被評定者の叙述を伴うデジタル署名による表現豊かな評定スキーム

穴田 啓晃[1]　ルジ スシミタ[2]　櫻井 幸一[3,4]

概要：五つ星評価による評定とコメントなどの例に見られる評判ボードは，製品についての有用な情報を消費者に提供する利便性から親しまれている．本稿では，その評判ボードのための評定スキームの一種を提案する．その特徴は，製品のみならず供給者をもまた表現豊かに評定するのを可能にすることである．はじめに，その「表現豊かな評定スキーム」のシンタックスを定義する．次いで，属性ベース署名スキーム (ABS) の「表現豊かな評定スキーム」への一般的変換を提供する．その際，公開関連付け可能性 (public linkability) が二重評定を禁ずるために用いられる．

キーワード：評判システム，評定，デジタル署名，属性，叙述

Hiroaki Anada[1]　Sushmita Ruj[2]　Kouichi Sakurai[3,4]

1. Introduction

評判は世間で基本的な現象であるといってよい．インターネット上におけるそれは益々重要になってきている．典型的な例は “amazon.com” のような取り引きのウィブサイトにおける評判ボードに見受けられる．評判ボードでは，供給者による製品は消費者によって評定される．後々，評判ボードのシステム管理者は，それらの個別の評定に対し，典型的には統計処理である何らかの “評判関数” を用い，“評判に” 集約する．このような評判ボードは，その在り方から現実問題まで広く探求されてきた．([4], [10], [11] 等)．とりわけ暗号学の見地から，評判ボードは格好の研究対象であり続けている [4], [13], [15]．その理由は，評判ボードへの要求機能には評定の偽造不可，評定の匿名性，二重評定不可，評定の追跡可能性といったものがあり，これらに対し，暗号学のアプローチが好適だからである．そして，暗号学のアプローチによる評判ボード (評判システムと呼ばれることが多い)，あるいは評定スキームの構成においては，中心的な要素技術はグループ署名スキーム [5], [6], [7], [9] であった．

評判ボードのための評定スキームの構成の一つは，(“amazon.com” のような) システム管理者と呼ばれる単一の権限機関と，製品の供給者達，また消費者達から成るものである．供給者の製品は，取り引きを経て消費者によって購入され，使用される．システム管理者は正直 (honest) であると仮定され，供給者及び消費者の両方の登録を制御する．本稿では，供給者もまた正直 (honest) であると仮定する．というのも，消費者は製品を評定し，そしてその評定は供給者の振る舞いにとって重要だからである (なので正直に振る舞う)．他方，消費者対しては，本稿で我々はその振る舞いを議論する．以降，本稿では消費者をユーザと呼ぶ．

上記の暗号学に関わる要求機能 [8], [12], [16] は次のように捉えられる．

第一に，正当なユーザになりすました評定は出来ないようにしなければならない．すなわち，評定スキームは評定の偽造が不可でなければならない．第二に，ユーザがある製品を評定するとき，彼は供給者及び他のユーザに対し匿名でなければならない．すなわち，正直な評定に関する限り，評定スキームは評定者が匿名で扱われなければならない．第三に，一つの製品に対する二重評定は出来ないようにしなければならない．このための一つのアプローチとして，評定スキームは，一人のユーザによる評定が，公開された場でリンク付け可能でなければならない．第四に，評定したユーザが (不法に振る舞った場合など) 特定されるべき状況では，システム管理者がそのユーザを追跡するこ

[1] 長崎県立大学 情報セキュリティ学科
[2] インド統計研究所 暗号とセキュリティ研究ユニット
[3] 九州大学大学院 システム情報科学研究院
[4] 公益財団法人九州先端科学技術研究所 情報セキュリティ研究室

とが可能でなければならない．すなわち，評定スキームは (現実の運用を想定すると) ユーザ追跡可能性を有さなければならない．

上記の要求機能については既に多くの研究があるが，その一方，本稿では，次のような状況が今なお課題であると考える．すなわち，評判ボードの使用においては，評定者は彼の購入した製品を様々な観点から見る．例えば，価格，運用コスト，機能性，品質，信頼性，保証，といった性質の観点である．現在，上記の性質が相互に依存していることが多いにも関わらず，上記の性質は別々に扱われてきた．例えば，ユーザが製品を繰り返し購入する場合，価格と運用コストは別々に扱われるべきではない．この場合，評定は「価格または運用コストが三つ星 (⋆⋆⋆) である」と表わせられれば都合が良い．更に，ユーザ (消費者) が，個々の製品についてでなく，それらの供給者についての評判を必要とする場合も多い．例えば，評定としてもし次のような陳述が。できれば有用である：「この供給者の製品は，価格について二つ星かつ信頼性について三つ星であるか，もしくは価格について四つ星かつ信頼性について四つ星である．その一方，保証はどの製品も五つ星である.」以降，製品もしくは供給者をまとめて被評定者と呼ぶことにする．上記の例から，ユーザ (評定者) が被評定者を，被評定者の属性についての叙述で表した評定でもって評価したい場合があると考えられる．本稿では，このような評定を表現豊かな評定と呼ぶことにする．

1.1 提案事項

本稿では，上述の課題を念頭に，表現豊かな評定スキーム，つまり評定が被評定者の属性についての叙述を伴う評定スキームを与える．なお，本稿の著者らは文献 [1], [3] において上述の課題を解決することを目的とする研究を継続してきており，新規の結果を文献 [2] に著した．本稿の以降では，[2] における提案事項の背景及び趣旨に力点を置き説明する．

第一の提案事項は，表現豊かな評定スキームのシンタックスを定義し，また，表現豊かな評定スキームに対する攻撃を実験 (experiment) で定義した点である．

第二の提案事項は，属性ベース署名スキームの表現豊かな評定スキームへの一般的変換を与えた点である．その要点は，属性プライバシーを有する属性ベース署名スキームを，(わざわざ) 公開リンク付け可能性を持つよう，ダウングレードすることである．この目的は，属性ベース暗号と同様に属性ベース署名のソフトウェア実装例が多く見られるようになった際，これを容易に表現豊かな評定スキームに変換できるようにして頂くためである．

第三の提案事項は，上記の一般的変換によらず，はじめから公開リンク付け可能性を持つ属性ベース署名スキームを構成技術要素に用い，表現豊かな評定スキームを構成した点である．この目的は，一般的変換で得られるものよりも計算時間の効率，及び評定データ長の効率の良い方式も可能であることを提示するためである．フィアット - シャミア署名型の属性ベース署名スキームを用いた

第四の提案事項は，表現豊かな評定スキームのユースケースを提示した点である．定量的属性と定性的属性を区別し，上述のように表現豊かに評定する簡単な事例を示した．

上記の四つの提案事項については文献 [2] を参照されたい．

1.2 関連研究

属性ベース評定スキームあるいは属性ベース評判システムは，これまで評定者の属性に基づくものが発表されていた [12], [14]．これに対し，被評定者の属性に基づく属性ベース評定スキームは [2] での提案がはじめてであると考えられる．

謝辞 第一著者に関し，本研究は JSPS 科研費 JP15K00029 の助成を受けたものです．第三著者に関し，本研究は JSPS 科研費 JP15H02711 の助成を受けたものです．

参考文献

[1] H. Anada, S. Ruj, and K. Sakurai.
Expressive rating scheme based on attributes of ratees.
In **暗号と情報セキュリティシンポジウム** *2016* **予稿集**, pages 2E2–2, 2016.

[2] H. Anada, S. Ruj, and K. Sakurai.
Expressive rating scheme by signatures with predications on ratees.
In *The 10th International Conference on Network and System Security (NSS 2016)*, page (to appear), 2016.

[3] H. Anada and K. Sakurai.
Reputation system based on attributes of ratees.
In **コンピュータセキュリティシンポジウム** *2015* **予稿集**, pages 2C1–1, 2015.

[4] E. Androulaki, S. G. Choi, S. M. Bellovin, and T. Malkin.
Reputation systems for anonymous networks.
In *Privacy Enhancing Technologies, 8th International Symposium, PETS 2008, Leuven, Belgium, July 23-25, 2008, Proceedings*, pages 202–218, 2008.

[5] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik.
A practical and provably secure coalition-resistant group signature scheme.
In *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, pages 255–270, 2000.

[6] M. Bellare, D. Micciancio, and B. Warinschi.
Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions.
In *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-*

8, 2003, Proceedings, pages 614–629, 2003.

[7] M. Bellare, H. Shi, and C. Zhang.
Foundations of group signatures: The case of dynamic groups.
In *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, pages 136–153, 2005.

[8] J. Blömer, J. Juhnke, and C. Kolb.
Anonymous and publicly linkable reputation systems.
In *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers*, pages 478–488, 2015.

[9] D. Boneh, X. Boyen, and H. Shacham.
Short group signatures.
In *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, pages 41–55, 2004.

[10] S. Clauß, S. Schiffner, and F. Kerschbaum.
k-anonymous reputation.
In *8th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '13, Hangzhou, China - May 08 - 10, 2013*, pages 359–368, 2013.

[11] C. Dellarocas.
Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior.
In *EC*, pages 150–157, 2000.

[12] L. Guo, C. Zhang, Y. Fang, and P. Lin.
A privacy-preserving attribute-based reputation system in online social networks.
J. Comput. Sci. Technol., 30(3):578–597, 2015.

[13] F. Kerschbaum.
A verifiable, centralized, coercion-free reputation system.
In *Proceedings of the 2009 ACM Workshop on Privacy in the Electronic Society, WPES 2009, Chicago, Illinois, USA, November 9, 2009*, pages 61–70, 2009.

[14] J. K. Liu, M. H. Au, X. Huang, W. Susilo, J. Zhou, and Y. Yu.
New insight to preserve online survey accuracy and privacy in big data era.
In *Computer Security - ESORICS 2014 - 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II*, pages 182–199, 2014.

[15] A. Michalas and N. Komninos.
The lord of the sense: A privacy preserving reputation system for participatory sensing applications.
In *IEEE Symposium on Computers and Communications, ISCC 2014, Funchal, Madeira, Portugal, June 23-26, 2014*, pages 1–6, 2014.

[16] T. Nakanishi and N. Funabiki.
An anonymous reputation system with reputation secrecy for manager.
IEICE Transactions, 97-A(12):2325–2335, 2014.

付　　録

A.1 表現豊かな評定スキームのエンティティ

下記のエンティティ (entity, 役割付けられた登場物) とそれらの間の関係を図 A·1 に示す.

システムマネージャ *(system manager)*

供給者 *(provider)*

製品 *(product)*

アイテム *(item)*

ユーザ *(user)*

評定者 *(rater)*

被評定者 *(ratee)*

図 A·1 Relation between entities in a expressive rating scheme.