結託耐性を備えた アイデンティティ識別不可能な属性認証方式

穴田 啓晃[1,a)]

概要：ユーザが複数の属性権限を付与されるとき，認証システムは複数の属性を同時に認証する属性認証方式が便利である．近年，プライバシー保護の観点から，ユーザのアイデンティティが識別不可能である属性認証方式が必要とされている．他方，属性認証方式においては，攻撃者が複数のユーザから属性権限を収集し検証者に認証を受理させようとする結託攻撃が典型的にありうる．本稿では，結託耐性を備えた，アイデンティティ識別不可能な属性認証方式を提案する．

キーワード：証拠識別不可能な証明システム，結託耐性

Identity-Indistinguishable Attribute-Authentication Scheme with Collusion Resistance

Hiroaki ANADA[1,a)]

Abstract: When a user is given plural rights of attributes, an authentication system with a scheme that is capable of simultaneous authentication of the plural attributes is useful. Recent years, from the view point of users' privacy, there arises a need for such an attribute-authentication scheme but with indistinguishablity of users' identities. On the other hand, in the attribute-authentication scheme, a collusion attack is typical, where an adversary collects rights of attributes from plural users and tries to make a verifier accept an authentication. In this paper, we propose an identity-indistinguishable attribute-authentication scheme with the collusion resistance.

Keywords: witness-indistinguishable proof system, collusion resistance

1. Introduction

認証（authentication）は，ネットワークの管理者がネットワークのユーザのアイデンティティや属性を確認するための基本的な処理である．ユーザがネットワークのユーザとして複数の属性権限を付与されるとき，認証システムとしては複数の属性を同時に認証する属性認証方式が便利である．近年，クラウドサーバが提供する多様なサービスが必須になってきているという観点，また，ビッグデータの解析等で利用履歴が知らずと収集されるという観点から，プライバシー保護が重要になってきている．この背景から，ユーザのアイデンティティが識別不可能であるという要件をも実現した属性認証方式が要望されてきている．

他方，ユーザのアイデンティティが一意に特定できないという上記の属性認証方式においては，攻撃者が複数のユーザから属性権限を収集し検証者に認証を受理させようとする結託攻撃が典型的にありうる．

本稿では，これらの背景に鑑み，アイデンティティ識別不可能性を備え，なおかつ，結託攻撃に対する耐性（以降，結託耐性）を実現する属性認証方式の設計を課題とする．計算機科学，特に，暗号学の学術領域では，従来より，証拠識別不可能な証明システムと呼ばれる，一つの叙述（statement）に対し複数の証拠（witnesses）のいずれか

[1] 長崎県立大学 〒851–2195 長崎県西彼杵郡長与町まなび野 1–1–1 University of Nagasaki 1–1–1, Manabino, Nagayo-cho, Nishisonigi-gun, Nagasaki 851–2195, Japan
[a)] anada@sun.ac.jp

を有していることを立証する対話型アルゴリズムが知られている（witness-indistinguishable proof system, [4], [6]）．ここで，証拠は各ユーザが秘密にする情報である．証拠識別不可能な証明システムを要素技術の一つとし，ユーザの各属性に対し，証拠識別不可能な証明システムが証明する言語（language）を一つずつ考え，これらを（安直に）連接（concatenation）すると，アイデンティティが識別不可能な属性認証方式を作ることができる．しかしながら，この属性認証方式は結託攻撃に弱く，上記の課題を解決できない．

そこで，本稿では，コミットメントスキーム（[6]）をもう一つの要素技術として加える，というアプローチを採る．連接された言語の部分集合として定義される言語に対する証明システムを設計することで，結託耐性を備えたアイデンティティ識別不可能な属性認証方式を提案する．

2. Preliminaries

セキュリティパラメータを λ と記す．p をビット長 λ の素数とする．ストリング x のビット長を $|x|$ と記す．．ストリング x とストリング y の連接を $x \| y$ と記す．集合 S からの元 a の一様ランダムサンプリングを $a \in_R S$ と記す．アルゴリズム A が a を入力とし z を出力することを $z \leftarrow A(a)$ もしくは $A(a) \to z$ と記す．

2.1 Blinear Maps [5]

$(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi)$ を Type 2 [5] の素数位数 p の双線形群とする．ただし，効率的に計算可能な双線形写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ があり, また, Type 2 ゆえ効率的に計算可能な群準同型写像 $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ with $\psi(g_2) = g_1$ があるものとする．$g_2 \in_R \mathbb{G}_2 \backslash \{1_{\mathbb{G}_2}\}$ を $\mathbb{G}_2$ の生成元とし，$g_1 := \psi(g_2)$ とし，また $\mathbb{G}_T$ は $e(g_1, g_2) (\neq 1_{\mathbb{G}_T})$ により生成されるものとする．1^λ を入力とし params $:= (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi)$ を出力する確率的アルゴリズムを `BlGrp` と記す．

2.2 Number Theoretic Assumptions

本稿の提案方式の安全性は，DLin Assumption [3], n-DHE Assumption [1], q-SFP Assumption [1] といった数論的な仮定に依存する．

2.3 Structure Preserving Signatures [1], [2]

Structure preserving signature scheme [1], [2] はデジタル署名方式の一種である．演算には双線形群 `BlGrp` を用いる．

2.4 Groth-Sahai NIWI Proofs [6]

Groth-Sahai の非対話型証拠識別不可能な証明システム [6] は証拠識別不可能な証明システムの一種である．演算には双線形群 `BlGrp` を用いる．

3. Our Proposed Scheme

3.1 Procedure

本稿の提案方式では，属性権限はデジタル署名の形で発行されるものとする．すなわち，権限機関がユーザに対し，各属性権限についてのデジタル署名を各々発行する．ただし，アイデンティティは，一つのデジタル署名のうちの一つの要素によって表されるものとする．複数のデジタル署名については，上記の一つの要素が共通である（同じ元である）ことによって実現される．具体的には，双線形群 `BlGrp` を用い，デジタル署名の方式として structure preserving signatures [1], [2] を使う．

次いで，本稿の提案方式では，ユーザが各属性権限についての各デジタル署名を証拠とする．ユーザは，検証者に対し，各属性権限についての，非対話型の証拠識別不可能な証明システムを各々実行する．具体的には，双線形群 `BlGrp` を用い，非対話型の証拠識別不可能な証明システムとしては Groth-Sahai の証明システム [6] を使う．

提案方式の procedure の概要を下記に示す．

(1) 権限機関はユーザに対し各属性権限についてのデジタル署名を structure preserving signature scheme [1], [2] により発行する．ただし，複数の属性権限についてのデジタル署名を発行する場合，単一のユーザに対し，$\zeta \in_R \mathbb{Z}_p$ を 1 回だけサンプリングし，デジタル署名の成分 $\tilde{G}^\zeta$（[1]）を共通にする．

(2) ユーザは検証者に対し，Groth-Sahai の非対話型証拠識別不可能な証明システム [6] により，属性権限のデジタル署名について証明を実行する．証明プロトコルは，複数の属性権限に応じて複数を並行し実行する．加えて，各デジタル署名の共通成分 $\tilde{G}^\zeta$ について Groth-Sahai のコミットメント [6] を生成する．そして同じく，Groth-Sahai の非対話型証拠識別不可能な証明システム [6] により，証明を実行する．

3.2 Discussion

各々の証明システムの言語を $L_i, i = 1, \ldots, n$ とする．このとき，複数の属性権限に応じた（Groth-Sahai の非対話型証拠識別不可能な）複数の証明システムの並行な実行は，連接された言語 $\prod_{1 \le i \le n} L_i$ についての証明システムの実行である．加えて，各デジタル署名の共通成分 $\tilde{G}^\zeta$ について Groth-Sahai のコミットメント [6] を生成し証明システムを実行することは，連接された言語 $\prod_{1 \le i \le n} L_i$ の部分集合として定義される言語 $L^{\mathrm{bnd}} \stackrel{\mathrm{def}}{=} \prod_{1 \le i \le n, \tilde{G}^\zeta : \text{共通}} L_i$ に対する証明システムを実行することである．

Theorem1 (アイデンティティ識別不可) 提案する属性認証方式はアイデンティティ識別不可である．

Theorem2 (結託攻撃不可) 提案する属性認証方式は結託攻撃不可である．

4. Conclusion

本稿では，証拠識別不可能な証明システム及びコミットメントスキームを要素技術とし，結託攻撃に弱いという課題を解決する，アイデンティティ識別不可能な属性認証方式の概要を提案した．連接された言語の部分集合として定義される言語 L^{bnd} に対する証明システムを設計することで，結託耐性を備えさせることができた．

謝辞 本研究は JSPS 科研費 JP15K00029 の助成を受けたものです．

参考文献

[1] Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K. and Ohkubo, M.: Structure-Preserving Signatures and Commitments to Group Elements, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, pp. 209–236 (online), DOI: 10.1007/978-3-642-14623-7_12 (2010).

[2] Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K. and Ohkubo, M.: Structure-Preserving Signatures and Commitments to Group Elements, *J. Cryptol.*, Vol. 29, No. 2, pp. 363–421 (online), DOI: 10.1007/s00145-014-9196-7 (2016).

[3] Boneh, D., Boyen, X. and Shacham, H.: Short Group Signatures, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, pp. 41–55 (online), DOI: 10.1007/978-3-540-28628-8_3 (2004).

[4] Feige, U. and Shamir, A.: Witness Indistinguishable and Witness Hiding Protocols, *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pp. 416–426 (online), DOI: 10.1145/100216.100272 (1990).

[5] Galbraith, S. D., Paterson, K. G. and Smart, N. P.: Pairings for cryptographers, *Discrete Applied Mathematics*, Vol. 156, No. 16, pp. 3113–3121 (online), DOI: 10.1016/j.dam.2007.12.010 (2008).

[6] Groth, J. and Sahai, A.: Efficient Non-interactive Proof Systems for Bilinear Groups, *Proceedings of the Theory and Applications of Cryptographic Techniques 27th Annual International Conference on Advances in Cryptology*, EUROCRYPT'08, Berlin, Heidelberg, Springer-Verlag, pp. 415–432 (online), available from ⟨http://dl.acm.org/citation.cfm?id=1788414.1788438⟩ (2008).