

رمزگذاری مبتنی بر شناسه فازی سلسله مراتبی

سید هاتف حسینیان برزی^{۱*}، حسین ملکی^۲

۱- کارشناسی ارشد علوم کامپیوتر، دانشگاه شهید بهشتی تهران ۲- کارشناسی ارشد مهندسی کامپیوتر نرم افزار، دانشگاه صنعتی امیرکبیر تهران

(دریافت: ۹۶/۰۵/۰۶، پذیرش: ۹۶/۱۲/۲۶)

چکیده

در یک طرح رمزگذاری مبتنی بر شناسه فازی، یک کاربر با کلید خصوصی شناسه ID در صورتی می تواند متن رمز شده با شناسه ID' را رمزگشایی نماید، اگر و تنها ID و ID' به اندازه معینی با یکدیگر اشتراک داشته باشند. البته طرح هایی که تا به حال برای رمزگذاری مبتنی بر شناسه فازی ارائه شده است بر این فرض استوار هستند که همه ویژگی ها اهمیت یکسانی دارند. در حالی که این فرض برای بسیاری از مواقع مناسب نیست. در این مقاله به فرض رایجی در این نوع سیستم های رمزگذاری می پردازیم به طوری که ویژگی ها از اهمیت یکسانی برخوردار نیستند. در این فرض مجموعه ویژگی های ممکن در یک ساختار سلسله مراتبی قرار می گیرند به طوری که در طول فرآیند رمزگشایی، ویژگی ها در سطوح پایین تر می توانند با ویژگی های سطوح بالاتر جایگزین شوند. برای حل این مسئله، یک طرح جدید موسوم به رمزگذاری مبتنی بر شناسه فازی سلسله مراتبی معرفی شد، سپس یک تعریف صوری از امنیت و یک پیاده سازی برای آن ارائه گردید. امنیت طرح پیشنهادی در مدل امنیتی شناسه منتخب بر اساس فرض سخت بودن مسئله تصمیم گیری دوخطی اصلاح شده دیفی هلمن استوار است.

کلیدواژه ها: سلسله مراتبی، مبتنی بر شناسه فازی، رمزگذاری

۱- مقدمه

رمزنگاری مبتنی بر شناسه که اولین بار در سال ۱۹۸۴ میلادی توسط شمیر^۱ پیشنهاد شد، مدیریت گواهی در زیرساخت کلید عمومی سنتی^۲ (PKI) را به شکلی ساده حل می کند. در این سیستم ها، کلید عمومی هر کاربر، از یکی از ویژگی های منحصر به فرد (برای مثال، آدرس پست الکترونیکی یا شماره تلفن) آن به دست می آید و کلید خصوصی توسط تولیدکننده کلید خصوصی^۳ (PKG) تولید می شود. شمیر [۱] همچنین اولین طرح امضای مبتنی بر شناسه^۴ (IBS) را ارائه داد و طرح رمزگذاری آن را به عنوان یک مسئله باز مطرح نمود.

اولین طرح عملی رمزگذاری مبتنی بر شناسه^۵ (IBE) در سال

*رایانامه نویسنده مسئول: hatefbarz@gmail.com

1- Shamir
2- Traditional public key infrastructure
3- Private Key Generator
4- Identity-Based Signature
5- Identity-Based Encryption

۲۰۰۱ میلادی به وسیله بونه و فرانکلین [۲] طراحی شد. در سال ۲۰۰۵ میلادی، ساهای و واترز^۶ [۳] شرایطی را در نظر گرفتند که در آن کاربران شناسه دقیق یکدیگر را نمی دانند و ممکن است فقط به وسیله مجموعه ای از ویژگی های توصیفی شان شناخته شوند و سیستم رمزگذاری جدیدی موسوم به رمزگذاری مبتنی بر شناسه فازی^۷ ($FIBE$) را معرفی کردند. در طرح های $FIBE$ هر فرد به وسیله مجموعه ای از ویژگی های توصیفی خود که زیرمجموعه ای از ویژگی های U است، شناخته می شود. سپس، یک کاربر با کلید خصوصی وابسته به شناسه (مجموعه ای از ویژگی ها) ω قادر است متن رمزی را که با کلید عمومی شناسه ω' رمز شده است را رمزگشایی نماید اگر و تنها اگر اشتراک بین ω و ω' مقدار آستانه ای (k) باشد. به عبارت دیگر، یک کاربر با شناسه ω قادر است متن رمزی را که با شناسه ω' رمز شده است را رمزگشایی کند اگر و تنها اگر $|\omega \cap \omega'| \geq k$.

6- Sahai and Waters
7- Fuzzy Identity-Based Encryption

قادر به رمزگشایی یک پیام رمز شده با شناسه ω است اگر اشتراک بین ویژگی‌های دو شناسه ω و ω' در هر سطح حداقل به اندازه کافی (k_i) باشد، به عبارت دیگر

$$|\cup_{j=0}^i \omega_j \cap \cup_{j=0}^i \omega'_j| \geq k_i$$

این مفهوم می‌تواند همچنین پاسخگوی مسئله باز مطرح شده به وسیله ساهای و واترز [۳] باشد که در مورد طرح *FIBE* با تفاوت فاصله متریک شناسه‌ها است.

کاربرد: در یک شبکه اجتماعی، فردی می‌خواهد دسترسی به اطلاعات شخصی خود را براساس یک ساختار سلسله‌مراتبی از علایق خود محدود کند. او می‌خواهد مطمئن شود که فقط افراد خاصی از "جنس مخالف" قادر به رمزگشایی پروفایلش هستند. همچنین، برای او ویژگی‌هایی از قبیل "درآمد بالا" یا "مدرک دانشگاهی" دارای اهمیت بیشتری نسبت به مشخصات ظاهری ("رنگ چشم" یا "قد" یا ...) است به طوری که می‌توانند جایگزین آن‌ها شوند. به همین منظور، او ویژگی‌های مدنظر خود را به مجموعه‌های {"جنس مخالف" $U_0 = \{$ "درآمد بالا" و "مدرک دانشگاهی" $\}$ و $U_1 = \{$ "چشمان سبز" و "قد بلند" $\}$ تقسیم‌بندی می‌کند، همچنین، مقادیر $k_0 = 1$ ، $k_1 = 2$ و $k_2 = 3$ را در طرح *HFIBE* مقادیر می‌کند؛ بنابراین، افراد با "جنس مخالف" که هر دو ویژگی "درآمد بالا" و "مدرک دانشگاهی" را دارند دیگر نیازی به داشتن مشخصات ظاهری موردنظر ندارند. اگرچه افراد با "جنس مخالف" که "تحصیل کرده" و با "درآمد پایین" هستند باید حداقل یکی از خصوصیات ظاهری توصیف شده را داشته باشند تا بتوانند پروفایل آن فرد را مشاهده نمایند. قابل ذکر است که این مثال را نمی‌توان با استفاده از طرح‌های *FIBE* فعلی پیاده‌سازی کرد.

به منظور تحقق این هدف، اولین طرح رمزگذاری مبتنی بر شناسه فازی سلسله‌مراتبی به همراه اثبات امنیتی آن در مدل شناسه منتخب، ارائه شده است. علاوه بر آن، نشان داده می‌شود که امنیت طرح ارائه شده براساس فرض سختی مسئله *DMBDH* استوار است.

بقیه مقاله به صورت زیر سازماندهی شده است. بخش ۲ شامل تعاریف اولیه است. در بخش ۳، شمای کلی و تعریف صوری مدل امنیت طرح *HFIBE* مطرح می‌شود. در بخش ۴، پیاده‌سازی طرح پیشنهادی ارائه و در بخش ۵، از لحاظ امنیتی تحلیل می‌شود. در بخش ۶، کارایی آن بررسی و با طرح *FIBE* ساهای و واترز مقایسه می‌شود و در بخش پایانی نتیجه‌گیری بیان خواهد شد.

از قابلیت فازی بودن علاوه بر رمزگذاری در زمینه امضاء نیز استفاده گردید که در شاخه مجزایی از طرح‌های *FIBE* موسوم به امضای مبتنی بر شناسه فازی $(FIBS)$ در حال پیشرفت است [۴].

ساهای و واترز در [۳] به دو کاربرد مهم این نوع سیستم‌ها اشاره کردند. اولین کاربرد باعث ایجاد سیستم رمزگذاری مبتنی بر شناسه زیستی [۵] و دومین کاربرد باعث ایجاد رمزگذاری مبتنی بر ویژگی [۶] شد. از زمان معرفی این نوع سیستم رمزگذاری، پیاده‌سازی‌های متفاوتی [۷-۹] نیز از طرح‌های *FIBE* ارائه شده است.

در چند سال اخیر، شکل نوینی از اینترنت با عنوان "اینترنت اشیا"^۱ به سمت فراگیر شدن پیش می‌رود که چگونگی انتقال اطلاعات به صورت امن در آن به مسئله مهمی تبدیل شده است و *FIBE* به عنوان یک کاندید برای حل این مسئله مطرح است [۱۰].

اگرچه طرح‌هایی که تا به حال ارائه شده‌اند بر این فرض استوار هستند که همه ویژگی‌ها در U در یک سطح از اهمیت قرار دارند؛ بنابراین، تصمیم‌گیری برای این که آیا یک شناسه ω می‌تواند پیام رمز شده با شناسه ω' را رمزگشایی کند یا نه، فقط تعداد ویژگی‌های مشترک بین آن‌ها (یعنی $|\omega \cap \omega'|$) اهمیت دارد. در دنیای امروزی چنین شرایطی فراگیر نیست زیرا هر فرد می‌تواند ویژگی‌هایی با سطوح اهمیت متفاوت داشته باشد. این تفاوت می‌تواند اغلب با استفاده از یک ساختار سلسله‌مراتبی توصیف شود به طوری که در فرآیند رمزگشایی، ویژگی‌ها با سطح اهمیت بالاتر می‌توانند جایگزین ویژگی‌ها با سطح اهمیت پایین‌تر شوند. برای پشتیبانی کردن از این قابلیت (ویژگی‌ها با درجه اهمیت متفاوت)، در این مقاله، مفهوم جدیدی موسوم به رمزگذاری مبتنی بر شناسه فازی سلسله‌مراتبی^۵ (*HFIBE*) را معرفی می‌کنیم. در *HFIBE*، مجموعه‌ای از ویژگی‌ها (U) را به چند زیرمجموعه سلسله‌مراتبی غیرمشترک ($U = \cup_{i=0}^m U_i$)، $U_i \cap U_j = \emptyset$ ($i \neq j$)، تقسیم می‌کنیم به طوری که ویژگی‌های موجود در سطح U_i با اهمیت‌تر از ویژگی‌های موجود در سطح U_j برای $0 \leq i < j \leq m$ هستند و می‌توانند جایگزین آن‌ها شوند. در این مفهوم، هر شناسه $\omega \subset U$ به زیرمجموعه‌های $\omega_0, \dots, \omega_m$ طوری تقسیم می‌شود که به ازای هر سطح i از 0 تا m ، $\omega_i \subset U_i$ و $\cup_{i=0}^m \omega_i = \omega$. حال یک دریافت‌کننده با شناسه ω

1- Fuzzy Identity-Based Signature

2- Biometric Identity-Based Encryption

3- Attribute Based Encryption

4- Internet of Things

5- Hierarchical Fuzzy Identity-Based Encryption

۲- تعاریف اولیه

در این بخش برخی از تعاریف اولیه شامل درون‌یابی بیرکوف^۱، نگاشت‌های دوخطی و فرض پیچیدگی که در این مقاله استفاده خواهند شد، مرور می‌شود.

۱-۲- درون‌یابی بیرکوف

ساختار دسترسی سلسله‌مراتبی در زمینه تسهیم راز^۲ به‌وسیله تاسا^۳ [۱۱] در سال ۲۰۰۵ میلادی استفاده شده است. تاسا نشان داد که چگونه از درون‌یابی بیرکوف می‌توان در پیاده‌سازی چنین ساختاری استفاده نمود. در ادامه اصطلاحات پایه‌ای از قضیه درون‌یابی بیرکوف [۱۲] آورده شده است.

تعریف ۱) مسئله درون‌یابی بیرکوف: فرض کنید مجموعه‌ای از نقاط مجزا و مثبت در \mathbb{R} باشد $X = \{x_1, \dots, x_k\}$ به‌طوری که بین آن‌ها رابطه $0 < x_1 < x_2 < \dots < x_k$ برقرار است. همچنین، ماتریس باینری با $N+1$ عنصر $E = (e_{i,j})_{1 \leq i \leq k, 0 \leq j \leq l}$ باشد، به‌عبارت دیگر $I(E) = \{(i, j) : e_{i,j} = 1\}$ باشد، $|I(E)| = N+1$ و $C = \{c_{i,j} : (i, j) \in I(E)\}$ مجموعه‌ای از $N+1$ عدد حقیقی باشد. سپس، مسئله درون‌یابی بیرکوف متناظر با سه‌تایی $\langle X, E, C \rangle$ عبارت است از تعیین چندجمله‌ای $P(x) \in R_N[x]$ که در $N+1$ شرط زیر صدق کند:

$$P^{(j)}(x_i) = c_{i,j}, (i, j) \in I(E) \quad (1)$$

که در آن، $P^{(j)}(\cdot)$ ، j امین مشتق $P(x)$ است.

برخلاف درون‌یابی لاگرانژ و هرمیت^۴ که بدون هیچ شرطی خوش وضع^۵ می‌باشند، درون‌یابی بیرکوف ممکن است دارای جواب یکتا نباشد. شروط کافی برای خوش وضع بودن درون‌یابی بیرکوف بر روی میدان‌های متناهی در [۱۱] آورده شده است. در زیر درون‌یابی بیرکوف را به‌صورت جزئی بررسی می‌کنیم:

فرض کنید $\varphi = \{g_0, g_1, \dots, g_N\}$ یک سیستم مستقل خطی از توابع حقیقی و N بار متوالی مشتق‌پذیر است و $I'(E) = \{\alpha_i : i = 1, \dots, N+1\}$ به‌وسیله یک ترتیب واژگانی^۶ از

بردار $I(E)$ به‌دست می‌آید در $I'(E)$ جفت (i, k) قبل از (i', k') قرار می‌گیرد اگر و تنها اگر $i < i'$ یا $i = i'$ و $k < k'$.

فرض کنید $\alpha_i(1)$ و $\alpha_i(2)$ به‌ترتیب عناصر اول و دوم از جفت $C' = \{c_i : i = 1, \dots, N+1\}$ را بیان می‌کنند. همچنین، برداری است که به‌وسیله یک ترتیب واژگانی بر روی اندیس عناصر C به‌دست می‌آید.

حال با استفاده از عناصر E ، X و φ می‌توانیم مسئله درون‌یابی بیرکوف را به‌صورت زیر حل نماییم:

$$P(x) = \sum_{j=0}^N \frac{|A(E, X, \Phi_j)|}{|A(E, X, \Phi)|} g_j(x) \quad (2)$$

به‌طوری‌که:

$$A(E, X, \Phi) = \begin{bmatrix} g_0^{(\alpha_1(2))}(x_{\alpha_1(1)}) & g_1^{(\alpha_1(2))}(x_{\alpha_1(1)}) & \dots & g_N^{(\alpha_1(2))}(x_{\alpha_1(1)}) \\ g_0^{(\alpha_2(2))}(x_{\alpha_2(1)}) & g_1^{(\alpha_2(2))}(x_{\alpha_2(1)}) & \dots & g_N^{(\alpha_2(2))}(x_{\alpha_2(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{(\alpha_{N+1}(2))}(x_{\alpha_{N+1}(1)}) & g_1^{(\alpha_{N+1}(2))}(x_{\alpha_{N+1}(1)}) & \dots & g_N^{(\alpha_{N+1}(2))}(x_{\alpha_{N+1}(1)}) \end{bmatrix} \quad (3)$$

عملگر درمینان است و $A(E, X, \Phi_j)$ به‌وسیله جابه‌جایی $(j+1)$ امین ستون ماتریس (۳) با C' به‌دست می‌آید.

با استفاده از معادله (۱)، معادله (۲) بسط $|A(E, X, \Phi_j)|$ بر روی $(j+1)$ امین ستون به‌صورت زیر بازنویسی می‌شود:

$$P(x) = \sum_{j=0}^N \sum_{i=0}^N (-1)^{(i+j)} c_{i+1} \frac{|A_i(E, X, \Phi_j)|}{|A(E, X, \Phi)|} g_j(x) \quad (4)$$

که در آن، $A_i(E, X, \Phi_j)$ به‌وسیله حذف سطر $(i+1)$ ام و ستون $(j+1)$ ام از ماتریس $A(E, X, \Phi_j)$ به‌دست می‌آید. به‌طور مشهود مقدار تابع در نقطه \cdot از معادله (۴) به‌صورت زیر به‌دست می‌آید:

$$P(0) = \sum_{j=0}^N \sum_{i=0}^N (-1)^{(i+j)} c_{i+1} \frac{|A_i(E, X, \Phi_j)|}{|A(E, X, \Phi)|} g_j(0) \quad (5)$$

اگر Φ را برابر $\{1, x, \dots, x^N\}$ در نظر بگیریم آن‌گاه $g_0(0) = 1$ و $g_j(0) = 0$ برای $1 \leq j \leq N$ ؛ بنابراین، مقدار تابع در نقطه \cdot را می‌توان به‌صورت زیر محاسبه نمود:

$$P(0) = \sum_{i=0}^N (-1)^{(i)} c_{i+1} \frac{|A_i(E, X, \Phi_0)|}{|A(E, X, \Phi)|} \quad (6)$$

- 1- Birkhoff Interpolation
- 2- Secret Sharing
- 3- Tassa
- 4- Lagrange And Hermite
- 5- Well Posed
- 6- Lexicographically

آماده‌سازی: این الگوریتم یک پارامتر امنیتی κ که اندازه گروه‌ها را تعیین می‌کند به‌عنوان ورودی دریافت می‌کند. این الگوریتم مجموعه‌ای از ویژگی‌های U را تعریف می‌کند و این ویژگی‌ها را به زیرمجموعه‌های سلسله‌مراتبی $U = (U_0, U_1, \dots, U_m)$ مطابق با میزان اهمیتی که در دنیای واقعی دارند، تقسیم‌بندی می‌کند. همچنین، دنباله‌ای از مقادیر آستانه‌ای $k = \langle k_0, k_1, \dots, k_m \rangle$ را تعیین می‌کند. این الگوریتم، پارامترهای عمومی سیستم $params$ و کلید مخفی msk را به‌طور تصادفی تولید می‌کند. سپس PKG ، پارامترهای عمومی سیستم $params$ را منتشر می‌کند و کلید مخفی msk را به‌عنوان راز نگه می‌دارد.

از این پس وقتی می‌گوییم اشتراک بین دو شناسه تمام مقادیر آستانه‌ای را برآورده می‌کند ($k = \langle k_0, k_1, \dots, k_m \rangle$)، منظورمان $|\bigcup_{j=0}^i ID_j \cap \bigcup_{j=0}^i ID'_j| \geq k_i$ به ازای i از ۰ تا m است. همچنین، وقتی می‌گوییم اشتراک بین دو شناسه حداقل یک مقدار آستانه‌ای را برآورده نمی‌کند ($k = \langle k_0, k_1, \dots, k_m \rangle$)، منظورمان این است که حداقل یک i از ۰ تا m وجود دارد که $|\bigcup_{j=0}^i ID_j \cap \bigcup_{j=0}^i ID'_j| < k_i$ در این جا ID_i و ID'_i نمادهایی از $ID \cap U_i$ و $ID' \cap U_i$ می‌باشند.

تولید کلید: این الگوریتم پارامترهای عمومی سیستم $params$ ، کلید مخفی msk و شناسه $ID \subset U$ را به‌عنوان ورودی دریافت می‌کند. PKG ، الگوریتم را برای تولید کلید خصوصی d_{ID} متناظر با شناسه ID اجرا می‌کند و از کانالی امن آن را به کاربر ارسال می‌کند.

رمزگذاری: ورودی‌های این الگوریتم احتمالی، پارامترهای عمومی سیستم $params$ ، پیام آشکار M و شناسه ID است. این الگوریتم یک متن رمز C را به‌عنوان خروجی تولید می‌کند.

رمزگشایی: ورودی‌های این الگوریتم قطعی، پارامترهای عمومی سیستم $params$ ، متن رمز C که با شناسه ID رمز شده و کلید خصوصی d_{ID} وابسته به شناسه ID است. اگر اشتراک شناسه‌های ID و ID' تمام مقادیر آستانه‌ای ($k = \langle k_0, k_1, \dots, k_m \rangle$) را برآورده کند، پیام M و در غیر این صورت \perp را به‌عنوان خروجی برمی‌گرداند.

۲-۲- نگاشت‌های دوخطی

فرض کنید G_1 و G_2 گروه‌های ضربی از مرتبه عدد اول p باشند. یک نگاشت دوخطی به‌صورت $e: G_1 \times G_1 \rightarrow G_2$ تعریف می‌شود و دارای خواص زیر است:

- دوخطی بودن: برای هر $g_1, g_2 \in G_1$ و $a, b \in \mathbb{Z}_p^*$ داریم $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
- ناتاباهیدگی^۱: $g_1, g_2 \in G_1$ وجود دارد به‌طوری‌که $e(g_1, g_2) \neq 1$.
- محاسبه‌پذیری: برای هر $g_1, g_2 \in G_1$ ، الگوریتم کارایی برای محاسبه $e(g_1, g_2)$ وجود دارد.

۲-۳- فرض پیچیدگی

مسئله تصمیم‌گیری دوخطی اصلاح شده دیفی هلمان^۲ ($DMBDH$): دو گروه ضربی G_1 و G_2 به‌طوری‌که مرتبه هر دو برابر عدد اول p و یک نگاشت دوخطی $e: G_1 \times G_1 \rightarrow G_2$ و یک چندتایی $(g, g^a, g^b, g^c, Z) \in G_1^4 \times G_2$ برای $a, b, c \in \mathbb{Z}_p$ داریم. مسئله $DMBDH$ در مورد این است که آیا $Z = e(g, g)^{abc}$ برقرار است یا خیر.

مزیت (احتمال برد) هر الگوریتم A با زمان چندجمله‌ای برای حل مسئله $DMBDH$ به‌صورت زیر تعریف می‌شود:

$$Adv_A^{DMBDH} = |Pr[A(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - Pr[A(g, g^a, g^b, g^c, Z) = 1]|$$

مسئله $DMBDH$ برای هر الگوریتم A با زمان چندجمله‌ای بر این فرض استوار است که مزیت (احتمال برد) Adv_A^{DMBDH} ناچیز است.

۳- تعریف و مدل امنیت رمزگذاری مبتنی بر شناسه فازی سلسله‌مراتبی

در این بخش تعریف صوری و مدل امنیتی طرح $HFIBE$ را ارائه می‌کنیم.

۳-۱- شمای کلی

یک طرح $HFIBE$ (Γ) از چهار الگوریتم آماده‌سازی، تولید کلید، رمزگذاری و رمزگشایی تشکیل شده است. در ادامه، هریک از این الگوریتم‌ها را شرح خواهیم داد.

1- Non-Degeneracy

2- Decisional Modified Bilinear Diffe-Hellman Problem

۳-۲- مدل امنیت

در این بخش مدل امنیتی که برای طرح پیشنهادی در نظر می‌گیریم براساس مدل امنیتی شناسه منتخب فازی^۱ است که ساهای و واترز [۳] برای طرح‌های *FIBE* به‌کار برده‌اند. در مدل امنیتی شناسه منتخب، مهاجم تعیین می‌کند که قبل از تولید پارامترهای عمومی سیستم به چه شناسه‌هایی می‌خواهد حمله کند. تنها تفاوت بین مدل امنیتی پیشنهادی و مدل امنیتی در طرح ساهای و واترز این است که در مدل جدید مهاجم اجازه ندارد کلید شناسه‌هایی که اشتراکشان با شناسه منتخب، تمام مقادیر آستانه‌ای را برآورده می‌کند، درخواست کند. به‌عبارت دیگر، تنها کلید شناسه‌هایی را می‌تواند درخواست کند که اشتراکشان با شناسه منتخب حداقل یکی از شرط‌های آستانه‌ای را برآورده نکند.

مدل امنیتی که برای طرح *HFIBE* در نظر گرفته می‌شود برپایه غیرقابل تشخیص بودن^۲ متن رمز شده برای اثبات محرمانگی است. بازی بین یک مهاجم (A) و یک چالشگر (G) برای اثبات امنیت یک طرح *HFIBE* (Γ) در مدل امنیتی شناسه منتخب فازی سلسله‌مراتبی به‌صورت زیر است.

$HFIBE_{A,\Gamma}^{Sel-ID}$ game

آغازگر: مهاجم شناسه‌ای ID را که قصد حمله به آن را دارد مشخص می‌کند.

آماده‌سازی: چالش‌گر الگوریتم آماده‌سازی را اجرا می‌کند و پارامترهای عمومی سیستم $params$ را برای مهاجم ارسال می‌کند. فاز ۱: مهاجم اجازه درخواست کلیدهای خصوصی به هر شناسه ID' را در صورتی دارد که اشتراک آن با شناسه ID حداقل یکی از مقادیر آستانه‌ای را برآورده نکند.

چالش: مهاجم دو پیام M_0 و M_1 با طول یکسان را به چالش‌گر ارسال می‌کند. سپس چالش‌گر بیت v را به‌طور تصادفی انتخاب می‌کند و پیام M_v را تحت شناسه ID رمز می‌کند. سپس چالش‌گر متن رمز شده را برای مهاجم ارسال می‌کند.

فاز ۲: مهاجم می‌تواند درخواست‌هایی همانند آن‌چه در فاز اول انجام‌داده را انجام دهد.

پاسخ: مهاجم مقدار بیت v' را به‌عنوان پاسخ برمی‌گرداند و در صورتی در این بازی برنده است که $v' = v$ باشد. مزیت (احتمال برد) مهاجم در این بازی به این صورت تعریف می‌شود:

$$Pr[v' = v] - \frac{1}{2}$$

تعریف ۲: یک طرح *HFIBE* در مدل امنیت شناسه منتخب فازی سلسله‌مراتبی، امن است اگر احتمال برد مهاجم در بازی بالا با زمان چندجمله‌ای مقدار ناچیزی باشد.

۴- طرح پیشنهادی

در این بخش قصد داریم تا مدل رسمی یک طرح رمزگذاری مبتنی بر شناسه فازی سلسله‌مراتبی را در مدل شناسه منتخب بیان کنیم. جزئیات طرح پیشنهادی به‌صورت زیر است:

۴-۱- آماده‌سازی

این الگوریتم توسط *PKG* انجام می‌شود.

- ورودی: پارامتر امنیت K .
 - پردازش:
 - انتخاب دو گروه دوری ضربی G_1 و G_2 ، به‌طوری‌که مرتبه‌شان برابر عدد اول p باشد.
 - انتخاب یک نگاشت دوخطی $e: G_1 \times G_1 \rightarrow G_2$.
 - تعریف مجموعه‌ای از ویژگی‌ها U (برای سادگی به تعداد $|U|$ عدد از اولین عناصر Z_p^* را به‌عنوان U در نظر می‌گیریم).
 - تقسیم تمام ویژگی‌های سیستم مطابق با میزان اهمیتشان در دنیای واقعی به زیرمجموعه‌های U_0, U_1, \dots, U_m .
 - انتخاب دنباله‌ای از مقادیر آستانه‌ای $\langle k_0, k_1, \dots, k_m \rangle$.
 - انتخاب اعداد تصادفی $t_1, t_2, \dots, t_{|U|}, y \in Z_p$ به‌عنوان کلید مخفی msk . انتخاب مولد g از گروه G_1 و محاسبه مقدار پارامترهای عمومی سیستم $params$ به‌صورت زیر:
- $$\{G_1, G_2, e, g, k_0, k_1, \dots, k_m, T_1 = g^{t_1}, \dots, T_{|U|} = g^{t_{|U|}}, Y = e(g, g)^y\}$$
- خروجی: پارامترهای عمومی سیستم $params$ که منتشر شده است و کلید مخفی msk که به‌صورت راز نگهداری شده است.

۴-۲- تولید کلید

این الگوریتم توسط PKG انجام می‌شود.

- ورودی: پارامترهای عمومی سیستم $params$ ، کلید مخفی msk و شناسه کاربر ID .

• پردازش:

۱. انتخاب یک چندجمله‌ای تصادفی $q(\cdot)$ از درجه $k_m - 1$ به طوری که $q(0) = y$.

۲. تقسیم شناسه ID به زیرمجموعه‌های ID_0, \dots, ID_m به طوری که به ازای تمام مقادیر j از $ID_j \subset Y_j$ ، m تا 0 .

۳. به ازای تمام مقادیر j از 0 تا m :

- محاسبه مقدار $D_i = g^{t_i^{(k-j-1)(i)}}$ به عنوان مؤلفه‌های کلید خصوصی برای $i \in ID_j$ (به ازای هر ویژگی i موجود در شناسه ID که در سطح j ام قرار دارد).

- خروجی: کلید خصوصی متناظر با شناسه ID یعنی $\{D_i\}_{i \in ID}$.

۴-۳- رمزگذاری

- ورودی: شناسه دریافت‌کننده ID ، پارامترهای عمومی سیستم $params$ و پیام $M \in G_2$.

• پردازش:

۱. انتخاب مقدار تصادفی $s \in Z_p$.

۲. محاسبه مقادیر $E' = M Y^s$ و $\{E_i = T_i^s\}_{i \in ID}$.

- خروجی: متن رمز $E = (ID, E', \{E_i\}_{i \in ID})$.

۴-۴- رمزگشایی

- ورودی: متن رمز $E = (ID, E', \{E_i\}_{i \in ID})$ ، پارامترهای عمومی سیستم $params$ و شناسه دریافت‌کننده ID' .

متناظر با کلید خصوصی $\{D_i\}_{i \in ID'}$.

• پردازش:

۱. اگر اشتراک شناسه ID و ID' تمام دنباله مقادیر

آستانه‌ای را برآورده کند آن‌گاه ID'' را به عنوان یک

زیرمجموعه از ID' طوری انتخاب می‌کنیم که

$|ID''| = k_m$ و اشتراک آن با ID تمام

دنباله مقادیر آستانه‌ای را برآورده کند. سپس، عبارت

زیر را محاسبه می‌کنیم:

$$M = E' / \left(\prod_{i \in ID''} (e(D_i, E_i))^{(-1)^{i_r} |A_{i_r}(E, X, \varphi_0)|} \right)^{|A(E, X, \varphi)|^{-1}} \quad (Y)$$

که در آن، i_r شماره ردیف ویژگی i در ماتریس (۳) است.

۲. در غیر این صورت $M = \perp$.

- خروجی: M .

یادآوری: طرح $FIBE$ ساهای و واترز [۳] یک مورد خاصی از طرح ارائه شده است چرا که همه ویژگی‌ها تنها در یک سطح از اهمیت قرار دارند، در نتیجه نیاز به هیچ مقدار مشتق نیست.

۴-۵- اثبات درستی

رابطه رمزگشایی (معادله (۷)) صحیح است، چرا که اگر اشتراک بین ID' و ID همه شرایط آستانه‌ای را برآورده کند، اشتراک بین ID' و ID'' نیز بنا بر تعریف همین خاصیت را دارد؛ بنابراین، کاربری با کلید خصوصی متناظر شناسه ID'' رمزگشایی را می‌تواند طبق مراحل زیر انجام دهد:

$$\begin{aligned} & E' / \left(\prod_{i \in ID''} (e(D_i, E_i))^{(-1)^{i_r} |A_{i_r}(E, X, \varphi_0)|} \right)^{|A(E, X, \varphi)|^{-1}} \\ &= Me(g, g)^{sy} / \left(\prod_{i \in ID''} (e(g^{t_i^{(k-j-1)(i)}}, g^{s t_i^{(k-j-1)(i)}}))^{(-1)^{i_r} |A_{i_r}(E, X, \varphi_0)|} \right)^{|A(E, X, \varphi)|^{-1}} \\ &= Me(g, g)^{sy} / \left(\prod_{i \in ID''} (e(g, g)^{(-1)^{i_r} s q^{(k-j-1)(i)}})^{|A_{i_r}(E, X, \varphi_0)|} \right)^{|A(E, X, \varphi)|^{-1}} \\ &= Me(g, g)^{sy} / e(g, g)^{s \cdot \left(\sum_{i \in ID''} \frac{(-1)^{i_r} q^{(k-j-1)(i) |A_{i_r}(E, X, \varphi_0)|}}{|A(E, X, \varphi)|} \right)} \\ &= Me(g, g)^{sy} / e(g, g)^{sq(0)} \\ &= Me(g, g)^{sy} / e(g, g)^{sy} \\ &= M \end{aligned}$$

۵- تحلیل امنیت

در این بخش امنیت طرح پیشنهادی در مدل شناسه منتخب که به مسئله سخت $DMBDH$ تقلیل داده شده اثبات می‌شود.

قضیه ۱: با فرض امکان ناپذیری مسئله $DMBDH$ ، طرح ارائه شده یک طرح $HFIBE$ امن تحت مدل شناسه منتخب فازی سلسله‌مراتبی است.

برهان: اجازه دهید A مهاجمی باشد که در بازی $HFIBE_{A, \Gamma}^{sel-ID}$ با احتمال ϵ پیروز می‌شود که Γ طرح پیشنهادی

- اشتراک بین U و $\alpha' \cup \{0\}$ تمام مقادیر آستانه‌ای را برآورده کند و به ازای i از 0 تا

$$m, k_i \geq |U_i \cap (\alpha' \cup \{0\})| \text{ برقرار باشد.}$$

- تعریف مقدار $S = \alpha' \cup \{0\}$,
- محاسبه مؤلفه‌های کلید خصوصی D_i برای ویژگی‌های $i \in \alpha'$ به روش زیر:
- اگر $i \in \alpha$ آن‌گاه انتخاب یک عدد تصادفی

$$D_i = g^{s_i}, s_i \in Z_p$$

- اگر $i \in \alpha' - \alpha$ آن‌گاه انتخاب یک عدد تصادفی $\lambda_i \in Z_p$ ، سپس محاسبه مقدار

$$D_i = g^{\frac{\lambda_i}{w_i}}$$

- بعد از تعریف مقادیر بالا K به‌طور ضمنی یک چندجمله‌ای $q(x)$ از درجه $k_m - 1$ با انتخاب $k_m - 1$ نقطه تصادفی به‌علاوه نقطه $q(0) = a$ تعریف می‌کند. برای $i \in \alpha$ مقدار تابع برابر $q^{(k_{j-1})}(i) = c\beta_i s_i$ و برای $i \in \alpha' - \alpha$ مقدار تابع برابر $q^{(k_{j-1})}(i) = \lambda_i$ است که j شماره سطحی است که ویژگی i در آن قرار دارد.
- چالش‌گر K به‌روش زیر مؤلفه‌های کلید خصوصی مطابق با ویژگی‌های $i \in ID' - \alpha'$ را تولید می‌کند:

$$D_i = g^{\frac{q^{(k_{j-1})}(i)}{w_i}}$$

که در آن، j شماره سطحی است که ویژگی i در آن قرار دارد.

بنابراین، طبق روش بالا چالش‌گر K توانست کلید خصوصی برای شناسه ID' را تولید کند. به‌علاوه، توزیع کلید خصوصی برای شناسه ID' مطابق با طرح اصلی است.

چالش: مهاجم A دو پیام M_0 و M_1 با طول یکسان را به چالش‌گر K می‌دهد. سپس، چالش‌گر یک بیت v را به‌طور تصادفی انتخاب می‌کند و پیام M_v را با استفاده از شناسه ID رمز می‌کند و متن رمز E را به A می‌دهد. متن رمز به‌صورت زیر است:

$$E = (ID, E' = M_v Z, \{E_i = B^{\beta_i}\}_{i \in ID})$$

است. آن‌گاه با استفاده از A ، چالش‌گر K را طوری طراحی می‌کنیم که مسئله $DMBDH$ را با احتمال ≈ 2 حل کند.

فرض کنید چالش‌گر K یک نمونه تصادفی $(g, A = g^a, B = g^b, C = g^c, Z) \in G_1^4 \times G_2$ از مسئله سخت $DMBDH$ را دریافت کرده است. فرض کنید مهاجم A با چالش‌گر K که در بازی $HFIBE_{A,\Gamma}^{Sel-ID}$ مدل شده است، تعامل دارد. در ادامه نشان خواهیم داد که چالش‌گر K چگونه با استفاده از A در طول بازی $HFIBE_{A,\Gamma}^{Sel-ID}$ می‌تواند جواب مسئله $DMBDH$ را به‌دست آورد. مدل‌سازی بازی $DMBDH$ ، برای اثبات این قضیه به‌صورت زیر است.

آغازگر: چالش‌گر K مهاجم A را اجرا و شناسه چالش ID را از مهاجم A دریافت می‌کند.

آماده‌سازی: چالش‌گر K پارامتر Y را برابر $e(g, A) = e(g, g)^a$ قرار می‌دهد. برای هر ویژگی $i \in U$ در سیستم مقادیر T_i را به‌صورت زیر مقداردهی می‌کند:

- اگر $i \in \alpha$ باشد، یک عدد تصادفی $\beta_i \in Z_p$ انتخاب می‌کند و T_i را برابر $C^{\beta_i} = g^{c\beta_i}$ قرار می‌دهد.
 - در غیر این‌صورت یک عدد تصادفی $w_i \in Z_p$ انتخاب می‌کند و T_i را برابر g^{w_i} قرار می‌دهد.
- سپس پارامترهای عمومی سیستم را به A می‌دهد.

فاز ۱: در این فاز A می‌تواند کلید خصوصی برای شناسه‌های متعدد ID' را به شرطی که اشتراک بین ID' و ID حداقل در یکی از شروط آستانه‌ای صدق نکند، درخواست کند. فرض کنید که A کلید خصوصی برای شناسه ID' را درخواست کند. چالش‌گر K کلید خصوصی شناسه ID' را مطابق مراحل زیر تولید می‌کند:

- تعریف مقدار $\alpha = ID \cap ID'$
- تعریف یک ویژگی بی‌تأثیر $0 \in U_0$
- انتخاب مقدار α' به‌طوری‌که:

$$\begin{aligned} \alpha' &\subset ID' & - \\ \alpha &\subseteq \alpha' & - \\ |\alpha'| &= k_m - 1 & - \end{aligned}$$

تعداد عملیات توان در گروه G_1 به منظور رمزگذاری برای یک شناسه، رابطه خطی با تعداد عناصر آن شناسه دارد. الگوریتم رمزگذاری به یک عملیات توان به ازای هر ویژگی شناسه نیاز دارد و هزینه رمزگشایی به محاسبه k_m نگاشت دوخطی محدود است.

تعداد عناصر گروه در پارامترهای عمومی سیستم به طور خطی با تعداد ویژگی‌های سیستم (U) افزایش می‌یابد. تعداد عناصر گروهی که در کلید خصوصی کاربر استفاده می‌شود با تعداد ویژگی‌های آن شناسه رابطه خطی دارد.

در نهایت، تعداد عناصر گروه در یک متن رمز با اندازه شناسه‌ای که برای آن رمز می‌شود رابطه خطی دارد.

در جدول (۱)، اندازه پارامترهای مختلف و هزینه محاسبه زیرالگوریتم‌ها در طرح پیشنهادی و نسخه اول ارائه شده توسط ساهای و واترز [۳] که با اختصار با SW نمایش داده می‌شود را مقایسه می‌کنیم. نماد $|G|$ نشان دهنده طول (برحسب بیت) عناصر گروه G است. در این جا مجموع تعداد ویژگی‌ها، نماد kG و kC_e برای $k > 0$ ، به ترتیب نشان دهنده k بار محاسبه بر روی G و عملگرهای زوج‌سازی است. r_1 مجموعه ویژگی‌های متن رمز و r_2 مجموعه ویژگی‌های طول کلید خصوصی است.

جدول (۱): نتایج مقایسه طرح‌های رمزگذاری مبتنی بر شناسه فازی

طرح پیشنهادی	SW	
$n G_1 + G_2 $	$n G_1 + G_2 $	طول کلید عمومی
$(n+1) Z_p $	$(n+1) Z_p $	طول کلید مخفی
$r_2 G_1 $	$r_2 G_1 $	طول کلید خصوصی
$r_1 G_1 + G_2 $	$r_1 G_1 + G_2 $	طول متن رمز
$r_1G_1 + 2G_2$	$r_1G_1 + 2G_2$	هزینه رمزگذاری
$k_m C_e + (k_m + 1)G_2$	$dC_e + (d+1)G_2$	هزینه رمزگشایی
شناسه منتخب	شناسه منتخب	مدل امنیت
بله	خیر	پشتیبانی از ویژگی‌ها با درجه اهمیت متفاوت

از جدول بالا به وضوح می‌توان برتری طرح پیشنهادی را نتیجه گرفت. طرح پیشنهادی علاوه بر پشتیبانی از ویژگی‌ها با درجه اهمیت‌های متفاوت از نظر پیچیدگی با طرح ساهای و واترز تفاوتی ندارد و از نظر امنیتی نیز در همان مدل امنیتی اثبات شده است.

فاز ۲: مهاجم می‌تواند درخواست‌هایی همانند آنچه در فاز اول انجام داده را انجام دهد و چالش‌گر K نیز به همان روش پاسخ دهد.

پاسخ: مهاجم A مقدار بیت v' را به عنوان پاسخ برمی‌گرداند. اگر $v' = v$ باشد، چالش‌گر K مقدار یک را به نشانه تساوی Z با مقدار $e(g, g)^{abc}$ برمی‌گرداند در غیر این صورت، مقدار صفر را برای نشان دادن این که Z یک عدد تصادفی در گروه G_2 است را برمی‌گرداند.

حال نشان می‌دهیم اگر مهاجم در بازی بالا با احتمال ε برنده شود، آن‌گاه چالش‌گر K می‌تواند مسئله سخت $DMBDH$ را با احتمال $\varepsilon/2$ حل نماید.

اگر Z برابر مقدار $e(g, g)^{\frac{ab}{c}}$ باشد آن‌گاه

$$E' = M_v e(g, g)^{ar'} = M_v Y^{r'}$$

$$r' = \frac{b}{c} \quad E_i = B^{\beta_i} = g^{b\beta_i} = g^{\frac{b}{c}\beta_i} = g^{r'c\beta_i} = (T_i)^{r'}$$

است؛ بنابراین، متن رمز یک رمزگذاری تصادفی از متن M_v تحت شناسه ID است. در این حالت، مزیت (احتمال برد) مهاجم بنا بر تعریف برابر ε است، یعنی $Pr[v = v'] = 1/2 + \varepsilon$.

در غیر این صورت، اگر Z برابر مقدار $e(g, g)^z$ به ازای یک عدد تصادفی $z \in Z_p$ باشد آن‌گاه $E' = M_v e(g, g)^z$. از آنجایی که z یک عدد تصادفی است، E' از دید مهاجم یک عنصر تصادفی از گروه G_2 است و شامل هیچ گونه اطلاعاتی از M_v نیست. در این حالت، مهاجم هیچ اطلاعی در مورد v به دست نمی‌آورد، در نتیجه $Pr[v = v'] = 1/2$.

بنابراین، مزیت (احتمال برد) چالش‌گر K برای حل مسئله $DMBDH$ برابر است با:

$$Adv_C^{DMBDH} = \left| Pr[C(g, g^a, g^b, g^c, e(g, g)^{abc}) | v = v'] - Pr[C(g, g^a, g^b, g^c, Z) | v = v'] \right|$$

$$= \frac{1}{2} \left(\frac{1}{2} + \varepsilon \right) - \frac{1}{2} = \frac{\varepsilon}{2}$$

۶- کارایی

در این بخش، کارایی طرح ارائه شده با توجه به طول متن رمز، طول کلید خصوصی و زمان رمزگشایی و رمزگذاری بررسی می‌شود.

۷- نتیجه‌گیری

امروزه، طرح‌های رمزگذاری مبتنی بر شناسه فازی بسیار مورد توجه قرار گرفته‌اند و دارای کاربردهای فراوانی می‌باشند. در این مقاله، مفاهیم رمزگذاری مبتنی بر شناسه فازی سلسله‌مراتبی (*HFIBE*) به‌عنوان راه‌حلی برای مسئله *FIBE* که دارای ویژگی‌ها با سطح اهمیت متفاوت است، معرفی گردید. مفهوم پیشنهادی می‌تواند به‌عنوان راه‌حل مسئله بازطرح‌شده به‌وسیله ساهای و واترز [۳] که در مورد طرح *FIBE* با تفاوت فاصله متریک شناسه‌ها پرسش شده است، مطرح شود. یک تعریف صوری برای امنیت طرح‌های *HFIBE* و یک روش پیاده‌سازی با استفاده از درون‌یابی بیرکوف ارائه شد؛ سپس، امنیت طرح پیشنهادی در مدل امنیتی شناسه منتخب سلسله‌مراتبی با فرض سخت‌بودن مسئله تصمیم‌گیری دوخطی اصلاح‌شده دیفی‌هلمان اثبات گردید.

۸- منابع

- [4] M. B. Atashgah and M. Gardeshi, "The (t,n) Threshold Proxy Signature Scheme with new known signers and Proof of security in the standard model," *Electronic and Cyber Defense Magazine*, vol. 2, no. 1, 2014. (in Persian)
- [5] N. Sarier, "A new biometric identity based encryption scheme secure against dos attacks," *Security and Communication Networks*, vol. 4, no. 1, p. 23-32, 2011.
- [6] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-Based Encryption for FineGrained Access Control of Encrypted Data," In *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89-98, 2006.
- [7] J. Baek, W. Susilo, and J. Zhou, "New Constructions of Fuzzy Identity-Based Encryption," In *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 368-370, 2007.
- [8] Y. Ren, D. Gu, S. Wang, and X. Zhang, "New Fuzzy Identity-Based Encryption in the Standard Model," *Informatica*, vol. 21, no. 3, pp. 393-407, 2010.
- [9] X. Wang, X. Yang, M. Zhang, and Y. Yu, "Cryptanalysis of a Fuzzy Identity Based Encryption Scheme in the Standard Model," *Informatica*, vol. 23, no. 2, pp. 299-314, 2012.
- [10] Y. Mao, J. Li, M. R. Chen, J. Liu, C. Xie, and Y. Zhan, "Fully secure fuzzy identity-based encryption for secure IoT communications," *Computer Standards & Interfaces*, vol. 44, pp. 117-121, 2016.
- [11] T. Tassa, "Hierarchical Threshold Secret Sharing," *Journal of Cryptology*, vol. 20, no. 2, pp. 237-264, 2007.
- [12] G. G. Lorentz, K. Jetter, and S. D. Riemenschneider, "Birkhoff Interpolation (Encyclopedia of Mathematics and its Applications)," Reading, Addison Wesley Publishing Company, 1983.
- [1] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Proceedings of CRYPTO'84*, vol. 84, pp. 47-53, 1985.
- [2] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," In *Advances in Cryptology-CRYPTO 2001*, pp. 213-229, 2003.
- [3] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," In *Eurocrypt*, vol. 3494, pp. 457-473, 2005.

Hierarchical Fuzzy Identity-Based Encryption

S. H. Hosseinian Barzi*, H. Maleki

*Shahid Beheshti University

(Received: 28/07/2017 , Accepted: 17/03/2018)

ABSTRACT

In a Fuzzy Identity-Based Encryption (FIBE) scheme, a user with the private key for an identity ID is able to decrypt a ciphertext encrypted with another identity ID' if and only if ID and ID' are within a certain distance of each other as judged by some metric. The existing literature on FIBE assumes that all attributes are equally important. However, this assumption may not be appropriate in some situations. In this paper, we consider the problem of FIBE with attributes of different importance level. In this setting, the set of possible attributes admits a hierarchical structure such that, during decryption process, attributes in lower levels can be replaced by those in higher levels. To solve this case, a new scheme called Hierarchical Fuzzy Identity-Based Encryption (HFIBE) was introduced then it was provided with a formal definition of security and an implementation method. The security of our proposed scheme is in the Selective-ID security model under the Decisional Modified Bilinear Diffie-Hellman assumption.

Keywords: Hierarchical, Fuzzy Identity-Based, Encryption

* Corresponding Author Email: hatefbarz@gmail.com