Computer Security Symposium 2015
21 - 23 October 2015

被評定物の属性に基づく評判システム*

穴田 啓晃 †　　　櫻井 幸一 ‡†

† 公益財団法人九州先端科学技術研究所
814-0001 福岡市早良区百道浜 2-1-22 福岡 SPR センタービル 7F
anada@isit.or.jp

‡ 九州大学大学院システム情報科学研究院
819-0395 福岡市西区元岡 744 W2-712
sakurai@inf.kyushu-u.ac.jp

あらまし 評判システムは，物の取引きのネットワーク上で，ユーザが物に個人別の評定を付すことを可能にする．後にシステム管理者は，評判関数を使ってそれらの評定を評判に集約する．本稿では，被評定物の属性に基づく評判システムを定義する．個人別の評定として，被評定物の属性について叙述したブール式に対する属性ベース署名を使う．また，評判関数はそれらの署名を入力に取るものとする．次いで本稿では，フィアット - シャミアの仕方の属性ベース署名スキームを用い，この評判システムを具体的に構成する．従来の類似の評判システムでは，システム管理者が予めセットアップし固定した属性ユニバースの下でシステムを運用しなければならない問題点があった．本稿の具体的方式では，属性ユニバースを随時更新することが可能である．

Reputation System Based on Attributes of Ratees

Hiroaki Anada†　　　Kouichi Sakurai‡†

†Institute of Systems, Information Technologies and Nanotechnologies.
7F, Fukuoka SRP Center Bldg., 2-1-22, Momochihama, Sawara-ku, Fukuoka, 814-0001 JAPAN
anada@isit.or.jp
‡Faculty of Information Science and Electrical Engineering, Kyushu University.
W2-712, 744, Motooka, Nishi-ku, Fukuoka, 819-0395 JAPAN
sakurai@inf.kyushu-u.ac.jp

Abstract A reputation system enables users to rate a ratee individually on the underlying transaction network. Later, the system manager merges those ratings into a reputation by using a reputation function, In this paper, we define a reputation system based on attributes of ratees. We use as an individual rating an attribute-based signature (ABS) on a boolean formula that tells about attributes of ratees. We let the reputation function take as an input those signatures. Then, using an ABS scheme of the Fiat-Shamir style, we construct the reputation system concretely. In analogous previous reputation systems, there is a problem that the system manager must operates the system under a fixed attribute universe set up beforehand. In our concrete system, the attribute universe can be updated at any time.

1 Introduction

Reputation is fundamental phenomenon in our world, even on the Internet. A typical example of reputation can be seen as a scoring board in a

*The first author is partially supported by Grants-in-Aid for Scientific Research of Japan Society for the Promotion of Science; Research Project Number:15K00029. The second author is partially supported by Grants-in-Aid for Scientific Research of Japan Society for the Promotion of Science; Research Project Number: 15H02711.

website of providers and consumers such as amazon.com. On such a website, a reputation system enables a user to rate a ratee that was obtained through a transaction. Later, the system manager merges those individual ratings into a reputation on the ratee by using a reputation function.

Such reputation systems have been studied widely from the paradigm to realistic problems [10, 3, 9]. From the cryptographic aspect, reputation systems have been studied with interest [3, 12, 15] because of the required functionality such as rater anonymity, traceability, unforgeability and public linkability. There the central building block is the group signature scheme [4, 5, 6, 8].

A reputation system consists of one authority called the system manager and users who are consumers of items provided via transactions. The system manager, like amazon.com, is assumed to be honest, issues the system manager's public key MPK, and control the registration of both providers of items and users of items. We don't care in this paper the registration of providers because we assume that they are honest. On the other hand, we care the registration of users because they can not be assumed to be honest.

Here the above cryptographic requirements arise [16, 7, 11]; that is, when a user rates an item, he should be treated anonymous to providers and other users. When a user acts unlegitimately, for example, rating an item twice or rating an item on behalf of other users, he should be traced by the system manager. To prevent such unlegitimate behaviors, rating should be unforgeable and publicly linkable.

1.1 Our Contribution

In the usage of a reputation system, a rater looks an item of a provider (that is, an item he actually bought) from various points of view such as price, functionality, quality, reliability, insurance, etc. That is, an item has plural aspects called attributes. Especially, it is natural that *a reputation is told as a boolean formula over those attributes of ratees.* But in the previous work, no such reputation system has been proposed yet.

In this paper, keeping the above functionalities in mind, we provide a definition of a reputation system based on attributes of ratees, for the first time. In our system, an attribute universe of ratees is considered, and a reputation value is about a boolean formula over attributes. Then, using an ABS scheme of the Fiat-Shamir style, we provide the reputation system concretely. Compared with the previous reputation systems that employ group signature schemes [4, 5, 6, 8], our reputation system can realize a fine-grained rating at a time. Note that the fine granularity of our reputation system is realized as *ratee's attributes.*

1.2 Related Work

Nakanishi and Funabiki [16] gave a simple efficient anonymous reputation system. In their reputation system, users are seller and buyers, and seller anonymity is achieved by employing a group signature scheme.

Blömer et al. [7] gave an anonymous and publicly linkable reputation system by employing a group signature scheme.

Guo et al. [11] gave a definition and construction of a privacy-preserving attribute-based reputation system. Their system differs from our work at the point that, in their scheme, attribute are of raters, not of ratees.

The contributions and comparison are summarized in the Table 1.

2 Preliminaries

2.1 Reputation System

Here, based on previous work [4, 5, 6, 8], we list up the requirements for a reputation system from the view point of cryptography.

Rater anonymity means that signatures of honest users are indistinguishable.

表 1: Comparison of functionalities.

	Seller Anonymity	Rater Anonymity	Traceability	Unforgeability	Public Link. (Prohibit Double Rating)	Fine Grained (Rater)	Fine Grained (Ratee)	Access Formula
Nakanishi et al. [16]	✓	✓	✓	✓	✓	-	-	-
Blömer et al. [7]	-	✓	✓	✓	✓	-	-	-
Guo et al. [11]	✓	✓	✓	✓	✓	✓	-	Non-mono.
Our approach	-	✓	✓	✓	✓	-	✓	Monotone

Traceability means that it is impossible for any set of colluding users to create ratings that can not be traced back to a user of the system.
Unforgeability means that nobody can produce signatures on behalf of honest users.
Public linkability requires that anyone can decide whether or not two ratings for the same product were created by the same user, i.e. no secret key is required to link messages. Note that public linkability implies that users can only stay anonymous as long as they rate products just once.

Though preferable, other features such as *verifier-local revokability* is not treated in this paper.

2.2 Attribute-Based Signature [13, 1]

2.2.1 Scheme

An attribute-based signature scheme, ABS, consists of four PPT algorithms: ABS =(**ABS.Setup**, **ABS.KG**, **ABS.Sign**, **ABS.Vrfy**).
ABS.Setup$(1^\lambda, \mathcal{U}) \rightarrow (\mathbf{MPK}, \mathbf{MSK})$**.** It takes as input the security parameter λ and an attribute universe $\mathcal{U}$. It outputs a public key MPK and a master secret key MSK.
ABS.KG$(\mathbf{MPK}, \mathbf{MSK}, S) \rightarrow \mathbf{SK}_{\mathbf{id},S}$**.** It takes as input the public key MPK, the master secret key MSK, and an attribute set $S \subset \mathcal{U}$. It outputs a signing key $\mathrm{SK}_{\mathrm{id},S}$ corresponding to S.
ABS.Sign$(\mathbf{MPK}, \mathbf{SK}_{\mathbf{id},S}, (m, f)) \rightarrow \sigma$**.** It takes as input a public key MPK, a private secret key $\mathrm{SK}_{\mathrm{id},S}$ corresponding to an attribute set S, a pair (m, f) of a message $\in \{1,0\}^*$ and an access formula. It outputs a signature σ.
ABS.Vrfy$(\mathbf{MPK}, (m, f), \sigma)$**.** It takes as input a public key MPK, a pair (m, f) of a message and an access formula, and a signature σ. It outputs a decision 1 or 0. When it is 1, we say that $((m, f), \sigma)$ is *valid*. When 0, we say that $((m, f), \sigma)$ is *invalid*. We demand correctness of ABS; for any λ, any $\mathcal{U}$, any $S \subset \mathcal{U}$ and any (m, f) such that $f(S) = 1$, $\Pr[(\mathrm{MPK}, \mathrm{MSK}) \leftarrow \mathbf{ABS.Setup}(1^\lambda, \mathcal{U}), \mathrm{SK}_{\mathrm{id},S} \leftarrow \mathbf{ABS.KG}(\mathrm{MPK}, \mathrm{MSK}, S), \sigma \leftarrow \mathbf{ABS.Sign}(\mathrm{MPK}, \mathrm{SK}_{\mathrm{id},S}, (m, f)), b \leftarrow \mathbf{ABS.Vrfy}(\mathrm{MPK}, (m, f), \sigma) : b = 1] = 1$.

2.2.2 Chosen-Message Attack on ABS

An adversary $\mathcal{F}$'s objective is to make an *existential forgery*. $\mathcal{F}$ tries to make a forgery $((m^*, f^*), \sigma^*)$ that consists of a message, a target access policy and a signature. The following experiment $\mathbf{Exprmt}^{\text{euf-cma}}_{\mathcal{F},\mathtt{ABS}}(\lambda, \mathcal{U})$ of a forger $\mathcal{F}$ defines the *chosen-message attack on ABS to make an existential forgery*.

$$
\begin{aligned}
&\mathbf{Exprmt}^{\text{euf-cma}}_{\mathcal{F},\mathtt{ABS}}(\lambda, \mathcal{U}) : \\
&\quad (\mathrm{MPK}, \mathrm{MSK}) \leftarrow \mathbf{ABS.Setup}(1^\lambda, \mathcal{U}) \\
&\quad ((m^*, f^*), \sigma^*) \leftarrow \mathcal{F}^{\mathcal{ABSKG}, \mathcal{ABSSIGN}}(\mathrm{MPK}) \\
&\quad \text{If } \mathbf{ABS.Vrfy}(\mathrm{MPK}, (m^*, f^*), \sigma^*) = 1 \\
&\quad\quad \text{then Return } \textsc{Win} \\
&\quad \text{else Return } \textsc{Lose}
\end{aligned}
$$

In the experiment, $\mathcal{F}$ issues key-extraction queries to its key-generation oracle $\mathcal{ABSKG}$ and signing queries to its signing oracle $\mathcal{ABSSIGN}$. Giving an attribute set S_i, $\mathcal{F}$ queries $\mathcal{ABSKG}(\mathrm{MPK}, \mathrm{MSK}, \cdot)$ for the secret key $\mathrm{SK}_{\mathrm{id},S_i}$. In addition, giving an attribute set S_j and a pair (m, f) of a message and an access formula, $\mathcal{F}$ queries $\mathcal{ABSSIGN}(\mathrm{MPK}, \mathrm{SK}_{\cdot,\cdot}, (\cdot, \cdot))$ for a signature σ that satisfies $\mathbf{ABS.Vrfy}(\mathrm{MPK}, (m, f), \sigma) = 1$ when $f(S_j) = 1$.

The access formula f^* declared by $\mathcal{F}$ is called a *target access formula*. Here we consider the *adaptive* target in the sense that $\mathcal{F}$ is allowed to choose f^* after seeing MPK and issuing some key-extraction queries and signing queries. In key-extraction queries, S_i that satisfies $f^*(S_i) = 1$ was never queried. In signing queries, (m^*, f^*) was never queried. The number of key-extraction queries and the number of signing queries are at most q_{k} and q_{s} in total, respectively, which are bounded by a polynomial in λ.

The *advantage* of $\mathcal{F}$ over ABS in the game of chosen-message attack to make existential forgery is defined as:

$$\mathbf{Adv}^{\text{euf-cma}}_{\mathcal{F},\mathtt{ABS}}(\lambda) \stackrel{\text{def}}{=} \Pr[\textsc{Win} \leftarrow \mathbf{Exprmt}^{\text{euf-cma}}_{\mathcal{F},\mathtt{ABS}}(\lambda, \mathcal{U})].$$

ABS is called *existentially unforgeable against chosen-message attacks* if, for any PPT $\mathcal{F}$ and for any $\mathcal{U}$, $\mathbf{Adv}^{\text{euf-cma}}_{\mathcal{F},\mathtt{ABS}}(\lambda)$ is negligible in λ.

3 Reputation System Based on Attributes of Ratees

In this section, we define our reputation system based on attributes. In our reputation system we need rater anonymity, traceability, unforgeability and public linkability.

First, we define entities in our reputation system based on attributes of ratees.

System manager is an authority of our reputation system, and is assumed to be honest. It issues the system manager's public key MPK.

Providers provides items for transactions on the underlying network. We don't care in this paper the registration of providers because we assume that they are honest.

Items are things provided by providers.

Users use items and later become *raters* of the items. Given a private key $\mathrm{SK}_{\mathrm{id},S}$, a user is registered by the system manager.

Raters are users who bought an item of a provider.

Attribute universe $\mathcal{U}$ is the set of all possible attributes of ratees. It is required that $\mathcal{U}$ can be updated even after the set up phase by the system manager.

Ratees are items bought by users.

Reputation board is a public board to show reputation information publicly.

Second, we define a scheme of algorithms in our reputation system based on attributes of ratees. Our reputation system based on attributes consists of seven PPT algorithms: (**RS**.**Setup**, **RS**.**KG**, **RS**.**Sign**, **RS**.**Vrfy**, **RS**.**Eval**, **RS**.**Open**, **RS**.**Link**). Entities in Our Reputation System Based on Attributes are as follows.

RS.**Setup**$(1^\lambda, \mathcal{U}) \rightarrow (\mathrm{MPK}, \mathrm{MSK})$: This randomized algorithm is run by the system manager in the setup phase. It executes **ABS**.**Setup**$(\lambda, \mathcal{U})$ to generate the master public key MPK and the master secret MSK.

RS.**KG**$(\mathrm{MPK}, \mathrm{MSK}, \mathrm{id}, S, \mathrm{IDList}) \rightarrow (\mathrm{SK}_{\mathrm{id},S}, \mathrm{IDList})$: This randomized algorithm is run by the system manager in each registration of a user. It executes **ABS**.**KG**$(\mathrm{MPK}, \mathrm{MSK}, S)$ to generate a signing key $\mathrm{SK}_{\mathrm{id},S}$ with ID id attached to the user. It also maintains IDList; id is added in IDList.

RS.**Sign**$(\mathrm{MPK}, \mathrm{SK}_{\mathrm{id},S}, (\mathit{item}, f)) \rightarrow \sigma$: This randomized algorithm is run by a user in each rating. It executes **ABS**.**Sign**$(\mathrm{MPK}, \mathrm{SK}_{\mathrm{id},S}, (\mathit{item}, f))$ to generate a signature σ for the specified *item* which he is going to rate. Note that an *item* is treated as a message in the algorithm **ABS**.**Sign**.

RS.**Vrfy**$(\mathrm{MPK}, (\mathit{item}, f), \sigma) \rightarrow 1/0$: This deterministic algorithm is run by a provider in each verification of a rating to his *item* by a user. It executes **ABS**.**Vrfy**$(\mathrm{MPK}, (\mathit{item}, f), \sigma)$ to obtain the decision 1 or 0 that means whether σ is a valid signature for (item, f) or not.

Correctness should hold: $\Pr[(\mathrm{MPK}, \mathrm{MSK}) \leftarrow \mathbf{RS}.\mathbf{Setup}(1^\lambda, \mathcal{U}), \mathrm{SK}_{\mathrm{id},S} \leftarrow \mathbf{RS}.\mathbf{KG}(\mathrm{MPK}, \mathrm{MSK}, \mathrm{id}, S, \mathrm{IDList}), \sigma \leftarrow \mathbf{RS}.\mathbf{Sign}(\mathrm{MPK}, \mathrm{SK}_{\mathrm{id},S}, (\mathit{item}, f)) : 1 \leftarrow \mathbf{RS}.\mathbf{Vrfy}(\mathrm{MPK}, (\mathit{item}, f), \sigma)] = 1$.

RS.**Eval**$((\mathit{item}, f), (\sigma_i)_i) \rightarrow \mathit{repval}$: This deterministic algorithm is run by the system manager in the phase of evaluating a reputation value on an *item*. It computes a reputation value $\mathit{repval} \in \{f; f : \text{boolean formula on } \mathcal{U}\}$ from ratings $(\sigma_i)_i$ on (item, f).

RS.**Open**$(\mathrm{MPK}, \mathrm{MSK}, (\mathit{item}, f), \sigma) \rightarrow \{\mathrm{id}, \perp\}$: This deterministic algorithm is run by the system manager to open rating; that is, a signature σ. It computes the identity id of the signer or failure $\perp$ on input $(\mathrm{MPK}, \mathrm{MSK}), (\mathit{item}, f), \sigma$.

RS.Link(MPK, $((item, f'), \sigma'), ((item, f''), \sigma'')) \to$ 1/0: This deterministic algorithm can be run by any user to decide whether two ratings, σ' and σ'', were generated by the same user identified by id. It computes the decision 1 or 0 that means whether σ' and σ'' are publicly linkable ratings or not.

3.1 Attacks on a Reputation System Based on Attributes of Ratees

We assume the communication between users and the system manager is via secure channel. Attacks should be considered for properties that a reputation system should have, rater anonymity, traceability, unforgeability, public linkability.

We only describe here an attack against unforgeability. It is basically the same an attack against existential unforgeability of ABS.

$$
\begin{aligned}
&\mathbf{Exprmt}^{\text{euf-cma}}_{\mathcal{F},\mathtt{RS}}(\lambda, \mathcal{U}) :\\
&\quad (\mathrm{MPK}, \mathrm{MSK}) \leftarrow \mathbf{RS}.\mathbf{Setup}(1^\lambda, \mathcal{U})\\
&\quad ((m^*, f^*), \sigma^*) \leftarrow \mathcal{F}^{\mathcal{RSKG}, \mathcal{RSSIGN}}(\mathrm{MPK})\\
&\quad \text{If } \mathbf{RS}.\mathbf{Vrfy}(\mathrm{MPK}, (m^*, f^*), \sigma^*) = 1\\
&\quad\quad \text{then Return } \textsc{Win}\\
&\quad \text{else Return } \textsc{Lose}
\end{aligned}
$$

The *advantage* of $\mathcal{F}$ over RS in the game of chosen-message attack to make existential forgery of a rating is defined as:

$$\mathbf{Adv}^{\text{euf-cma}}_{\mathcal{F},\mathtt{RS}}(\lambda) \stackrel{\text{def}}{=} \Pr[\textsc{Win} \leftarrow \mathbf{Exprmt}^{\text{euf-cma}}_{\mathcal{F},\mathtt{RS}}(\lambda, \mathcal{U})].$$

Definition 1 (Unforgeability) *RS is called existentially unforgeable against chosen-message attacks if, for any PPT $\mathcal{F}$ and for any $\mathcal{U}$,* $\mathbf{Adv}^{euf\text{-}cma}_{\mathcal{F},RS}(\lambda)$ *is negligible in λ.*

4 Our Concrete Construction of Reputation System Based on Attributes of Ratees

In this section, using an ABS scheme of the Fiat-Shamir style [1, 2], we construct a reputation system based on attributes of ratees, concretely. We employ the boolean proof system [2, 1] (App. A).

4.1 Scheme

RS.Setup$(1^\lambda, \mathcal{U}) \to (\mathrm{MPK}, \mathrm{MSK})$: This PPT algorithm chooses, on input 1^λ and $\mathcal{U}$, a pair $(x_{\mathrm{mst}}, w_{\mathrm{mst}})$ at random from $R = \{(x, w)\}$ by running $\mathrm{Inst}_R(1^\lambda)$, where $|x|$ and $|w|$ are bounded by a polynomial in λ. It also chooses a hash key μ at random from a hash-key space $Hashkeysp(\lambda)$. It outputs a public key $\mathrm{MPK} = (x_{\mathrm{mst}}, \mathcal{U}, \mu)$ and a master secret key $\mathrm{MSK} = (w_{\mathrm{mst}})$.

$$
\begin{aligned}
&\mathbf{RS}.\mathbf{Setup}(1^\lambda, \mathcal{U}) :\\
&\quad (x_{\mathrm{mst}}, w_{\mathrm{mst}}) \leftarrow \mathrm{Inst}_R(1^\lambda), \mu \leftarrow Hashkeysp(\lambda)\\
&\quad \mathrm{MPK} := (x_{\mathrm{mst}}, \mu), \mathrm{MSK} := (w_{\mathrm{mst}})\\
&\quad \mathrm{Return}(\mathrm{MPK}, \mathrm{MSK})
\end{aligned}
$$

RS.KG$(\mathrm{MPK}, \mathrm{MSK}, \mathrm{id}, S, \mathrm{IDList}) \to (\mathrm{SK}_{\mathrm{id},S}, \mathrm{IDList})$: This PPT algorithm chooses, on input MPK, MSK, S, a PRF key k from $PRFkeysp(\lambda)$ at random and a random string τ from $\{1,0\}^\lambda$ at random. Then KG applies the credential bundle technique [13, 14] for each message $m_i := (\tau \parallel i), i \in S$. Here we employ the Fiat-Shamir signing algorithm $\mathrm{FS}(\mathbf{\Sigma})^{\mathrm{sign}}$.

$$
\begin{aligned}
&\mathbf{RS}.\mathbf{KG}(\mathrm{MPK}, \mathrm{MSK}, \mathrm{id}, S, \mathrm{IDList}) :\\
&\quad k \leftarrow PRFkeysp(\lambda), \mathrm{id} := \tau \leftarrow \{1, 0\}^\lambda\\
&\quad \text{For } i \in S :\\
&\quad\quad m_i := (\tau \parallel i), a_i \leftarrow \mathbf{\Sigma}^2(x_{\mathrm{mst}}, w_{\mathrm{mst}})\\
&\quad\quad c_i \leftarrow Hash_\mu(a_i \parallel m_i), w_i \leftarrow \mathbf{\Sigma}^3(x_{\mathrm{mst}}, w_{\mathrm{mst}}, a_i, c_i)\\
&\quad \mathrm{SK}_{\mathrm{id},S} := (k, \tau, (a_i, w_i)_{i \in S}),\ \mathrm{IDList} := \mathrm{IDList} \parallel \mathrm{id}\\
&\quad \mathrm{Return}\ (\mathrm{SK}_{\mathrm{id},S}, \mathrm{IDList}).
\end{aligned}
$$

The algorithm **RS.Sign** uses a supplementation algorithm **Supp** and a statement-generator algorithm **StmtGen**.

Supp$(\mathrm{MPK}, \mathrm{SK}_{\mathrm{id},S}, f)$. This PPT algorithm runs for j, $1 \le j \in \mathrm{arity}(f)$, and generates simulated keys (a_{i_j}, w_{i_j}) for $i_j \notin S$.

$$
\begin{aligned}
&\mathbf{Supp}(\mathrm{MPK}, \mathrm{SK}_{\mathrm{id},S}, f) :\\
&\quad \text{For } j = 1 \text{ to arity}(f) :\\
&\quad\quad \text{If } i_j \notin S, \text{ then}\\
&\quad\quad\quad m_{i_j} := (\tau \parallel i_j), c_{i_j} \leftarrow PRF_k(m_{i_j} \parallel 0)\\
&\quad\quad\quad (a_{i_j}, w_{i_j}) \leftarrow \mathbf{\Sigma}^{\mathrm{sim}}(x_{\mathrm{mst}}, c_{i_j}; PRF_k(m_{i_j} \parallel 1))\\
&\quad \text{Return } (a_{i_j}, w_{i_j})_{1 \le j \le \mathrm{arity}(f)}
\end{aligned}
$$

StmtGen(MPK, τ, $(a_{i_j})_{1\le j\le \mathrm{arity}(f)}$):
This PPT algorithm generates, for each j, $1 \le j \in \mathrm{arity}(f)$, a statement x_{i_j}. Note that we employ here the algorithm $\boldsymbol{\Sigma}^{\mathrm{stmtgen}}$ which is associated with $\boldsymbol{\Sigma}$, and whose existence is assured by our assumption.

$$
\begin{aligned}
&\mathbf{StmtGen}(\mathrm{MPK}, \tau, (a_{i_j})_{1\le j\le \mathrm{arity}(f)}) :\\
&\quad \text{For } j = 1 \text{ to arity}(f) :\\
&\qquad m_{i_j} := (\tau \parallel i_j), c_{i_j} \leftarrow \mathit{Hash}_{\mu}(a_{i_j} \parallel m_{i_j})\\
&\qquad x_{i_j} \leftarrow \boldsymbol{\Sigma}^{\mathrm{stmtgen}}(x_{\mathrm{mst}}, a_{i_j}, c_{i_j})\\
&\quad \text{Return } (x_{i_j})_{1\le j\le \mathrm{arity}(f)}
\end{aligned}
$$

Note that $(x_i, w_i) \in R$ for $i \in S$ but $\Pr[(x_i, w_i) \in R] = \mathrm{neg}(\lambda)$ for $i \notin S$.
RS.**Sign**(MPK, $\mathrm{SK}_{\mathrm{id},S}$, (item, f)) $\to \sigma$: This PPT algorithm is obtained by adding **Supp** and **StmtGen** to $\boldsymbol{\Sigma}^3$.

$$
\begin{aligned}
&\mathbf{Supp}(\mathrm{MPK}, \mathrm{SK}_{\mathrm{id},S}, f) \to (a_{i_j}, w_{i_j})_{1\le j\le \mathrm{arity}(f)}\\
&w := (w_{i_j})_{1\le j\le \mathrm{arity}(f)}\\
&\mathbf{StmtGen}(\mathrm{MPK}, \tau, (a_{i_j})_{1\le j\le \mathrm{arity}(f)})\\
&\quad \to (x_{i_j})_{1\le j\le \mathrm{arity}(f)} =: x
\end{aligned}
$$

The above procedures are needed to input a pair of statement and witness, $(x = (x_{i_j})_{1\le j\le \mathrm{arity}(f)}, w = (w_{i_j})_{1\le j\le \mathrm{arity}(f)})$, to $\boldsymbol{\Sigma}^1_f$. Note here that $(x_{i_j}, w_{i_j}) \in R$ for any $i_j \in S$. On the other hand, $(x_{i_j}, w_{i_j}) \notin R$ for any $i_j \notin S$, without a negligible probability, $\mathrm{neg}(\lambda)$.

Therefore, the message on the first move has to include not only commitments $(\mathrm{CMT}_l)_{l\in \mathrm{Leaf}(\mathcal{T}_f)}$ but also a string τ and elements $(a_{i_j})_{1\le j\le \mathrm{arity}(f)}$ for the verifier $\mathcal{V}$ to be able to produce the same statement x.

Hence a rating, that is, a signature, is $\sigma := (\tau, (a_{i_j})_{1\le j\le \mathrm{arity}(f)}, (\mathrm{CMT}_l)_l, (\mathrm{CHA}_n)_n, (\mathrm{RES}_l)_l)$.
RS.**Vrfy**(MPK, $(\mathit{item}, f), \sigma$) $\to 1/0$: This deterministic algorithm utilizes **StmtGen** and $\boldsymbol{\Sigma}^{\mathrm{vrfy}}_f$ to check validity of the pair of message and access formula, (m, f), and the signature σ, under the public key MPK.
RS.**Eval**($(\mathit{item}, f), (\sigma_i)_i$) $\to$ *repval*: This deterministic algorithm counts the number cnt of σ_i each of which has a different tag τ. It returns (f, cnt).
RS.**Open**(MPK, MSK, $(\mathit{item}, f), \sigma$) $\to \{\mathrm{id}, \perp\}$: This deterministic algorithm searches, in IDList, id that is in σ as a tag τ, and returns id. If it finds no such id, it returns $\perp$.
RS.**Link**(MPK, $((\mathit{item}, f'), \sigma'), ((\mathit{item}, f''), \sigma'')$) $\to 1/0$: This deterministic algorithm decides whether two tags, τ' and τ'', are the same or not. If so, then it returns 1 and otherwise, 0.

4.2 Security

Security is discussed for each properties that a reputation system should have.

Theorem 1 (Rater Anonymity) *Our reputation system* `RS` *has rater anonymity.*

Proof. The employed ABS scheme, `ABS`, has anonymity for signers. Therefore, our reputation system `RS` has rater anonymity. □

Theorem 2 (Traceability) *Our reputation system* `RS` *has rater traceability.*

Proof. Any signature σ of the employed ABS scheme, `ABS`, has a tag τ. The tag τ is a part of the secret key $\mathrm{SK}_{\mathrm{id},S}$ given by the system manager to the user who made the signature σ. So, the system manager can identify the user by σ. Therefore, `RS` has rater traceability. □

Theorem 3 (Unforgeability) *Our reputation system* `RS` *has unforgeability in the random oracle model.*

Proof. The employed ABS scheme, `ABS`, is existentially unforgeable in the random oracle model [1, 2]. Therefore, our reputation system `RS` has unforgeability in the random oracle model. □

Theorem 4 (Public Linkability) *Our reputation system* `RS` *has public linkability.*

Proof. Any signature σ of the employed ABS scheme, `ABS`, has a tag τ. The tag τ is a part of the secret key $\mathrm{SK}_{\mathrm{id},S}$ given by the system manager to the user who made the signature σ. So, two signatures, σ_1 and σ_2, generated by the same user using a single $\mathrm{SK}_{\mathrm{id},S}$, can be publicly identified that σ_1 and σ_2 was generated by the same user. Therefore, `RS` has public linkability. □

5 Application to Scoring Board

In this section, we discuss what we have done by providing a reputation system based on attributes of ratees.

A critical example is the following. Let a boolean formula over attributes of a ratee is:
$f = [[\text{price is cheaper}] \wedge [\text{quality is normal}]$
$\vee[[\text{price is higher}] \wedge [\text{quality is good}]$. We can consider the formula that the price balances with quality.

6 Conclusions

In this paper, we defined a reputation system based on attributes of ratees. We used as an individual rating an attribute-based signature (ABS) on a boolean formula that told about attributes of ratees. We made the reputation function take as an input those signatures. Then, using an ABS scheme of the Fiat-Shamir style, we constructed the reputation system concretely.

参考文献

[1] H. Anada, S. Arita, and K. Sakurai. Attribute-based signatures without pairings by the fiat-shamir transformation. *IACR Cryptology ePrint Archive*, 2014:567, 2014.

[2] H. Anada, S. Arita, and K. Sakurai. Attribute-based signatures without pairings via the fiat-shamir paradigm. In *ASIAPKC'14, Proceedings of the 2nd ACM Wookshop on ASIA Public-Key Cryptography, June 3, 2014, Kyoto, Japan*, pages 49–58, 2014.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] H. K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures. *IACR Cryptology ePrint Archive*, 2010:595, 2010.

[14] H. K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures. In *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, pages 376–392, 2011.

[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.

A Boolean Proof System [2]

Basically, a boolean proof system (by Anada et al. [1, 2]) $\mathbf{\Sigma}_f$ is a 3-move protocol between interactive PPT algorithms $\mathcal{P}$ and $\mathcal{V}$ on initial input $(x := (x_{i_j})_{1\le j\le \mathrm{arity}(f)}, w := (w_{i_j})_{1\le j\le \mathrm{arity}(f)}) \in R_f$ for $\mathcal{P}$ and x for $\mathcal{V}$ (Fig. 1).

It is shown [1] that their boolean proof system $\mathbf{\Sigma}_f$ is certainly a Σ-protocol.

$$
\begin{array}{lcl}
\mathcal{P}(x,w,f): & & \mathcal{V}(x,f): \\
\quad \mathbf{\Sigma}_f^{\mathrm{eval}}(\mathcal{T}_f,S)\to(v_n)_n & & \\
 & & \\
\quad \text{If } v_{r(\mathcal{T}_f)}\neq 1,\text{ then abort} & & \\
\quad \text{else } \textsc{Cha}_{r(\mathcal{T}_f)}:=*,\eta\xleftarrow{\$}\mathbb{Z} & & \\
\quad\quad \mathbf{\Sigma}_f^1(x,w,\mathcal{T}_f,(v_n)_n,\textsc{Cha}_{r(\mathcal{T}_f)}) & & \\
\quad\quad \to((\textsc{Cmt}_l)_l,(\textsc{Cha}_n)_n,(\textsc{Res}_l)_l) & \xrightarrow{(\textsc{Cmt}_l)_l} & \\
 & & \\
\quad\quad \textsc{Cha}_{r(\mathcal{T}_f)}:=\textsc{Cha} & \xleftarrow{\textsc{Cha}} & \textsc{Cha}\leftarrow\mathbf{\Sigma}_f^2(1^\lambda) \\
\quad\quad \mathbf{\Sigma}_f^3(x,w,\mathcal{T}_f,(v_n)_n, & & \\
\quad\quad\quad (\textsc{Cmt}_l)_l,(\textsc{Cha}_n)_n,(\textsc{Res}_l)_l) & & \mathbf{\Sigma}_f^{\mathrm{vrfy}}(x,\mathcal{T}_f,\textsc{Cha}, \\
\quad\quad \to((\textsc{Cha}_l)_l,(\textsc{Res}_l)_l) & \xrightarrow{(\textsc{Cha}_l)_l,(\textsc{Res}_l)_l} & \quad(\textsc{Cmt}_l)_l,(\textsc{Cha}_l)_l,(\textsc{Res}_l)_l) \\
 & & \to b,\text{Return } b
\end{array}
$$

$\mathbf{\Sigma}_f^1(x,w,\mathcal{T},(v_n)_n,\textsc{Cha}):$
$\quad\mathcal{T}_{\mathrm{L}}:=\mathrm{Lsub}(\mathcal{T}),\mathcal{T}_{\mathrm{R}}:=\mathrm{Rsub}(\mathcal{T})$
$\quad$If $\quad r(\mathcal{T})$ is $\wedge$-node, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}:=\textsc{Cha},\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=\textsc{Cha}$
$\quad\quad\mathrm{Return}(\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})},\mathbf{\Sigma}_f^1(x,w,\mathcal{T}_{\mathrm{L}},(v_n)_n,\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}),\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})},\mathbf{\Sigma}_f^1(x,w,\mathcal{T}_{\mathrm{R}},(v_n)_n,\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}))$
$\quad$else if $r(\mathcal{T})$ is $\vee$-node, then
$\quad\quad$If $\quad v_{r(\mathcal{T}_{\mathrm{L}})}=1\wedge v_{r(\mathcal{T}_{\mathrm{R}})}=1$, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}:=*,\quad \textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=*$
$\quad\quad$else if $v_{r(\mathcal{T}_{\mathrm{L}})}=1\wedge v_{r(\mathcal{T}_{\mathrm{R}})}=0$, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}:=*,\quad \textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}\leftarrow\mathbf{\Sigma}^2(1^\lambda)$
$\quad\quad$else if $v_{r(\mathcal{T}_{\mathrm{L}})}=0\wedge v_{r(\mathcal{T}_{\mathrm{R}})}=1$, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}\leftarrow\mathbf{\Sigma}^2(1^\lambda),\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=*$
$\quad\quad$else if $v_{r(\mathcal{T}_{\mathrm{L}})}=0\wedge v_{r(\mathcal{T}_{\mathrm{R}})}=0$, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}\leftarrow\mathbf{\Sigma}^2(1^\lambda),\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=\textsc{Cha}\oplus\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}$
$\quad\quad\mathrm{Return}(\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})},\mathbf{\Sigma}_f^1(x,w,\mathcal{T}_{\mathrm{L}},(v_n)_n,\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}),\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})},\mathbf{\Sigma}_f^1(x,w,\mathcal{T}_{\mathrm{R}},(v_n)_n,\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}))$
$\quad$else if $r(\mathcal{T})$ is a leaf-node, then
$\quad\quad$If $\quad v_{r(\mathcal{T})}=1$, then $\textsc{Cmt}_{r(\mathcal{T})}\leftarrow\mathbf{\Sigma}^1(x_{\rho(r(\mathcal{T}))},w_{\rho(r(\mathcal{T}))}),\textsc{Res}_{r(\mathcal{T})}:=*$
$\quad\quad$else if $v_{r(\mathcal{T})}=0$, then $(\textsc{Cmt}_{r(\mathcal{T})},\textsc{Res}_{r(\mathcal{T})})\leftarrow\mathbf{\Sigma}^{\mathrm{sim}}(x_{\rho(r(\mathcal{T}))},\textsc{Cha})$
$\quad\quad\mathrm{Return}(\textsc{Cmt}_{r(\mathcal{T})},\textsc{Res}_{r(\mathcal{T})})$

$$\mathbf{\Sigma}_f^2(1^\lambda):\textsc{Cha}\leftarrow\mathbf{\Sigma}^2(1^\lambda),\mathrm{Return}(\textsc{Cha})$$

$\mathbf{\Sigma}_f^3(x,w,\mathcal{T},(v_n)_n,(\textsc{Cmt}_l)_l,(\textsc{Cha}_n)_n,(\textsc{Res}_l)_l):$
$\quad\mathcal{T}_{\mathrm{L}}:=\mathrm{Lsub}(\mathcal{T}),\mathcal{T}_{\mathrm{R}}:=\mathrm{Rsub}(\mathcal{T})$
$\quad$If $\quad r(\mathcal{T})$ is $\wedge$-node, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}:=\textsc{Cha},\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=\textsc{Cha}$
$\quad\quad\mathrm{Return}(\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})},\mathbf{\Sigma}_f^3(x,w,\mathcal{T}_{\mathrm{L}},(v_n)_n,(\textsc{Cmt}_l)_l,(\textsc{Cha}_n)_n,(\textsc{Res}_l)_l),\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})},\mathbf{\Sigma}_f^3(x,w,\mathcal{T}_{\mathrm{R}},(v_n)_n,(\textsc{Cmt}_l)_l,(\textsc{Cha}_n)_n,(\textsc{Res}_l)_l))$
$\quad$else if $r(\mathcal{T})$ is $\vee$-node, then
$\quad\quad$If $\quad v_{r(\mathcal{T}_{\mathrm{L}})}=1\wedge v_{r(\mathcal{T}_{\mathrm{R}})}=1$, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}\leftarrow\mathbf{\Sigma}^2(1^\lambda),\quad \textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=\textsc{Cha}\oplus\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}$
$\quad\quad$else if $v_{r(\mathcal{T}_{\mathrm{L}})}=1\wedge v_{r(\mathcal{T}_{\mathrm{R}})}=0$, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}:=\textsc{Cha}\oplus\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})},\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}$
$\quad\quad$else if $v_{r(\mathcal{T}_{\mathrm{L}})}=0\wedge v_{r(\mathcal{T}_{\mathrm{R}})}=1$, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}:=\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})},\quad \textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=\textsc{Cha}\oplus\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}$
$\quad\quad$else if $v_{r(\mathcal{T}_{\mathrm{L}})}=0\wedge v_{r(\mathcal{T}_{\mathrm{R}})}=0$, then $\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}:=\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})},\quad \textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}:=\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})}$
$\quad\quad\mathrm{Return}(\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})},\mathbf{\Sigma}_f^3(x,w,\mathcal{T}_{\mathrm{L}},(v_n)_n,(\textsc{Cmt}_l)_l,(\textsc{Cha}_n)_n,(\textsc{Res}_l)_l),\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})},\mathbf{\Sigma}_f^3(x,w,\mathcal{T}_{\mathrm{R}},(v_n)_n,(\textsc{Cmt}_l)_l,(\textsc{Cha}_n)_n,(\textsc{Res}_l)_l))$
$\quad$else if $r(\mathcal{T})$ is a leaf-node, then
$\quad\quad$If $\quad v_{r(\mathcal{T})}=1$, then $\textsc{Res}_{r(\mathcal{T})}\leftarrow\mathbf{\Sigma}^3(x_{\rho(r(\mathcal{T}))},w_{\rho(r(\mathcal{T}))},\textsc{Cmt}_{r(\mathcal{T})},\textsc{Cha})$
$\quad\quad$else if $v_{r(\mathcal{T})}=0$, then $\textsc{Res}_{r(\mathcal{T})}\leftarrow\textsc{Res}_{r(\mathcal{T})}$
$\quad\quad\mathrm{Return}(\textsc{Res}_{r(\mathcal{T})})$

$\mathbf{\Sigma}_f^{\mathrm{vrfy}}(x,\mathcal{T},\textsc{Cha},\textsc{Cmt}_l)_l,(\textsc{Cha}_l)_l,(\textsc{Res}_l)_l):\mathrm{Return}(\mathbf{VrfyCha}(\mathcal{T},\textsc{Cha},(\textsc{Cha}_l)_l)\wedge\mathbf{VrfyRes}(x,\mathcal{T},(\textsc{Cmt}_l,\textsc{Cha}_l,\textsc{Res}_l)_l))$
$\mathbf{VrfyCha}(\mathcal{T},\textsc{Cha},(\textsc{Cha}_l)_l):$
$\quad\mathcal{T}_{\mathrm{L}}:=\mathrm{Lsub}(\mathcal{T}),\mathcal{T}_{\mathrm{R}}:=\mathrm{Rsub}(\mathcal{T})$
$\quad$If $r(\mathcal{T})$ is an $\wedge$-node,
$\quad\quad$then Return $((\textsc{Cha}\stackrel{?}{=}\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})})\wedge(\textsc{Cha}\stackrel{?}{=}\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})})\wedge\mathbf{VrfyCha}(\mathcal{T}_{\mathrm{L}},\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})},(\textsc{Cha}_l)_l)\wedge\mathbf{VrfyCha}(\mathcal{T}_{\mathrm{R}},\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})},(\textsc{Cha}_l)_l))$
$\quad$else if $r(\mathcal{T})$ is an $\vee$-node,
$\quad\quad$then Return $((\textsc{Cha}\stackrel{?}{=}\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})}\oplus\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})})\wedge\mathbf{VrfyCha}(\mathcal{T}_{\mathrm{L}},\textsc{Cha}_{r(\mathcal{T}_{\mathrm{L}})},(\textsc{Cha}_l)_l)\wedge\mathbf{VrfyCha}(\mathcal{T}_{\mathrm{R}},\textsc{Cha}_{r(\mathcal{T}_{\mathrm{R}})},(\textsc{Cha}_l)_l))$
$\quad$else if $r(\mathcal{T})$ is a leaf node,
$\quad\quad$then Return $(\textsc{Cha}\stackrel{?}{\in}\textsc{ChaSp}(1^\lambda))$
$\mathbf{VrfyRes}(x,\mathcal{T},(\textsc{Cmt}_l,\textsc{Cha}_l,\textsc{Res}_l)_l):$
$\quad$For $l\in\mathrm{Leaf}(\mathcal{T})$: If $\mathbf{\Sigma}^{\mathrm{vrfy}}(x_{\rho(l)},\textsc{Cmt}_l,\textsc{Cha}_l,\textsc{Res}_l)=0$, then Return (0)
$\quad$Return (1)

図 1: Boolean proof system $\mathbf{\Sigma}_f$ [1, 2].