Kripke semantics for Epistemic Logic of Relational Information between Ciphertexts

Shigeki Hagihara[1], Hiroaki Oguro[2], Naoki Yonezaki[1]

[1]Department of Computer Science
Graduate School of Information Science and Engineering
Tokyo Institute of Technology

{hagihara, yonezaki}@fmx.cs.titech.ac.jp

[2]IT Security Business Section
System Platforms Sector
NTT DATA Corporation

ogurohr@nttdata.co.jp

ABSTRACT

By configuring an adequate set of messages obtained by an adversary and analyzing the information which can be obtained by an adversary, it is possible to verify the secrecy of cryptography protocols. We have already proposed a deduction system for analyzing whether an adversary can obtain relational information between contents or keys of two ciphertexts, such as "the contents of two ciphertexts are equal" or "the keys of two ciphertexts are different". We have also proposed the semantics of this system. In the semantics, acquisition of relational information by an adversary is intuitionistically defined as his ability to show the evidence to succeed in obtaining the information. In this paper, we reconsider the deduction system as a kind of epistemic logic, and give Kripke semantics for the system. In Kripke semantics, acquisition of relational information by an adversary can be naturally defined as his knowledge of relational information. We also make a comparison between the two semantics.

Keywords

Epistemic Logic, Kripke semantics, Relational Information between Ciphertexts, Security Protocol Analysis

1. INTRODUCTION

Recently, communication networks have become highly developed and various types of information are flowing through these networks. Much of this is confidential information which should not be revealed to other persons, e.g. passwords for authentication, privacy of individual, etc. Usually, this kind of information is communicated with cryptography. Even if cryptography is perfect, confidential information may possibly be revealed to an adversary if he uses an impersonation attack. To prevent such attacks and ensure the security of network communication, security protocols themselves should be secure. In order to confirm this, we require verification methods for security protocols.

There are many works of verification methods, which analyze security properties such as secrecy, authenticity, privacy, etc. Among these properties, it is possible to verify secrecy, by configuring an adequate set of messages obtained by an adversary, analyzing the information which can be obtained by the adversary, and checking whether or not confidential information is included in such information.

In [2], we proposed a deduction system for analyzing whether an adversary can obtain relational information between contents or keys of two ciphertexts, such as "the contents of two ciphertexts are equal" or "the keys of two ciphertexts are different". In [8], we also proposed semantics for the subsystem of the deduction system proposed in [2], and showed the completeness of the subsystem for the semantics. In this semantics, acquisition of relational information by an adversary is intuitionistically defined as his ability to show the evidence to succeed in obtaining the information. In this paper, we reconsider the deduction system as a kind of epistemic logic, and give the Kripke semantics for the system. In Kripke semantics, acquisition of relational information by an adversary can be naturally defined as his knowledge of relational information. We also make a comparison between the two semantics, and show that if a formula is satisfied in intuitionistic semantics, it is also satisfied in Kripke semantics. This means that the subsystem proposed in [8] satisfies soundness for the Kripke semantics.

This paper is organized as follows. First, in Sect.2 we define a syntax of a logic which is an extended version of deduction system in [8]. In Sect.3, we give Kripke semantics for the logic. In Sect.4, we give intuitionistic semantics which is

an abstract version of the semantics proposed in [8], and make a comparison between the two semantics in Sect.5. In Sect.6, we discuss the relation between other works and ours. Finally, we conclude our results in Sect.7.

2. SYNTAX OF EPISTEMIC LOGIC OF RELATIONAL INFORMATION BETWEEN CIPHERTEXTS

In this paper, we propose a logic for analyzing whether or not an adversary can recognize relational information between two ciphertexts regarding their content or their keys,. In this section, we define the syntax for the logic.

2.1 Symbols

We first define symbols for representing messages as follows.

- $\mathcal{K}$: a set of symbols representing symmetric keys.
- $\mathcal{I}$: a set of symbols representing public messages.
- $\mathcal{N}$: a set of symbols representing secret messages.
- $\mathcal{R} = \mathcal{R}_{hon} \cup \mathcal{R}_{adv}$: a set of symbols representing random numbers which are used in encryption.
  - $\mathcal{R}_{hon}$: a set of symbols representing random numbers which are used by honest principals.
  - $\mathcal{R}_{adv}$: a set of symbols representing random numbers which are used by an adversary.

2.2 Messages and Extended Messages

The set of messages are inductively defined as follows.

1. $K \in \mathcal{K}$ is a message.
2. $I \in \mathcal{I}$ is a message.
3. $N \in \mathcal{N}$ is a message.
4. If T_1 and T_2 are messages, (T_1, T_2) is a message.
5. If T is a message, $K \in \mathcal{K}$ and $R \in \mathcal{R}$, then $\{T\}_K^R$ is a message.

(T_1, T_2) is a pair of T_1 and T_2. $\{T\}_K^R$ is an encryption of T under K, where R is a symbol representing random numbers which are used in encryption. We say $\{T\}_K^R$ is an encrypted message.

EXAMPLE 1. *We encrypt a pair of I and K_2 under a key K_1, and then we encrypt it under a key K_3. The result is represented as the message $\{\{(I, K_2)\}_{K_1}^R\}_{K_3}^{R'}$.*

We extend the syntax of messages and refer to the contents of encrypted messages and keys which are used in encryption. The set of extended messages is inductively defined as follows.

1. A message T is an extended message.
2. If E is an extended message, *content_of*(E) and *key_of*(E) are also extended messages.

If E represents an encrypted message, *content_of*(E) and *key_of*(E) are intended to represent its contents and a key which is used in encryption for E, respectively. If E does not represent an encrypted message, these are intended to be undefined.

We use meta-variables $T, T_1, T_2, \ldots$ for messages, and meta-variables $E, E_1, E_2, \ldots$ for extended messages.

2.3 Formulae

By using extended messages, we define the syntax of formulae. Using formulae, we can refer to the constructability of messages, and equality and non-equality of contents or keys of ciphertexts. Furthermore, we can refer to an adversary's knowledge about these facts. The set of formulae are inductively defined as follows.

1. If T_1, T_2 are messages, $T_1 \geqslant T_2$ is a formula.
2. If E_1, E_2 are extended messages, $E_1 \equiv E_2$ and $E_1 \not\equiv E_2$ are formulae.
3. If φ_1, φ_2 are formulae, $\varphi_1 \wedge \varphi_2, \neg\varphi_1$ are formulae.
4. If T is a message and φ is a formula, $T \triangleright \varphi$ is a formula.

$T_1 \geqslant T_2$ represents that the value of T_2 can be generated from the value of T_1. $E_1 \equiv E_2$ represents that the values of E_1 and E_2 are defined and these values are equal. $E_1 \not\equiv E_2$ represents that the values of E_1 and E_2 are defined and these values are not equal [1]. $\varphi_1 \wedge \varphi_2$ and $\neg\varphi_1$, represent that both φ_1 and φ_2 hold and that φ_1 does not hold, respectively. $T \triangleright \varphi$ represents that an adversary having the value of T can recognize that φ holds. We say $T \triangleright \varphi$ is a modal formula.

We also use the notation $\varphi_1 \vee \varphi_2$ and $\varphi_1 \rightarrow \varphi_2$ as abbreviations for $\neg(\neg\varphi_1 \wedge \neg\varphi_2)$, $\neg(\varphi_1 \wedge \neg\varphi_2)$, respectively.

EXAMPLE 2. *Let T, T_1, T_2 be messages.*

- *content_of*$(T_1) \equiv T_2$ *is a formula representing that T_1 is an encrypted message and the value of contents of T_1 is equal to the value of T_2.*
- *key_of*$(T_1) \not\equiv$ *key_of*(T_2) *is a formula representing that T_1 and T_2 are encrypted messages and the values of keys which are used in T_1 and T_2 are different.*
- $T \triangleright$ *content_of*$(T_1) \equiv T_2$ *is a modal formula representing that an adversary having the value of T recognizes that T_1 is an encrypted message and the value of the contents of T_1 is equal to the value of T_2.*
- $T \triangleright$ *key_of*$(T_1) \not\equiv$ *key_of*(T_2) *is a modal formula representing that an adversary having the value of T recognizes that T_1 and T_2 are encrypted messages and the values of keys which are used in T_1 and T_2 are different.*

[1]The formula $E_1 \not\equiv E_2$ is syntactically different from the formula $\neg(E_1 \equiv E_2)$. In the semantics defined in Sect.3, interpretation of these two formulae are different.

3. KRIPKE SEMANTICS

In this section, we give an interpretation of messages, extended messages, and formulae defined in Sect.2. In order to interpret modal formulae, we use Kripke semantics. Generally, Kripke semantics are widely used as semantics for modal logic including epistemic logic. In Kripke semantics for epistemic logic, various situations are regarded as possible worlds. An observer's recognition of a fact is interpreted as that the fact holds in all the situations (possible worlds) which are indistinguishable from the current situation (the current possible world) by the observer. In this paper, we give a similar interpretation.

We give an interpretation for messages, extended messages and formulae in Sect.3.1, Sect.3.2 and Sect.3.3, respectively. In Sect.3.4, we give examples for interpretation of several formulae, mainly including modal formulae.

3.1 Interpretation of Messages

A message is interpreted using message algebra.

3.1.1 Message Algebra

Message algebra is defined by $\mathcal{A} = \langle A_{key}, A_{pub}, A_{sec}, A_{ct}, A_{pair}, R_{hon}, R_{adv}, pair, enc\rangle$, where A_{key} is a set of key data, A_{pub} is a set of public data, A_{sec} is a set of secret data, A_{ct} is a set of ciphertext data, A_{pair} is a set of pair data. R_{hon} and R_{adv} are sets of random data used in encryption by honest principals and adversaries, respectively. We say $A = A_{key} \cup A_{pub} \cup A_{sec} \cup A_{ct} \cup A_{pair}$ is a set of message data. $pair : A \times A \rightarrow A_{pair}$ is a pairing function which takes two items of message data as input, and returns a pair of data items as output. $enc : A \times A_{key} \times (R_{hon} \cup R_{adv}) \rightarrow A_{ct}$ is an encryption function which takes an item of message data, an item of key data and an item of random data as inputs, and outputs resulting ciphertext data.

Furthermore, $A_{key}, A_{pub}, A_{sec}, A_{ct}, A_{pair}$ are disjointed, which means that an item of message data is uniquely determined what kind of message data it is.

Furthermore, *pair* and *enc* are bijective, i.e. the following properties hold:

- $\forall d_1, d_2, d_3, d_4 \in A\ (pair(d_1, d_2) = pair(d_3, d_4) \Rightarrow d_1 = d_3 \wedge d_2 = d_4)$,
  $\forall d \in A_{pair} \exists d', d'' \in A\ (d = pair(d', d''))$,
- $\forall d, d' \in A \forall k, k' \in A_{key} \forall r, r' \in R_{hon} \cup R_{adv}\ (enc(d, k, r) = enc(d', k', r') \Rightarrow d = d' \wedge k = k' \wedge r = r')$,
  $\forall d \in A_{ct} \exists d' \in A, \exists k' \in A_{key} \exists r' \in R_{hon} \cup R_{adv}\ (d = enc(d', k', r'))$.

Let U be a set of message data. Then, the closure $cl(U)$ of U is the smallest set X of message data which satisfies the following.

- $U \subseteq X$
- $A_{pub} \subseteq X$
- $d_1, d_2 \in X \Rightarrow pair(d_1, d_2) \in X$
- $pair(d_1, d_2) \in X \Rightarrow d_1, d_2 \in X$
- $d, k \in X, k \in A_{key}, r \in R_{adv} \Rightarrow enc(d, k, r) \in X$
- $enc(d, k, r), k \in X \Rightarrow d \in X$

Intuitively, $cl(U)$ represents the set of message data which can be constructed by an adversary by using U.

3.1.2 Interpretation of Messages

Let $\mathcal{A} = \langle A_{key}, A_{pub}, A_{sec}, A_{ct}, A_{pair}, R_{hon}, R_{adv}, pair, enc\rangle$ be a message algebra, m be an assignment which assigns message data or random data of an appropriate type to message symbols and random number symbols as follows:

- key data in A_{key} are assigned to key symbols in $\mathcal{K}$,
- public data in A_{pub} are assigned to public message symbols in $\mathcal{I}$,
- secret data in A_{sec} are assigned to secret message symbols in $\mathcal{N}$,
- random data in R_{hon} are assigned to random number symbols in $\mathcal{R}_{hon}$,
- random data in R_{adv} are assigned to random number symbols in $\mathcal{R}_{adv}$,

where m assigns different data to different symbols [2].

By using $\mathcal{A}$ and m, we define interpretation $[\![T]\!]_{\mathcal{A},m}$ of a message T as follows.

- $[\![K]\!]_{\mathcal{A},m} = m(K)$
- $[\![I]\!]_{\mathcal{A},m} = m(I)$
- $[\![N]\!]_{\mathcal{A},m} = m(N)$
- $[\![(T_1, T_2)]\!]_{\mathcal{A},m} = pair([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m})$
- $[\![\{T\}_K^R]\!]_{\mathcal{A},m} = enc([\![T]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))$

3.2 Interpretation of Extended Messages

In this section, we give an interpretation for extended messages. In extended messages, we can refer to contents or keys which are used in the encryption of encrypted messages. Even if an adversary has an encrypted message, if he does not have its key, he cannot understand either what its content is or what its key is. In order to formalize such an aspect, in Sect.3.2.1 we define permutation (called reinterpretation) on the set of message data, which maps ciphertext data into ciphertext data indistinguishable from it. A reinterpretation of message data in a situation results in

[2] It is possible to define interpretation without the constraint 'm assigns different data to different symbols'. Even if we does not adopt this constraint, theorem 1 stated in Sect.5 holds. In Sect.5, we will state that the deduction system proposed in [8] is sound for this Kripke semantics. Since the soundness of this deduction system requires the constraint 'm to assign different data to different symbols', we include the constraint about m.

another situation which is indistinguishable by the adversary from the original situation. Various reinterpretations produce various situations which are indistinguishable from the original one, and such situations are regarded as possible worlds. This kind of method defining possible worlds by using reinterpretation was used in [5], to propose Kripke semantics of epistemic logic for privacy verification of security protocols. In this paper, we modify this method to adapt it to the epistemic logic of relational information between ciphertexts. By using reinterpretation, we give interpretation of extended messages in Sect.3.2.2.

3.2.1 Reinterpretation for message data

Let $U \subseteq A$ be a set of message data which an adversary has. Then, a permutation π on A (a bijection from A to A) is called semi-reinterpretation under U if π satisfies the following conditions 1-5.

1. $d \in A_{key} \cup A_{pub} \cup A_{sec} \Rightarrow \pi(d) = d$
2. $\pi(pair(d_1, d_2)) = pair(\pi(d_1), \pi(d_2))$
3. $d \in A_{ct} \Rightarrow \pi(d) \in A_{ct}$
4. $enc(d, k, r), k \in U \Rightarrow \pi(enc(d, k, r)) = enc(\pi(d), k, r)$
5. $enc(d, k, r), k' \in U$ and $k \neq k' \Rightarrow$
   $\forall d' \forall r' \pi(enc(d, k, r)) \neq enc(d', k', r')$

π is called reinterpretation under U if π is semi-reinterpretation under U and π^{-1} is also semi-reinterpretation under $\pi(U)$.

If there exists a reinterpretation π under U such that $\pi(d_1) = d_2$ holds, it represents that d_1 and d_2 are not indistinguishable by an adversary to whom only U is given. Condition 1 represents that an adversary can distinguish key data, public data and secret data. Condition 2 represents that adversary can distinguish $pair(d_1, d_2)$ from data except for $pair(d_1', d_2')$ such that he cannot distinguish d_1, d_2 from d_1', d_2' respectively. Condition 3 represents that an adversary can distinguish ciphertext data from data of other type. Condition 4 represents that if an adversary has ciphertext data $enc(d, k, r)$ and its key k, he can distinguish $enc(d, k, r)$ from data except for $enc(d', k, r)$ such that he cannot distinguish d from d'. Condition 5 represents that if an adversary has ciphertext data $enc(d, k, r)$ and a key k' such that $k \neq k'$, he can distinguish $enc(d, k, r)$ from any ciphertext data $enc(d', k', r')$ encrypted with the key k', since he can try to decrypt $enc(d, k, r)$ with k' and it fails.

Next, we extend the definition of π to adapt it to a set of message data, i.e. $\pi(X) = \{\pi(d) | d \in X\}$. We write $R(U)$ as the set of reinterpretation under U.

Then, the properties 1 and 2 hold.

PROPERTY 1. *1. $id \in R(U)$, where id is the identity permutation.*

2. if $\pi \in R(U)$, then $\pi^{-1} \in R(\pi(U))$.

3. if $\pi \in R(U)$ and $\pi' \in R(\pi(U))$, then $\pi' \circ \pi \in R(U)$.

PROOF. Proofs for 1 and 2 are trivial. For proving 3, First, we show that $\nu' \circ \nu$ is a semi-reinterpretation under X if ν is a semi-reinterpretation under X and ν' is a semi-reinterpretation under $\nu(X)$. Suppose that ν is a semi-reinterpretation under X and ν' is a semi-reinterpretation under $\nu(X)$. $\nu' \circ \nu$ trivially satisfies conditions 1,2 and 3. Now we show that $\nu' \circ \nu$ satisfies condition 4. Suppose that $enc(d, k, r), k \in X$. Then, $\nu(enc(d, k, r)), k \in \nu(X)$ holds. Hence, $\nu' \circ \nu(enc(d, k, r)) = \nu'(\nu(enc(d, k, r))) = \nu'(enc(\nu(d), k, r)) = enc(\nu'(\nu(d)), k, r) = enc(\nu' \circ \nu(d), k, r)$ holds since ν is a semi-reinterpretation under X and ν' is a semi-reinterpretation under $\nu(X)$. Therefore, we conclude that $\nu' \circ \nu$ satisfies condition 4. Next we show that $\nu' \circ \nu$ satisfies condition 5. Suppose that $enc(d, k, r), k' \in X$ and $k \neq k'$ hold. Since ν is a semi-reinterpretation under X, ν satisfies conditions 3 and 5, for any d'', k'', r'' such that $\nu(enc(d, k, r)) = enc(d'', k'', r'')$, $k'' \neq k'$ holds. Hence, $\nu' \circ \nu(enc(d, k, r)) = \nu'(\nu(enc(d, k, r))) = \nu'(enc(d'', k'', r''))$ holds. Since $\nu(enc(d, k, r)), k' \in \nu(X)$ and ν' is a semi-reinterpretation under $\nu(X)$, ν' satisfies conditions 3 and 5, for any d''', k''', r''' such that $\nu'(enc(d'', k'', r'')) = enc(d''', k''', r''')$, $k''' \neq k'$ holds. Therefore, we conclude that $\nu' \circ \nu$ satisfies condition 5.

Next, we show that $\pi' \circ \pi \in R(U)$ if $\pi \in R(U)$ and $\pi' \in R(\pi(X))$. From $\pi \in R(U)$, (a) π is a semi-reinterpretation under U. and (b) π^{-1} is a semi-reinterpretation under $\pi(U)$. From $\pi' \in R(\pi(X))$, (c) π' is a semi-reinterpretation under $\pi(U)$ and (d) π'^{-1} is a semi-reinterpretation under $\pi'(\pi(U))$. From (a) and (c), $\pi' \circ \pi$ is a semi-reinterpretation under U. From (b) and (d), $\pi^{-1} \circ \pi'^{-1}$ is a semi-reinterpretation under $\pi'(\pi(U))$. Since $\pi^{-1} \circ \pi'^{-1} = (\pi' \circ \pi)^{-1}$, we conclude $\pi' \circ \pi \in R(U)$. □

PROPERTY 2. *if $\pi \in R(cl(\{d_1\}))$ and $d_2 \in cl(\{d_1\})$, then $\pi(d_2) \in cl(\{\pi(d_1)\})$.*

Property 2 can be easily shown by induction on the definition of $d_2 \in cl(\{d_1\})$.

3.2.2 Interpretation of Extended Messages

Let π be a reinterpretation of message data. Then, we define interpretation $[\![E]\!]^{\pi}_{\mathcal{A},m}$ of an extended message E as follows:

- $[\![T]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T]\!]_{\mathcal{A},m})$,
- $[\![content\_of(E)]\!]^{\pi}_{\mathcal{A},m} = \begin{cases} d & \text{if } [\![E]\!]^{\pi}_{\mathcal{A},m} = enc(d, k, r) \\ undef & \text{otherwise} \end{cases}$,
- $[\![key\_of(E)]\!]^{\pi}_{\mathcal{A},m} = \begin{cases} k & \text{if } [\![E]\!]^{\pi}_{\mathcal{A},m} = enc(d, k, r) \\ undef & \text{otherwise} \end{cases}$,

where $undef$ is special data representing undefined, and $undef \notin A$ holds. Extended messages are interpreted with reinterpretation π. If an extended message is a message T, we reinterpret message data obtained by interpretation of T. If a message data obtained by interpretation of E is ciphertext data d, $content\_of(E)$ and $key\_of(E)$ are interpreted as the contents of d and the key used in encryption of d, otherwise $content\_of(E)$ and $key\_of(E)$ are interpreted as data representing undefined.

3.3 Interpretation of Formulae

Let $\mathcal{A}$ be a message algebra, m be an assignment which assigns message data or random data to message symbols and random number symbols, π be a reinterpretation. $\mathcal{A}, m, \pi \models_K \varphi$ represents that a formula φ is true in $\mathcal{A}, m, \pi$, which is defined as follows.

- $\mathcal{A}, m, \pi \models_K T_1 \geqslant T_2 \Leftrightarrow [\![T_2]\!]^{\pi}_{\mathcal{A},m} \in cl(\{[\![T_1]\!]^{\pi}_{\mathcal{A},m}\})$
- $\mathcal{A}, m, \pi \models_K E_1 \equiv E_2 \Leftrightarrow$
  $[\![E_1]\!]^{\pi}_{\mathcal{A},m} = [\![E_2]\!]^{\pi}_{\mathcal{A},m} \wedge [\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq undef$
- $\mathcal{A}, m, \pi \models_K E_1 \not\equiv E_2 \Leftrightarrow$
  $[\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq [\![E_2]\!]^{\pi}_{\mathcal{A},m}$
  $\wedge [\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq undef \wedge [\![E_2]\!]^{\pi}_{\mathcal{A},m} \neq undef$
- $\mathcal{A}, m, \pi \models_K \varphi_1 \wedge \varphi_2 \Leftrightarrow$
  $\mathcal{A}, m, \pi \models_K \varphi_1 \ \wedge \ \mathcal{A}, m, \pi \models_K \varphi_2$
- $\mathcal{A}, m, \pi \models_K \neg\varphi_1 \Leftrightarrow \mathcal{A}, m, \pi \not\models_K \varphi_1$
- $\mathcal{A}, m, \pi \models_K T \triangleright \varphi \Leftrightarrow$
  $\forall \pi' \in R(\pi(cl([\![T]\!]_{\mathcal{A},m})))(\mathcal{A}, m, \pi' \circ \pi \models_K \varphi)$

$T_1 \geqslant T_2$ is interpreted as true if the data of T_2 can be constructed from the data of T_1. $E_1 \equiv E_2$(w.r.t. $E_1 \not\equiv E_2$) is interpreted as true if both the data of E_1 and the data E_2 are defined and these are equal (w.r.t. different). The interpretations of $\wedge, \neg$ are the usual ones. For modal formulae, interpretation is similar to interpretation for usual epistemic logic. This means, $T \triangleright \varphi$ is true in the current situation if φ is true in all the situations which are obtained by reinterpretation of the original situation. Intuitively, an adversary owning the data of T recognizes that φ holds, if φ holds for all the interpretations which are indistinguishable from the current interpretation of messages.

Let id be the identity permutation. If $\mathcal{A}, m, id \models_K \varphi$ holds for any $\mathcal{A}, m$, we say φ is valid in the Kripke semantics, written by $\models_K \varphi$.

3.4 Examples of Interpretation

In this section, we show the interpretation of several formulae as examples.

EXAMPLE 3. *$\models_K (\{N\}^R_K, K) \geqslant N$ holds, since $[\![N]\!]^{id}_{\mathcal{A},m} \in cl([\![(\{N\}^R_K, K)]\!]^{id}_{\mathcal{A},m})$ holds as follows.*
$[\![(\{N\}^R_K, K)]\!]^{id}_{\mathcal{A},m} = id([\![(\{N\}^R_K, K)]\!]_{\mathcal{A},m}) = [\![(\{N\}^R_K, K)]\!]_{\mathcal{A},m}$
$= pair(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m})$. *Hence,*
$cl([\![(\{N\}^R_K, K)]\!]^{id}_{\mathcal{A},m}) = cl(\{pair(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m})\}) = cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\})$. *Since $[\![N]\!]_{\mathcal{A},m} \in cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\})$ and $[\![N]\!]_{\mathcal{A},m} = [\![N]\!]^{id}_{\mathcal{A},m}$ hold, $[\![N]\!]^{id}_{\mathcal{A},m} \in cl([\![(\{N\}^R_K, K)]\!]^{id}_{\mathcal{A},m})$ holds.*

This represents the fact that if an adversary has the encrypted message $\{N\}^R_K$ and the key K, he can extract its content.

EXAMPLE 4. *$\models_K (\{N\}^R_K, K) \triangleright (\{N\}^R_K, K) \geqslant N$ holds obviously, due to example 3 and property 2 in Sect.3.2.1. This represents that if an adversary has the encrypted message $\{N\}^R_K$ and the key K, he recognizes the fact that he can extract its contents.*

EXAMPLE 5. *$\models_K content\_of(\{N\}^R_K) \equiv N$ holds, since the following hold.*

- $[\![\{N\}^R_K]\!]^{id}_{\mathcal{A},m} = id([\![\{N\}^R_K]\!]_{\mathcal{A},m}) = [\![\{N\}^R_K]\!]_{\mathcal{A},m}$
  $= enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))$
- $[\![content\_of(\{N\}^R_K)]\!]^{id}_{\mathcal{A},m} = [\![N]\!]_{\mathcal{A},m} = [\![N]\!]^{id}_{\mathcal{A},m}$

This represents the fact that $\{N\}^R_K$ is an encrypted message and its contents are equal to N.

EXAMPLE 6. *$\models_K (\{N\}^R_K, K) \triangleright content\_of(\{N\}^R_K) \equiv N$ holds as follows.*
$\mathcal{A}, m, id \models_K (\{N\}^R_K, K) \triangleright content\_of(\{N\}^R_K) \equiv N$
$\Leftrightarrow \forall \pi \in R(id(cl([\![(\{N\}^R_K, K)]\!]_{\mathcal{A},m})))$
$\mathcal{A}, m, \pi \circ id \models_K content\_of(\{N\}^R_K) \equiv N$
$\Leftrightarrow \forall \pi \in R(cl([\![(\{N\}^R_K, K)]\!]_{\mathcal{A},m}))$
$\mathcal{A}, m, \pi \models_K content\_of(\{N\}^R_K) \equiv N$
$\Leftrightarrow \forall \pi \in R(cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\}))$
$[\![content\_of(\{N\}^R_K)]\!]^{\pi}_{\mathcal{A},m} = [\![N]\!]^{\pi}_{\mathcal{A},m}$
Now, since $enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m} \in cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\})$ holds, if $\pi \in R(cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\}))$ holds, the following holds.
$[\![\{N\}^R_K]\!]^{\pi}_{\mathcal{A},m} = \pi([\![\{N\}^R_K]\!]_{\mathcal{A},m})$
$= \pi(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)))$
$= enc(\pi([\![N]\!]_{\mathcal{A},m}), [\![K]\!]_{\mathcal{A},m}, m(R)))$. *Hence,*
$[\![content\_of(\{N\}^R_K)]\!]^{\pi}_{\mathcal{A},m} = \pi([\![N]\!]_{\mathcal{A},m}) = [\![N]\!]^{\pi}_{\mathcal{A},m}$
Therefore, we can conclude $\models_K (\{N\}^R_K, K) \triangleright content\_of(\{N\}^R_K) \equiv N$ holds.

This represents that if an adversary has the encrypted message $\{N\}^R_K$ and the key K, he recognizes the fact that the content of $\{N\}^R_K$ is equal to N.

EXAMPLE 7. *$\models_K \{N\}^R_K \triangleright content\_of(\{N\}^R_K) \equiv N$ does not hold as follows.*

First the following hold.
$\mathcal{A}, m, id \models_K \{N\}^R_K \triangleright content\_of(\{N\}^R_K) \equiv N$
$\Leftrightarrow \forall \pi \in R(cl(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))))$
$[\![content\_of(\{N\}^R_K)]\!]^{\pi}_{\mathcal{A},m} = [\![N]\!]^{\pi}_{\mathcal{A},m}$
Now, since $[\![K]\!]_{\mathcal{A},m} \notin cl(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)))$ holds, the following π is a reinterpretation under $cl(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)))$.

$$\pi = \begin{pmatrix} enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)) \mapsto enc(n', k', r') \\ enc(n', k', r') \mapsto enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)) \\ [\![N]\!]_{\mathcal{A},m} \mapsto [\![N]\!]_{\mathcal{A},m} \\ [\![K]\!]_{\mathcal{A},m} \mapsto [\![K]\!]_{\mathcal{A},m} \\ n' \mapsto n' \\ k' \mapsto k' \end{pmatrix},$$

where $[\![N]\!]_{\mathcal{A},m} \neq n'$ holds.
Now, the following holds.
$[\![\{N\}^R_K]\!]^{\pi}_{\mathcal{A},m} = \pi([\![\{N\}^R_K]\!]_{\mathcal{A},m})$
$= \pi(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))) = enc(n', k', r')$
Hence, $[\![content\_of(\{N\}^R_K)]\!]^{\pi}_{\mathcal{A},m} = n' \neq [\![N]\!]_{\mathcal{A},m}$

$= \pi([\![N]\!]_{\mathcal{A},m}) = [\![N]\!]^{\pi}_{\mathcal{A},m}$
Therefore $\models_K \{N\}^R_K \triangleright content\_of(\{N\}^R_K) \equiv N$ *does not hold.*

This represents that if an adversary has only the encrypted message $\{N\}^R_K$ *and does not have its key, he cannot recognize the fact that the content of* $\{N\}^R_K$ *is equal to* N.

EXAMPLE 8. *If* $R \in \mathcal{R}_{adv}$ *holds,* $\models_K (N, K) \triangleright content\_of(\{N\}^R_K) \equiv N$ *holds, due to a similar reason to example 6.*

This represents that $\{N\}^R_K$ *is an encrypted message which was encrypted by an adversary, he recognizes the fact that the content of* $\{N\}^R_K$ *is equal to* N.

EXAMPLE 9. *The following formulae are valid.*

- *Axioms of classical propositional logic.*
- *Formulae characterizing equality* $\equiv$ *and non-equality* $\not\equiv$*, e.g.*
  - $E \equiv E$,
  - $E_1 \equiv E_2 \rightarrow E_2 \equiv E_1$,
  - $E_1 \equiv E_2 \wedge E_2 \equiv E_3 \rightarrow E_1 \equiv E_3$,
  - $E_1 \not\equiv E_2 \wedge E_2 \equiv E_3 \rightarrow E_1 \not\equiv E_3$,
  - $E_1 \not\equiv E_2 \rightarrow \neg E_1 \equiv E_2$.
- *Formulae characterizing content_of , key_of , e.g.*
  - $content\_of(\{T\}^R_K) \equiv T$,
  - $key\_of(\{T\}^R_K) \equiv K$.
- *Axioms for epistemic logic, due to property 1, i.e.*
  - $T \triangleright (\varphi \rightarrow \psi) \rightarrow (T \triangleright \varphi \rightarrow T \triangleright \psi)$,
  - $T \triangleright \varphi \rightarrow \varphi$,
  - $T \triangleright \varphi \rightarrow T \triangleright T \triangleright \varphi$,
  - $\neg T \triangleright \neg\varphi \rightarrow T \triangleright \neg T \triangleright \neg\varphi$.
- *Monotonicity of adversary's knowledge, i.e.,*
  - $T_1 \geqslant T_2 \rightarrow (T_2 \triangleright \varphi \rightarrow T_1 \triangleright \varphi)$.

4. INTUITIONISTIC SEMANTICS BASED ON CONSTRUCTABILITY OF EVIDENCE

In this section, we introduce intuitionistic semantics based on constructability of evidence, which was proposed in [8]. In the Kripke semantics defined in Sect.3, acquisition of relational information by an adversary can be directly defined as his knowledge of relational information. On the other hand, in the intuitionistic semantics proposed in [8], acquisition of relational information by an adversary is intuitionistically defined as his ability to show the evidence to succeed in obtaining the information, which in brief, is defined as inclusion of evidence in the closure. In [8], we proposed the intuitionistic semantics defined on the computational model by using probabilistic polynomial time Turing machines. In this section, we redefine the intuitionistic semantics on the symbolic model by using message algebra.

We define the intuitionistic semantics for a subset of the syntax defined in Sect.2. In Sect.4.1, we restrict the syntax defined in Sect.2. In Sect.4.2, we give the intuitionistic semantics based on the constructability of evidence.

4.1 Restriction of Syntax

The Intuitionistic semantics gives an interpretation for formulae of the following forms:

- $T_1 \geqslant T_2$,
- $T \triangleright E_1 \equiv E_2$, $T \triangleright E_1 \not\equiv E_2$, where E_1, E_2 are extended messages of the form $content\_of(T')$, $key\_of(T')$ or T'.

4.2 Intuitionistic Semantics

In the intuitionistic semantics, we adopt the interpretation of messages defined in 3.1.

Let $\mathcal{A}$ be a message algebra, and m be an assignment which assigns message data or random data to message symbols and random number symbols. $\mathcal{A}, m \models_I \varphi$ represents that a formula φ is true in $\mathcal{A}, m$, which is defined as follows.

For formulae of the form $T_1 \geqslant T_2$, we give the same interpretation as defined in Sect.3.3.

- $\mathcal{A}, m \models_I T_1 \geqslant T_2 \Leftrightarrow [\![T_2]\!]_{\mathcal{A},m} \in cl(\{[\![T_1]\!]_{\mathcal{A},m}\})$

For formulae of the form $T \triangleright E_1 \equiv E_2$ and $T \triangleright E_1 \not\equiv E_2$, we define interpretation by 12 cases according to the form of E_1 and E_2.

1. $T \triangleright T_1 \equiv T_2$
   $T \triangleright T_1 \equiv T_2$ is true if an adversary can construct evidence of the equality of the values of T_1 and T_2 from the value of T, where the evidence is the identical values of T_1 and T_2.

   $\mathcal{A}, m \models_I T \triangleright T_1 \equiv T_2 \Leftrightarrow$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge [\![T_1]\!]_{\mathcal{A},m} = [\![T_2]\!]_{\mathcal{A},m}$

2. $T \triangleright T_1 \not\equiv T_2$
   $T \triangleright T_1 \not\equiv T_2$ is true if an adversary can construct evidence of a difference between the values of T_1 and T_2, where the evidence is the different values of T_1 and T_2.

   $\mathcal{A}, m \models_I T \triangleright T_1 \not\equiv T_2 \Leftrightarrow$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge [\![T_1]\!]_{\mathcal{A},m} \neq [\![T_2]\!]_{\mathcal{A},m}$

3. $T \triangleright content\_of(T_1) \equiv T_2$
   $T \triangleright content\_of(T_1) \equiv T_2$ is true if an adversary can construct evidence of equality between the value of contents of T_1 and the value of T_2, where the evidence is $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k)$ such that $[\![T_1]\!]_{\mathcal{A},m}$ is ciphertext data, k is a key data, and the result of decryption of $[\![T_1]\!]_{\mathcal{A},m}$ by k is equal to $[\![T_2]\!]_{\mathcal{A},m}$.

   $\mathcal{A}, m \models_I T \triangleright content\_of(T_1) \equiv T_2 \Leftrightarrow$
   $\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) = [\![T_2]\!]_{\mathcal{A},m})$

   dec is the decryption function satisfying the following, and $\perp$ is a special data representing 'decryption failure'.
   $$dec(d,k) = \begin{cases} d_1 & d = enc(d_1, k, r) \text{ for some } r \\ \perp & \text{otherwise} \end{cases}$$

4. $T \triangleright content\_of(T_1) \not\equiv T_2$
   $T \triangleright content\_of(T_1) \not\equiv T_2$ is true if an adversary can construct evidence of a difference between the value of contents of T_1 and the value of T_2, where the evidence is $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k)$ such that $[\![T_1]\!]_{\mathcal{A},m}$ is ciphertext data, k is key data, and the result of decryption of $[\![T_1]\!]_{\mathcal{A},m}$ by k is different from $[\![T_2]\!]_{\mathcal{A},m}$.

   $\mathcal{A}, m \models_I T \triangleright content\_of(T_1) \not\equiv T_2 \Leftrightarrow$
   $\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge$
   $dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \perp \wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq [\![T_2]\!]_{\mathcal{A},m})$

5. $T \triangleright content\_of(T_1) \equiv content\_of(T_2)$
   $T \triangleright content\_of(T_1) \equiv content\_of(T_2)$ is true if an adversary can construct evidence of equality of the values of contents of T_1 and T_2, where the evidence is either $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m})$ such that $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ are identical ciphertext data, or $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k, k')$ such that $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ are ciphertext data and k and k' are key data and the result of decryption of $[\![T_1]\!]_{\mathcal{A},m}$ by k is equal to the result of decryption of $[\![T_2]\!]_{\mathcal{A},m}$ by k'.

   $\mathcal{A}, m \models_I T \triangleright content\_of(T_1) \equiv content\_of(T_2) \Leftrightarrow$
   $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct})$
   $\vee \exists k, k'([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k, k' \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge k, k' \in A_{key} \wedge$
   $dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \perp \wedge$
   $dec([\![T_1]\!]_{\mathcal{A},m}, k) = dec([\![T_2]\!]_{\mathcal{A},m}, k'))$

6. $T \triangleright content\_of(T_1) \not\equiv content\_of(T_2)$
   $T \triangleright content\_of(T_1) \not\equiv content\_of(T_2)$ is true if an adversary can construct evidence of a difference between the values of contents of T_1 and T_2, where the evidence is $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k, k')$ such that $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ are ciphertext data, k and k' are key data, and the result of decryption of $[\![T_1]\!]_{\mathcal{A},m}$ by k is different from the result of decryption of $[\![T_2]\!]_{\mathcal{A},m}$ by k'.

   $\mathcal{A}, m \models_I T \triangleright content\_of(T_1) \not\equiv content\_of(T_2) \Leftrightarrow$
   $\exists k, k'([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k, k' \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge k, k' \in A_{key} \wedge$
   $dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \perp \wedge \quad dec([\![T_2]\!]_{\mathcal{A},m}, k') \neq \perp$
   $\wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq dec([\![T_2]\!]_{\mathcal{A},m}, k'))$

7. $T \triangleright key\_of(T_1) \equiv T_2$
   $T \triangleright key\_of(T_1) \equiv T_2$ is true if an adversary can construct evidence of equality between the value of a key of T_1 and the value of T_2, where the evidence is $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m})$ such that $[\![T_1]\!]_{\mathcal{A},m}$ is ciphertext data, and decryption of $[\![T_1]\!]_{\mathcal{A},m}$ by $[\![T_2]\!]_{\mathcal{A},m}$ succeeds.

   $\mathcal{A}, m \models_I T \triangleright key\_of(T_1) \equiv T_2 \Leftrightarrow$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge [\![T_2]\!]_{\mathcal{A},m} \in A_{key} \wedge$
   $dec([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}) \neq \perp$

8. $T \triangleright key\_of(T_1) \not\equiv T_2$
   $T \triangleright key\_of(T_1) \not\equiv T_2$ is true if an adversary can construct evidence of difference between the value of a key of T_1 and the value of T_2, where the evidence is $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m})$ such that $[\![T_1]\!]_{\mathcal{A},m}$ is ciphertext data and $[\![T_2]\!]_{\mathcal{A},m}$ is not a key, or decryption of $[\![T_1]\!]_{\mathcal{A},m}$ by $[\![T_2]\!]_{\mathcal{A},m}$ fails.

   $\mathcal{A}, m \models_I T \triangleright key\_of(T_1) \not\equiv T_2 \Leftrightarrow$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge$
   $([\![T_2]\!]_{\mathcal{A},m} \notin A_{key} \vee dec([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}) = \perp)$

9. $T \triangleright key\_of(T_1) \equiv key\_of(T_2)$
   $T \triangleright key\_of(T_1) \equiv key\_of(T_2)$ is true if an adversary can construct evidence of equality of the values of keys of T_1 and T_2, where the evidence is either $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m})$ such that $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ are identical ciphertext data, or $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k)$ such that $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ are ciphertext data and k is key data and both decryption of $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ by k succeed.

   $\mathcal{A}, m \models_I T \triangleright key\_of(T_1) \equiv key\_of(T_2) \Leftrightarrow$
   $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m} = [\![T_2]\!]_{\mathcal{A},m}) \vee$
   $\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge$
   $dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \perp \wedge dec([\![T_2]\!]_{\mathcal{A},m}, k) \neq \perp)$

10. $T \triangleright key\_of(T_1) \not\equiv key\_of(T_2)$
    $T \triangleright key\_of(T_1) \not\equiv key\_of(T_2)$ is true if an adversary can construct evidence of a difference between the values of keys of T_1 and T_2, where the evidence is $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k)$ such that $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ are ciphertext data, k is a key data and either of decryption of $[\![T_1]\!]_{\mathcal{A},m}$ or $[\![T_2]\!]_{\mathcal{A},m}$ by k succeeds.

    $\mathcal{A}, m \models_I T \triangleright key\_of(T_1) \not\equiv key\_of(T_2) \Leftrightarrow$
    $\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
    $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge$
    $((dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \perp \wedge dec([\![T_2]\!]_{\mathcal{A},m}, k) = \perp) \vee$
    $(dec([\![T_1]\!]_{\mathcal{A},m}, k) = \perp \wedge dec([\![T_2]\!]_{\mathcal{A},m}, k) \neq \perp)))$

11. $T \triangleright content\_of(T_1) \equiv key\_of(T_2)$
    $T \triangleright content\_of(T_1) \equiv key\_of(T_2)$ is true if an adversary can construct evidence of equality between the value of contents of T_1 and the value of a key of T_2, where the evidence is $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k)$ such that $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ are ciphertext data, k is key data for decryption of $[\![T_1]\!]_{\mathcal{A},m}$, and decryption of $[\![T_2]\!]_{\mathcal{A},m}$ by the contents of $[\![T_1]\!]_{\mathcal{A},m}$ succeeds.

    $\mathcal{A}, m \models_I T \triangleright content\_of(T_1) \equiv key\_of(T_2) \Leftrightarrow$
    $\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
    $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge$
    $k, dec([\![T_1]\!]_{\mathcal{A},m}, k) \in A_{key} \wedge$
    $dec([\![T_2]\!]_{\mathcal{A},m}, dec([\![T_1]\!]_{\mathcal{A},m}, k)) \neq \perp)$

12. $T \triangleright content\_of(T_1) \not\equiv key\_of(T_2)$
    $T \triangleright content\_of(T_1) \not\equiv key\_of(T_2)$ is true if an adversary can construct evidence of difference between the value of contents of T_1 and the value of a key of T_2, where the evidence is $([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k)$ such that $[\![T_1]\!]_{\mathcal{A},m}$ and $[\![T_2]\!]_{\mathcal{A},m}$ are ciphertext data, k is key data for decryption of $[\![T_1]\!]_{\mathcal{A},m}$, and the contents of $[\![T_1]\!]_{\mathcal{A},m}$ is not a key, or decryption of $[\![T_2]\!]_{\mathcal{A},m}$ by the contents of $[\![T_1]\!]_{\mathcal{A},m}$ fails.

    $\mathcal{A}, m \models_I T \triangleright content\_of(T_1) \not\equiv key\_of(T_2) \Leftrightarrow$
    $\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
    $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge$
    $dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \perp \wedge$
    $(dec([\![T_1]\!]_{\mathcal{A},m}, k) \notin A_{key} \vee$
    $dec([\![T_2]\!]_{\mathcal{A},m}, dec([\![T_1]\!]_{\mathcal{A},m}, k)) = \perp))$

If $\mathcal{A}, m \models_I \varphi$ holds for any $\mathcal{A}, m$, we say φ is valid in the intuitionistic semantics, written by $\models_I \varphi$.

In [8], we proposed a deduction system for analyzing whether an adversary can obtain relational information. This deduction system deduces the formulae of the restricted form defined in Sect.4.1. We introduce this system in Appendix A. If a formula φ is derivable by this system, we write $\vdash_{JD} \varphi$. This deduction system is sound and complete for the intuitionistic semantics as shown in the following proposition.

PROPOSITION 1. *Let φ be a formula of the restricted form defined in Sect.4.1. Then, $\vdash_{JD} \varphi$ holds, if and only if $\models_I \varphi$ holds.*

This proposition can be proved in a similar way to the proof in [8].

5. RELATION BETWEEN THE TWO SEMANTICS

Between the Kripke semantics proposed in Sect.3 and the intuitionistic semantics introduced in Sect.4, the following relation holds.

THEOREM 1. *Let φ be a formula of the restricted form defined in Sect.4.1. Let $\mathcal{A}$ be a message algebra, m be an assignment which assigns message data or random data to message symbols and random number symbols. Then, if $\mathcal{A}, m \models_I \varphi$ holds, then $\mathcal{A}, m, id \models_K \varphi$ holds.*

PROOF. (Case for φ is of the form $T \triangleright T_1 \not\equiv T_2$)
Suppose that $\mathcal{A}, m \models_I T \triangleright T_1 \not\equiv T_2$, i.e. $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge [\![T_1]\!]_{\mathcal{A},m} \neq [\![T_2]\!]_{\mathcal{A},m}$. Let $\pi \in R(cl([\![T]\!]_{\mathcal{A},m}))$ be arbitrary reinterpretation under $cl([\![T]\!]_{\mathcal{A},m})$. Then, $[\![T_1]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T_1]\!]_{\mathcal{A},m})$ and $[\![T_2]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T_2]\!]_{\mathcal{A},m})$ hold. Now, $\pi([\![T_1]\!]_{\mathcal{A},m}) \neq \pi([\![T_2]\!]_{\mathcal{A},m})$ holds, since $[\![T_1]\!]_{\mathcal{A},m} \neq [\![T_2]\!]_{\mathcal{A},m}$ holds and π is a permutation, i.e. bijection. This means, $\mathcal{A}, m, \pi \models_K T_1 \not\equiv T_2$ holds. Therefore, $\mathcal{A}, m, id \models_K T \triangleright T_1 \not\equiv T_2$ holds.
(Case for φ is of the form $T \triangleright content\_of(T_1) \equiv T_2$)
Suppose that $\mathcal{A}, m \models_I T \triangleright content\_of(T_1) \equiv T_2$, i.e. there exists k such that $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge [\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) = [\![T_2]\!]_{\mathcal{A},m}$. Then, due to $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) = [\![T_2]\!]_{\mathcal{A},m}$, there exists r such that $[\![T_1]\!]_{\mathcal{A},m} = enc([\![T_2]\!]_{\mathcal{A},m}, k, r)$ holds. Let $\pi \in R(cl([\![T]\!]_{\mathcal{A},m}))$ be arbitrary reinterpretation under $cl([\![T]\!]_{\mathcal{A},m})$. Then, $[\![T_1]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T_1]\!]_{\mathcal{A},m}) = \pi(enc([\![T_2]\!]_{\mathcal{A},m}, k, r))$ holds. Now, due to $[\![T_1]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m})$ and condition 4 of semi-reinterpretation, $\pi(enc([\![T_2]\!]_{\mathcal{A},m}, k, r)) = enc(\pi([\![T_2]\!]_{\mathcal{A},m}), k, r)$ holds. Hence, $[\![content\_of(T_1)]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T_2]\!]_{\mathcal{A},m}) = [\![T_2]\!]^{\pi}_{\mathcal{A},m}$ holds. This means, $\mathcal{A}, m, \pi \models_K content\_of(T_1) \equiv T_2$ holds. Therefore, $\mathcal{A}, m, id \models_K T \triangleright content\_of(T_1) \equiv T_2$ holds.
(Case for φ is of the form $T \triangleright key\_of(T_1) \not\equiv T_2$)
Suppose that $\mathcal{A}, m \models_I T \triangleright key\_of(T_1) \not\equiv T_2$, i.e. $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge [\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge ([\![T_2]\!]_{\mathcal{A},m} \notin A_{key} \vee dec([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}) = \bot)$. Then, due to $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct}$, there exists d, k, r such that $[\![T_1]\!]_{\mathcal{A},m} = enc(d, k, r)$. Let $\pi \in R(cl([\![T]\!]_{\mathcal{A},m}))$ be arbitrary reinterpretation under $cl([\![T]\!]_{\mathcal{A},m})$. (1) Let us consider the case of $[\![T_2]\!]_{\mathcal{A},m} \notin A_{key}$. There exists d', k', r' such that $[\![T_1]\!]^{\pi}_{\mathcal{A},m} = \pi(enc(d, k, r)) = enc(d', k', r')$, by condition 3 of semi-reinterpretation. Hence $[\![key\_of(T_1)]\!]^{\pi}_{\mathcal{A},m} = k' \in A_{key}$. On the other hand, $[\![T_2]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T_2]\!]_{\mathcal{A},m}) \notin A_{key}$, since $[\![T_2]\!]_{\mathcal{A},m} \notin A_{key}$ and π does not change data types. Therefore $[\![key\_of(T_1)]\!]^{\pi}_{\mathcal{A},m} \neq [\![T_2]\!]^{\pi}_{\mathcal{A},m}$ holds. (2) Let us consider the other case of $[\![T_2]\!]_{\mathcal{A},m} \in A_{key}$. Then, $dec([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}) = \bot$, which means $k \neq [\![T_2]\!]_{\mathcal{A},m}$. From this, there exists d', k', r' such that $[\![T_1]\!]^{\pi}_{\mathcal{A},m} = \pi(enc(d, k, r)) = enc(d', k', r')$ and $k' \neq [\![T_2]\!]_{\mathcal{A},m}$, by condition 3 and 5 of semi-reinterpretation. Hence $[\![key\_of(T_1)]\!]^{\pi}_{\mathcal{A},m} = k' \neq [\![T_2]\!]_{\mathcal{A},m}$. On the other hand, $[\![T_2]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T_2]\!]_{\mathcal{A},m}) = [\![T_2]\!]_{\mathcal{A},m}$, by condition 1 of semi-reinterpretation. Hence, $[\![key\_of(T_1)]\!]^{\pi}_{\mathcal{A},m} \neq [\![T_2]\!]^{\pi}_{\mathcal{A},m}$ holds. For both cases of (1) and (2), we conclude $\mathcal{A}, m, \pi \models_K key\_of(T_1) \not\equiv T_2$ holds. Therefore, $\mathcal{A}, m, id \models_K T \triangleright key\_of(T_1) \not\equiv T_2$ holds.

We can prove the other cases in which φ has other forms in a similar way, we omit the proof. □

On the other hand, the converse of theorem 1 does not hold. For instance, $N \triangleright content\_of(\{N\}^R_K) \equiv content\_of(\{N\}^R_K)$ is valid in the Kripke semantics, although it is not valid in the intuitionistic semantics.

Due to proposition 1 and theorem 1, the following corollary holds.

COROLLARY 1. *Let φ be a formula of the restricted form defined in Sect.4.1. Then, if $\vdash_{JD} \varphi$ holds, then $\models_K \varphi$ holds.*

This corollary means that the deduction system proposed in [8], which is shown in Appendix A, is sound for the Kripke semantics.

6. RELATED WORKS

There have been various studies about verification methods of security protocols by using epistemic logic. The most famous study is BAN logic proposed by M. Burrows, M. Abadi and R. Needham in [3]. BAN logic is used in verification of authenticity for cryptographic authentication protocols. In BAN logic, the authenticity property is verified by deducing a formula representing authenticity from axioms representing protocol definitions. For BAN logic, Kripke semantics was given in [1]. Various succeeding works of BAN logic were also studied, e.g. [6, 10, 11, 7].

Protocol Composition Logic (PCL) in [4] is used for verification of authenticity and secrecy for protocols. PCL can be regarded as epistemic logic. PCL is Hoare-style logic, of which formulae have preconditions, postconditions and programs representing protocol description by process calculus. PCL has Kripke semantics of which reachability relation is defined by using traces of programs.

For verification of the anonymity of protocols by using epistemic logic, there have been several studies such as [9] and [5]. By these logics, the anonymity property is verified by showing that a formula representing anonymity is satisfied in the Kripke model which is obtained from various behaviors of the participants of the protocol.

The definition of authenticity and anonymity of security protocols is based on the transmission and receiving of messages. Hence, these logics above use atomic propositions

representing the transmission and receiving of messages. On the other hand, the logic proposed in this paper is intended to be used for verification of secrecy of relational information between ciphertext. Therefore, our logic uses atomic propositions representing the equality and non-equality of contents or keys of ciphertexts. Our logic is quite different from these logics above on this point.

7. CONCLUSION

In this paper, we applied Kripke semantics to the logic for analyzing whether an adversary can obtain relational information between contents or keys of two ciphertexts. We constructed the semantics of an epistemic logic by regarding relational information obtained by an adversary as the adversary's knowledge. Hence, this semantics is naturally defined, compared with the intuitionistic semantics proposed in [8]. We also made a comparison between this Kripke semantics and the intuitionistic semantics, and showed that if a formula is satisfied in the intuitionistic semantics, it is also satisfied in the Kripke semantics. This means that the deduction system proposed in [8] is sound for the Kripke semantics.

The logic proposed in this paper is intended to be used for verification of secrecy of relational information between ciphertexts in security protocols. For instance, it is intended to verify that an adversary can recognize equality or non-equality between a key which was used in the encryption of a ciphertext transmitted in the past and a key which was used in encryption of a ciphertext being transmitted now. Our future work is to provide a sound and complete axiomatic system of this logic. This work makes it possible to verify the secrecy of relational information by deduction of axiomatic system.

8. ACKNOWLEDGMENTS

This work was supported by a Grant-in-Aid for Scientific Research(C) (24500032).

9. REFERENCES

[1] M. Abadi and M. R. Tuttle. A semantics of a logic of authentication. In *Proceedings of the Tenth Annual ACM Symposium of Principles of Distributed Computing*, pages 201–216, 1991.

[2] A. Bhery, S. Hagihara, and N. Yonezaki. A formal system for analysis of cryptographic encryption and their security properties. In *International Symposium on Software Security 2003, Software Security - Theories and Systems*, volume 3233 of *Lecture Notes in Computer Science*, pages 87–112, 2004.

[3] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990.

[4] A. Datta, A. Derek, J. C. Mitchell, and A. Roy. Protocol composition logic (PCL). In *Computation, Meaning, and Logic: Articles dedicated to Gordon Plotkin*, volume 172 of *Electronic Notes in Theoretical Computer Science*, pages 311–358, 2007.

[5] F. D. Garcia, I. Hasuo, W. Pieters, and P. van Rossum. Provable anonymity. In *FMSE '05: Proceedings of the 2005 ACM workshop on Formal methods in security engineering*, pages 63–72, New York, NY, USA, 2005. ACM.

[6] L. Gong, R. Needham, and R. Yahalom. Reasoning About Belief in Cryptographic Protocols. In D. Cooper and T. Lunt, editors, *Proceedings 1990 IEEE Symposium on Research in Security and Privacy*, pages 234–248. IEEE Computer Society, 1990.

[7] S. Gürgens. SG logic - a formal analysis technique for authentication protocols. In *Security Protocols, 5th International Workshop*, volume 1361 of *Lecture Notes in Computer Science*, pages 159–176. Springer, 1997.

[8] S. Hagihara, H. Oguro, and N. Yonezaki. Completeness of a deduction system for relational information between ciphertexts based on probabilistic computational semantics. In *Theory and Practice of Computation*, volume 5 of *Proceedings in Information and Communications Technology*, pages 116–132. Springer, 2012.

[9] J. Halpern and K. O'Neill. Anonymity and information hiding in multiagent systems. In *Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE*, pages 75 – 88, 30 2003.

[10] P. F. Syverson and P. C. van Oorschot. On unifying some cryptographic protocol logics. In *Proceedings of the 13th IEEE Symposium on Security and Privacy*, pages 14–28, 1994.

[11] G. Wedel and V. Kessler. Formal semantics for authentication logics. In *Proceedings of the 4th European Symposium on Research in Computer Security*, volume 1146 of *Lecture Notes in Computer Science*, pages 219–241. Springer, 1996.

APPENDIX

A. DEDUCTION SYSTEM OF OBTAINABILITY OF RELATIONAL INFORMATION BY ADVERSARY

We introduce a deduction system of obtainability of relational information by an adversary, proposed in [8]. This deduction system deduces formulae of the restricted form defined in Sect.4.1.

The inference rules of deducing formulae of the form $T_1 \geqslant T_2$ are as follows:

$$\frac{}{T \geqslant T}, \quad \frac{}{T \geqslant I}, \quad \text{where } I \in \mathcal{I},$$

$$\frac{T \triangleright T_1 \quad T \geqslant T_1}{T \triangleright (T_1, T_2)}, \quad \frac{T \geqslant (T_1, T_2)}{T \geqslant T_1}, \quad \frac{T \geqslant (T_1, T_2)}{T \geqslant T_2},$$

$$\frac{T \geqslant \{T_1\}_K^R \quad T \geqslant K}{T \geqslant T_1},$$

$$\frac{T \geqslant T_1 \quad T \geqslant K}{T \geqslant \{T_1\}_K^R}, \text{ where } R \in \mathcal{R}_{adv}.$$

The inference rules of deducing formulae of the form $T \triangleright E_1 \equiv E_2$ and $T \triangleright E_1 \not\equiv E_2$ are as follows.

- If an adversary obtains a message T_1 from T, then he obtains relational information that the value of T_1 and the value of T_1 are equal.

$$\frac{T \geqslant T_1}{T \triangleright T_1 \equiv T_1}$$

- If an adversary obtains two different messages T_1 and T_2, then he obtains relational information that the value of T_1 and the value of T_2 are different.

$$\frac{T \geqslant T_1 \quad T \geqslant T_2}{T \triangleright T_1 \not\equiv T_2},$$

where T_1 and T_2 are syntactically different messages.

- If an adversary has relational information that the value of $\{T_1\}_K^R$ is equal to the value of $\{T_2\}_{K'}^{R'}$, then he also obtains information that the two messages $\{T_1\}_K^R$ and $\{T_2\}_{K'}^{R'}$ have the same contents and are encrypted with the same key.

$$\frac{T \triangleright \{T_1\}_K^R \equiv \{T_2\}_{K'}^{R'}}{T \triangleright f(\{T_1\}_K^R) \equiv f(\{T_2\}_{K'}^{R'}),}$$

where f is either *content_of* or *key_of*.

- If an adversary obtains an encrypted message $\{T_1\}_K^R$ and its key K, then the decryption succeeds and he obtains relational information that the value of the contents of $\{T_1\}_K^R$ is the value of T_1.

$$\frac{T \geqslant \{T_1\}_K^R \quad T \geqslant K}{T \triangleright \mathit{content\_of}(\{T_1\}_K^R) \equiv T_1}$$

- If an adversary obtains an encrypted message $\{T_1\}_K^R$ and its key K, then the decryption succeeds and he obtains relational information that the value of a key of $\{T_1\}_K^R$ is the value of K.

$$\frac{T \geqslant \{T_1\}_K^R \quad T \geqslant K}{T \triangleright \mathit{key\_of}(\{T_1\}_K^R) \equiv K}$$

- If an adversary obtains an encrypted message $\{T_1\}_K^R$ and a message T_2 which is different from the key K, then T_2 is not a key or the decryption fails, and he obtains relational information that the value of the key of $\{T_1\}_K^R$ is different from the value of T_2.

$$\frac{T \geqslant \{T_1\}_K^R \quad T \geqslant T_2}{T \triangleright \mathit{key\_of}(\{T_1\}_K^R) \not\equiv T_2,}$$

where T_2 is syntactically different from K.

- Symmetry and transitivity of equality and non-equality hold.

$$\frac{T \triangleright E_1 \equiv E}{T \triangleright E \equiv E_1} \qquad \frac{T \triangleright E_1 \not\equiv E}{T \triangleright E \not\equiv E_1}$$

$$\frac{T \triangleright E \equiv E_2 \quad T \triangleright E_2 \equiv E_1}{T \triangleright E \equiv E_1}$$

$$\frac{T \triangleright E \equiv E_2 \quad T \triangleright E_2 \not\equiv E_1}{T \triangleright E \not\equiv E_1}$$

If a formula φ is derivable by this system, we write $\vdash_{JD} \varphi$.