

- B زوج کلید عمومی صاحب امضاء را به صورت  $(pk_{ax}, pk_{ay}) = (g^a, g^b)$  و کلید عمومی تأییدکننده مشخص را به صورت  $pk_{cx} = g^c$  اختصاص می‌دهد که  $g^a, g^b, g^c$  ورودی‌های مسئله GDBH هستند.

- B اعداد تصادفی  $x_i, y_i \in \mathbb{Z}_p^*, i = 1, 2, \dots, t-1$  را انتخاب کرده و زوج کلید عمومی t-1 نماینده را به صورت 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  $u_i = pk_{ay}^{x_{ai}} g^{y_{ai}}, u' = pk_{ay}^{p-l_a k_a + x'_a} g^{y'_a}$  و  $\vec{u} = (u_1, u_2, \dots, u)$  را قرار می‌دهد.

- B عبارات  $m_i = pk_{ay}^{x_{bi}} g^{y_{bi}}, m' = pk_{ay}^{p-l_b k_b + x'_b} g^{y'_b}$  و  $\vec{m} = (m_1, m_2, \dots, m_n)$  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 به عبارت 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  $F_a(\omega) \neq 0 \pmod{p}$  است؛ در این حالت، برای تولید وکالت برای تک‌تک نمایندگان، شبیه‌ساز B عدد تصادفی

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

به کار گیرد؛  $t_1, t_2$  که به ترتیب زمان لازم برای محاسبه یک ضرب در گروه‌های  $G, T_1, T_2, G_T$  می‌باشد به ترتیب 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.** فرض کنید که شبیه‌ساز B، یک نمونه از مسئله GBDH را به صورت  $(g, g^a, g^b, g^c)$  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 ODBDH 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 به طور 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  $x'_a, x_{ai} \in \mathbb{Z}_{l_a}$

به علاوه، دو مقدار  $y'_a, y'_b$  و دو بردار n-تایی  $y_a = (y_{ai})$  و  $y_b = (y_{bi})$  را به طور 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  $\omega$ ،  $\mathcal{M} \subset \{1, 2, \dots, n\}$  و  $\mathcal{W} \subset \{1, 2, \dots, n\}$  مجموعه‌ای از تمامی‌های i در نظر گرفته می‌شود که  $\omega_i = 1$  و  $M_i = 1$  برای راحتی تحلیل، شش تابع  $F_a, F_b, J_b(M), J_a(\omega), K_b(M), K_a(\omega)$  که در طرح وایترز بیان شده است، تعریف می‌شود [۱۵].

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

$$K_a(\omega) = \begin{cases} 0 & \text{if } x'_a + \sum_{i \in \mathcal{W}} x_{ai} = 0 \pmod{l_a} \\ 1 & \text{Otherwise.} \end{cases} \quad (8)$$

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

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

را به پیشگوی DBDH یعنی ODBDH می‌دهد. اگر خروجی ODBDH برابر ۱ باشد، B، خروجی "معتبر بودن" را می‌دهد و در غیر این- صورت، 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  $\omega$  روی متن M را محاسبه و به جای 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

$$\left( (g^b)^{F_b(M)} g^{J_b(M)}, \frac{\sigma_{P_3}}{\sigma'_{P_3}}, g^c, \left( \frac{\sigma_{P_1}}{\sigma'_{P_1}} \right) e \left( g^c, \frac{\sigma'_{P_2}}{\sigma_{P_2}} \right)^{J_b(M)} \right) \quad (12)$$

را به پیشگوی DBDH یعنی ODBDH می‌دهد. اگر خروجی ODBDH 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  $\omega$  روی متن M را محاسبه و به جای 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

$$\left( (g^b)^{F_a(\omega)} g^{J_a(\omega)}, \frac{\sigma_{P_2}}{\sigma'_{P_2}}, g^c, \left( \frac{\sigma_{P_1}}{\sigma'_{P_1}} \right) e \left( g^c, \frac{\sigma'_{P_3}}{\sigma_{P_3}} \right)^{J_b(M)} \right) \quad (13)$$

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

اگر شبیه‌ساز B در حین شبیه‌سازی انصراف ندهد، مهاجم  $A_{IV}$  می‌تواند یک امضای وکالتی با تأییدکننده مشخص را به صورت  $\sigma_P^* = (\sigma_{P_1}^*, \sigma_{P_2}^*, \sigma_{P_3}^*)$  روی متن  $M^*$  و تحت گواهی  $\omega^*$  با احتمال موفقیت  $\epsilon$  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:

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

$r_{a_i} \in \mathbb{Z}_p^*$  را انتخاب و سهم وکالتی نماینده  $i$ -ام 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  $i$ -ام 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 شود که 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  $F_b(M) = 0$  و  $F_a(\omega) = 0$  باشد، B چندتایی

$$\left( g, g^a, g^b, g^c, \frac{\sigma_{P_1}}{e(\prod_{i=1}^t g^{x_i y_i}, g)^c e(g^c, \sigma_{P_2})^{J_a(\omega)} e(g^c, \sigma_{P_3})^{J_b(M)}} \right) \quad (11)$$



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

در نهایت، احتمال موفقیت شبیه‌ساز B برابر است با .

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 به عبارت 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،  $K_a(\omega) \neq 0 \pmod{l_a}$  باشد.

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

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

مدل استاندارد ارائه شد. طرح ارائه شده 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.

## 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.

## ۷. مراجع

- **قابل تأیید بودن:** در طرح ارائه شده، 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:** به خاطر سختی مسئله لگاریتم گسسته (DLP)، هیچ فردی نمی‌تواند کلید خصوصی نمایندگان را بیابد. در نتیجه، تنها هر نماینده کلید خصوصی خود را می‌داند. بنابراین، زمانی که نمایندگان یک امضای وکالتی معتبر تولید می‌نمایند، نمی‌توانند خود را به جای دیگران معرفی و متعاقباً سوءاستفاده نمایند؛ چرا که آنها در تولید امضاء باید از کلیدهای خصوصی خود استفاده نمایند.
  - **قابل شناسائی بودن:** در طرح ارائه شده، شناسه‌های نمایندگان امضاءکننده، هم در گواهینامه (w) و هم در یک امضای وکالتی معتبر به طور 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 (w)، 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. نتیجه گیری**
- 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 می‌تواند تضمین بهتری برای امنیت آن باشد. در این مقاله، اولین طرح امضای وکالتی آستانه به همراه تعریف انواع مهاجمان بالقوه آن در

- [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
- [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.

Archive of SID