۱ امضای کور غیرقابل انکار

[۱]

طرح امضای کور پروتکلی است که طی آن درخواست‌کننده بدون افشای محتوای سند از امضاکننده در خواست می‌کند تا سند را امضا کند.در سال ۱۹۸۲ اولین بار چام طرح امضای کور رامعرفی کرد. [۴] این طرح براساس مسئله RSA بنا شده است. [۱۴] از آنجا که اکثر طرح‌های امضای کور و تغییرات آن براساس سختی مسائل متفاوتی از جمله مسئله لگاریتم گسسته [۲] ، مسائل زوجیت‌مبنا [۳] و مسائل مشکبه‌مبنا [۴] ارائه شده است [۳، ۱۵، ۱۸] ، ولی تمام این طرح‌ها یک مشکل اساسی دارند و مشکل این است که در برابر متخاصم کوانتومی ایمن نمی‌باشند. امضاهای کور معرفی شده توسط چام [۴] ، کامنیش [۳] و ژانگ‌وکیم [۱۸] به دلیل الگوریتم شور [۵] در برابر حملات کوانتومی ایمن نیستند. چنان‌که در [۶] نشان داده شده است ، امضای کور مشبکه‌مبنای معرفی شده توسط روکرت [۱۵] که از مدل فیات‌شمیر [۷] استفاده می‌کند در برابر مدل اوراکل تصادفی کوانتومی ایمن [۶] نمی‌باشد.

امضای کور هر دو ویژگی ناشناس‌بودن [۷] و احرازهویت [۸] را در خود دارد. [۹، ۱۱] درنتیجه این طرح در بسیاری از پروتکل‌های حفظ حریم‌خصوصی [۹] ازجمله پول‌الکترونکی [۱۰] و رای‌گیری‌الکترونیکی [۱۱] استفاده می‌شود. [۱۲، ۱۳] چنان‌چه در ابتدا گفته‌شد امضاکننده هیچ کنترلی بر محتوای سندی که قرار است امضا شود را ندارد ، علاوه‌براین امضاکننده هیچ کنترلی در نحوه استفاده از امضا را هم ندارد. با این اوصاف احساس می‌شود اعطای درجه‌ای از کنترل به امضاکننده نیاز است. یک از راه‌های ممکن آن است که امضاکننده و درخواست کننده(امضا) روی بخشی از محتوای سند توافق کنند. این راه توسط تکنیکی که آبه و فوجیساکی در [۱] ارائه کرده‌اند قابل دستیابی

[1] Undeniable Blind Signature

[2] Discrete Logarithm Problem (DLP)

[3] pairing-based problems

[4] lattice-based problems

[5] در زمان چندجمله‌ای مسائل لگاریتم گسسته و تجزیه‌اعداد را در کامپیوترهای کوانتومی حل می‌کند

[6] quantum random oracle model

[7] anonymity

[8] authentication

[9] privacy-preserving

[10] e-cash

[11] e-voting

می‌باشد.

راه دیگر آن است که این اختیار به امضاکننده داده شود تا تصمیم بگیرد چه‌کسی مجاز به تایید امضا می‌باشد.این روش ؟؟؟؟. طرح امضای غیرقابل‌انکار معرفی‌شده توسط چام و ون‌آنترپن [۵] دقیقا مطالب بالا [۱۲] را دربرمی‌گیرد.

بنابراین مطلوب است طرحی داشته باشیم که ناشناس‌بودن و تاییدسازی‌کنترل‌شده را درخود داشته باشد که ویژگی‌های هر دو طرح امضای کور و امضای غیرقابل‌انکار را برآورده کند. در سال ۱۹۹۶ ، ساکوری و یامانه [۱۶] یک طرح امضای کور غیرقابل‌انکار را براساس مساله لگاریتم گسسته ارائه دادند. چنان‌که در [۵] گفته‌شده‌است با این تکنیک می‌توان یک طرح امضای کور غیرقابل‌انکار بر اساس مسئله آراس‌آ [۱۳] طراحی کرد. ذکر این نکته لازم است که تمام این طرح‌ها در برابر حملات کوانتموی ایمن نیستند.

در این پایان‌نامه در نظر داریم یک طرح امضای کور غیرقابل‌انکار مقاوم کوانتومی بر اساس سختی مسائل همسانی روی خم‌های بیضوی سوپرسینگولار ارائه کنیم.

سوخارو و همکارانش در [۱۷] پیشنهادی درباره‌ی ساخت یک طرح امضا با تاییدکننده معین‌شده براساس سختی مسائل همسانی که مقاوم کوانتومی نیز می‌باشد ارائه کرده است.آنها همچنین یک ساخت عمومی از طرح رمزگذاری تاییداعتبار کلید نامتقارن ؟؟؟ را نشان داده‌اند.جائو و سوخارو در [۱۰] یک طرح امضای غیرقابل‌انکار همسانی‌مبنا ارائه کرده‌اند.در این پایان‌نامه قصد داریم طرح جائو و سوخارو را به یک طرح امضای کور غیرقابل‌انکار توسعه دهیم.

۱.۱ تعریف استاندارد

[۱۴]

انتظار می‌رود طرح امضای کور غیرقابل‌انکار ($UBSS$)[۱۵] ، ویژگی‌های طرح امضای غیرقابل‌انکار و طرح امضای کور را همزمان داشته باشد.در نتیجه این طرح باید ویژگی‌های ناخوانابودن محتوای پیام‌اولیه(قبل از امضا) [۱۶] و تاییدسازی کنترل شده [۱۷] را دارا باشد.

[۱۲] در یک طرح امضای غیرقابل‌انکار، امضاکننده تصمیم می‌گیرد تا چه کسی امضا را تایید کند

[13] RSA

[14] Formal Definition

[15] Undeniable Blind Signature Scheme

[16] anonoymity of the message origination

[17] controlled verification

تعریف۱. طرح امضای کور غیرقابل‌انکار ، یک طرح امضای تعاملاتی است که‌بوسیله چندتایی زیر معرفی می‌شود:

$$\mathcal{UBSS} = \big(KeyGen, Blind, Sign, Unblind, Check, \mathcal{CON}, \mathcal{DIS}\big)$$

۱. الگوریتم تولید کلید تصادفی $KeyGen$ ، پارامتر امنیتی 1^λ را به عنوان ورودی گرفته و زوج کلیدهای (vk, sk) را که به عنوان کلیدتاییدساز و کلیدمخفی نامیده می‌شوند، به عنوان خروجی تولید می‌کند. شکل شماتیک این الگوریتم به‌صورت زیر می‌باشد:

$$(vk, sk) \longleftarrow KeyGen(1^\lambda)$$

۲. الگوریتم کورسازی تصادفی $Blind$ ، پیام m را به عنوان ورودی گرفته و خروجی آن کورشده‌ی پیام، یعنی m' می‌باشد. شکل شماتیک این الگوریتم به شکل زیر می‌باشد که r کاملا به صورت تصادفی توسط الگوریتم ساخته می‌شود:

$$m' \longleftarrow {}_rBlind(m)$$

۳. الگوریتم امضای قطعی یا تصادفی $Sign$ ، کلید مخفی sk و پیام m را به عنوان ورودی گرفته و امضای σ را به عنوان خروجی تولید می‌کند. این الگوریتم را می‌توان به صورت زیر نشان داد:

$$\sigma \longleftarrow Sign_{sk}(m)$$

۴. الگوریتم شفاف‌ساز قطعی $Unblind$ ،امضای کور σ' و عددتصادفی r (انتخاب شده توسط الگوریتم کورسازی) را به عنوان ورودی گرفته و امضای شفاف σ را به عنوان خروجی تولید می‌کند. این الگوریتم را می‌توان به شکل زیر نمایش داد:

$$\sigma := Unblind_r(\sigma')$$

۵. الگوریتم قطعی بررسی $Check$ ، پیام m ، امضای شفاف σ و زوج کلیدهای (vk, sk) را به عنوان ورودی گرفته و بیت b را به عنوان خروجی تولید می‌کند. $b = 1$ به معنای آن است

که امضا متعلق به پیام می‌باشد و $b = ۰$ نیز به این معناست که امضا غیرمعتبر می‌باشد. این الگوریتم به‌صورت زیر قابل نمایش است:

$$b := Check_{(vk,sk)}(m, \sigma)$$

۶. پروتکل تایید π_{con} توسط امضاکننده اجرا می‌شود تا تاییدکننده اطمینان یابد که امضا معتبر است.

۷. پروتکل انکار π_{dis} نیز توسط امضاکننده اجرا می‌شود و تاییدکننده متقاعد می‌شود که امضا نامعتبر است.

برای هر زوج کلید (vk, sk) که توسط الگوریتم $KeyGen(۱^{\lambda})$ تولید می‌شود و همچنین هر m از میان فضای پیام و هر عددتصادفی r که توسط الگوریتم $Blind$ تولید شده است، باید تساوی زیر برقرار باشد:

$$Check_{(vk,sk)}(m, Unblind_r(Sign_{sk}({}_rBlind(m)))) = ۱$$

علاوه‌براین، اگر الگوریتم امضا قطعی باشد آنگاه می‌توان فرض کرد اثر مراحل الگوریتم‌های کورسازی_امضا_شفافیت روی پیام دقیقا مشابه اجرای مستقیم الگوریتم امضا روی پیام می‌باشد. برای درک این مطلب آن را به صورت زیر نمایش می‌دهیم:

$$Unblind_r(Sign_{sk}({}_rBlind(m))) = Sign_{sk}(m)$$

۲.۱ کارکرد UBSS

۱۸

برای درک بهتر نقش الگوریتم‌های گفته شده در بخش قبلی، پروتکل را به صورت کامل اجرا می‌کنیم.

در ابتدا امضاکننده یک پارامتر امنیتی λ را انتخاب و الگوریتم $KeyGen(1^{\lambda})$ را برای به دست آوردن زوج کلید (vk, sk) اجرا می‌کند.کلید امضای sk به صورت مخفی پیش امضاکننده حفظ می‌شود و کلید تاییدساز vk توسط امضاکننده منتشر می‌شود. m پیامی است که درخواست‌کننده خواهان امضای آن به صورت ناخوانا است؟؟. به این منظور ، درخواست‌کننده ابتدا m[۱۹] را با اجرای الگوریتم $Blind(m)$ به m'[۲۰] تبدیل می‌کند. [۲۱] درادامه درخواست‌کننده m' را به همراه شناسه هویتی خود Id_R ، ارسال می‌کند. امضاکننده ابتدا شناسه درخواست‌کننده را تایید (۲.۱) و سپس الگوریتم $Sign_{sk}$ را روی m' اجرا می‌کند تا امضای کور σ' به دست آید. دریافت‌کننده پس از دریافت امضای کور از امضاکننده ، توسط الگوریتم $Unblind$ و مقدارتصادفی r انتخاب شده در مرحله کورسازی، امضا را از حالت کور خارج کرده وسپس زوج پیام اصلی و امضای شفاف (m, σ) پیام رابرای بخش تایید؟؟ ارسال می‌کند.

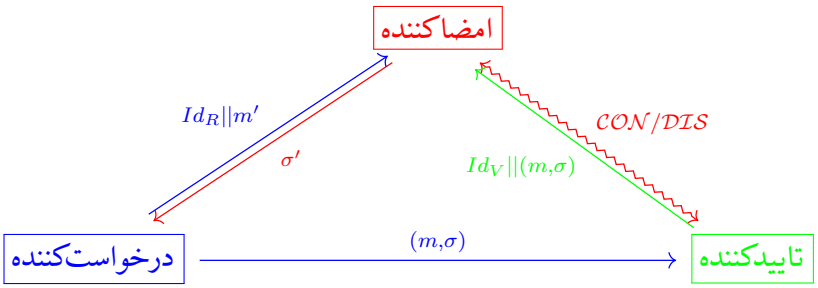
هربخشی که خواهان تایید امضا باشد، شناسه خود Id_V را به همراه زوج پیام و امضا (m, σ) برای امضاکننده ارسال می‌کند. امضاکننده در ابتدا شناسه تاییدکننده را بررسی می‌کند(۲.۱) آنگاه اگر Id_V یک شناسه معتبر در میان تاییدکنندگان احراز شده(مجاز) نباشد، امضاکننده از ادامه ارتباط خودداری می‌کند. در غیراینصورت الگوریتم بررسی $Check$ را اجرا می‌کند. اگر خروجی این الگوریتم معتبر باشد آنگاه پروتکل تایید $\mathcal{CON}$ توسط امضاکننده آغاز می‌شود؛ درغیراینصورت پروتکل انکار $\mathcal{DIS}$ اجرا می‌شود(شکل ۱ تمام مفاهیم طرح $UBSS$ را نشان می‌دهد).

[18] Workinf of UBSS

[۱۹] پیام خوانا

[۲۰] پیام ناخوانا

[۲۱] در زمان اجرای الگوریتم ، یک انتخاب تصادفی r توسط خود الگوریتم تولید می‌شود.



شکل ۱ : اطلاعات کامل طرح امضای کور غیرقابل‌انکار

توجه۱. در این پایان‌نامه عمدا چگونگی احراز هویت بین درخواست‌کننده و تاییدکننده با امضاکننده را مشخص نمی‌کنیم. این امر مستلزم آشنایی با احراهویت متقابل می‌باشد. این طرح در [۲، ۸] به‌صورت کامل آورده شده است که در مقابل حملات کوانتومی نیز ایمن می‌باشند.

۳.۱ ویژگی‌ها

۲۲

[22] Properties

مراجع

[1] Masayuki Abe and Eiichiro Fujisaki. How to date blind signatures. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 244–251. Springer, 1996.

[2] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Annual Cryptology Conference*, pages 361–379. Springer, 2013.

[3] Jan L Camenisch, Jean-Marc Piveteau, and Markus A Stadler. Blind signatures based on the discrete logarithm problem. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 428–432. Springer, 1994.

[4] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[5] David Chaum and Hans Van Antwerpen. Undeniable signatures. In *Conference on the Theory and Application of Cryptology*, pages 212–216. Springer, 1989.

[6] Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni. The fiat–shamir transformation in a quantum world. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 62–81. Springer, 2013.

[7] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 186–194. Springer, 1986.

[8] Sebastianus A Goorden, Marcel Horstmann, Allard P Mosk, Boris Škorić, and Pepijn WH Pinkse. Quantum-secure authentication of a physical unclonable key. *Optica*, 1(6):421–424, 2014.

[9] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai. An untraceable blind signature scheme. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 86(7):1902–1906, 2003.

[10] David Jao and Vladimir Soukharev. Isogeny-based quantum-resistant undeniable signatures. In *International Workshop on Post-Quantum Cryptography*, pages 160–179. Springer, 2014.

[11] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. A new blind signature based on the discrete logarithm problem for untraceability. *Applied Mathematics and Computation*, 164(3):837–841, 2005.

[12] Chun-Ta Li, Min-Shiang Hwang, and Chi-Yu Liu. An electronic voting protocol with deniable authentication for mobile ad hoc networks. *Computer Communications*, 31(10):2534–2540, 2008.

[13] Iuon-Chang Lin, Min-Shiang Hwang, and Chin-Chen Chang. Security enhancement for anonymous secure e-voting over a network. *Computer Standards & Interfaces*, 25(2):131–139, 2003.

[14] RL Rivest and B Kaliski. Rsa problem, encyclopedia of cryptography and security, 2005.

[15] Markus Rückert. Lattice-based blind signatures. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 413–430. Springer, 2010.

[16] Kouichi Sakurai and Yoshinori Yamane. Blind decoding, blind undeniable signatures, and their applications to privacy protection. In *International Workshop on Information Hiding*, pages 257–264. Springer, 1996.

[17] Vladimir Soukharev, David Jao, and Srinath Seshadri. Post-quantum security models for authenticated encryption. In *Post-Quantum Cryptography*, pages 64–78. Springer, 2016.

[18] Fangguo Zhang and Kwangjo Kim. Id-based blind signature and ring signature from pairings. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 533–547. Springer, 2002.