Japan Journal of Industrial and Applied Mathematics (2021) 38:677–692
https://doi.org/10.1007/s13160-021-00458-y

ORIGINAL PAPER

Formalisation of Bayesian concealment

Izumi Takeuti[1]

Received: 13 May 2020 / Revised: 10 December 2020 / Accepted: 28 December 2020 /
Published online: 11 February 2021

Abstract

In order to assure the concealment by cryptographic protocols, it is an effective measure to prove the concealment in a formal logical system. In the contemporary context of cryptographic protocol, the concealment has to be proved by using probability theory. There are several concepts of concealment in probability theory. One of them is Bayesian concealment. This study proposes a formal logical system to prove the Bayesian concealment of a secret sharing scheme.

Keywords Probabilistic concealment · Secret sharing · Formal proof · Bayesian theory

Mathematics Subject Classification 94A60 · 03F45

1 Introduction

1.1 Motivation

In order to assure the concealment by cryptographic protocols, it is an effective measure to prove the concealment in a formal logical system. In the contemporary context of cryptographic protocol, the concealment has to be proved by using probability theory. There are several concepts of concealment in probability theory, as is explained by Takeuti [9]. One of them is Bayesian concealment. This study proposes a formal logical system to prove the Bayesian concealment of a secret sharing scheme.

Takeuti and Adachi [10] state two reasons of using formal logical system to assure the concealment by cryptographic protocols as below.

The first is academic: formal logic can sometimes elicit the essential features underlying a proof that may remain hidden if an informal proof is used.

✉ Izumi Takeuti
takeuti@ni.aist.go.jp

[1] National Institute of Advanced Industrial Science and Technology, Umezono, Tukuba, Ibaraki 305-8560, Japan

The second reason is industrial: if you assure only yourself of the concealment of a protocol, you may prove the concealment informally. However, to assure other people of the concealment, you must demonstrate to them the proof of the concealment. Such proofs can be quite difficult to understand, particularly when the proof deals with probability. By itself, proof difficulty does not demonstrate concealment; however, a formal proof can be verified through mechanical checking using, e.g., computing. For these reasons, we use a formal logical system in this paper.

1.2 Concealment by cryptographic protocol

In this study the word of concealment refers to the concept of hiding some secret by a cryptographic protocol as in the study by Takeuti and Adachi [10], in which the concealment is explained as below.

In this study a cryptographic protocol refers to a protocol to use in order to conceal some data from some party.

As an example of a cryptographic protocol, Diffie–Hellman key exchange protocol is a protocol to conceal a secret key from an eavesdropper.

In this protocol, two participants A and B firstly share a finite group G and an element $e \in G$. Then, A generates an integer a and sends e^a to B. Also B generates an integer b and sends e^b to A. At last, A and B share a secret key e^{ab}. It takes too much time for an eavesdropper to obtain the secret key e^{ab} even if it knows sent messages such as G, e, e^a and e^b, according to a conjecture of contemporary mathematics. The secret key is concealed from the eavesdropper in this sense.

In this study we discuss a secret sharing scheme as a cryptographic protocol. In this protocol, the dealer sends a fragment of the secret to each of n participants. There is a threshold t such that a group of participants of number t can restore the secret from their fragments, although a group of participants of number less than t cannot do it. This protocol conceals the secret from a group of participants of number less than t.

1.3 Probabilistic variables

In the modern cryptographic theory, the concept of concealment is written in the words of probabilistic theory. This study proposes a formal logical system with probabilistic variables for proving concealment of cryptography. Some studies on formal systems for probabilistic theory implement probabilistic theory in general formal system of type theory. One of them is the literature [2] by Affeldt, Garrigue and Saikawa. Such studies implement the probabilistic theory as a special case of measure theory, and do not use probabilistic variables. Probabilistic variables are familiar for human, and give a nice abstraction which aids human's abstracted thought. That is why we propose a formal system with probabilistic variables.

1.4 Outline

We explain the preliminaries of probability theory and Bayesian theory in Sect. 2. We list up six concepts of concealment in Sect. 3, which consists of the quotation from the study by Takeuti [9]. We explain secret sharing schemata in Sect. 4. We explain the previous studies on formal logical system for proving concealment in Sect. 5. We propose our formal logical system in Sect. 6. By using this system, we prove the concealment of Shamir's secret sharing scheme in Sect. 7. We explain related works in Sect. 8.

2 Preliminaries of probability theory and Bayesian theory

In this section we put the preliminaries of probability theory and Bayesian theory, which we use to define the concepts of concealment.

2.1 Evenness and independency

The probability space consists of a triple $(\Omega, \mathscr{B}, \mu)$, where Ω is the set of elementary events, $\mathscr{B}$ is the set of measurable sets over Ω, and μ is the probability measure. In this study, the set Ω is always finite, and $\mathscr{B}$ is always the power set of Ω. Thus, for each $E \in \mathscr{B}$, the probability $\mu(E)$ is expressed by the summation $\sum_{\omega \in E} \mu(\{\omega\})$. We use the letters X, Y, $Z, \ldots$ for probabilistic variables. A probabilistic variable X represents a function f_X of Ω into V_X which is the set where X ranges. The notation $\Pr[X = x]$ denotes $\mu(\{\omega \in \Omega | f_X(\omega) = x\})$.

We say that the distribution of X is even when, for each $x \in V_X$, $\Pr[X = x] = 1/|V_X|$. We say that the distributions of X and Y are independent when, for each $x \in V_X$ and each $y \in V_Y$, $\Pr[X = x, Y = y] = \Pr[X = x] \cdot \Pr[Y = y]$.

2.2 Prior distribution and posterior distribution

There appear the concepts of joint probability distribution, prior distribution and posterior distribution in Bayesian theory. The joint probability distribution of X and Y is the distribution

$$(x, y) \mapsto \Pr[X = x, Y = y] \,:\, V_X \times V_Y \to [0, 1].$$

The prior distribution of X is the distribution

$$x \mapsto \Pr[X = x] = \sum_{y \in V_Y} \Pr[X = x, Y = y] \,:\, V_X \to [0, 1].$$

The posterior distribution of X after observing $Y = y$ is the distribution

$$x \mapsto \Pr[X = x, Y = y] \,:\, V_X \to [0, 1].$$

If the distributions of X and Y are independent, then the posterior distribution of X is equal to its prior distribution.

3 Concepts of concealment

As discussed by Takeuti [9], there are several concepts of concealment. The following subsections are the list of six concepts of concealment which is the quotation from his study [9]. In the following explanation, there appear the concepts of computational concealment and Bayesian concealment. Although many studies discuss computational concealment, we discuss Bayesian concealment in this study.

3.1 Possibilistic concealment and probabilistic concealment

Possibilistic concealment Although it is known that the concealed data X is either x_1 or x_0, both $X = x_0$ and $X = x_1$ are possible and the adversary cannot tell which of them is the case.

Probabilistic concealment When the concealed data X is either x_1 or x_0 in probability 1/2, even if the adversary observes any observable variables, both $\Pr[X = x_1]$ and $\Pr[X = x_0]$ are still equal or very near to 1/2 for the adversary.

The concept of 'very near' in the definition of probabilistic concealment should be defined formally. In most cases this concept of 'very near' is defined as in the concept of asymptotic concealment, which appears below.

The words 'possibilistic' and 'probabilistic' appear in the study by O'Neill and Halpern [7]. The concept of possibilistic concealment is called concealment under a non-probabilistic argument in the study by Takeuti and Adachi [10]. Both the studies by O'Neill and Halpern [7] and by Takeuti and Adachi [10] state that possibilistic concealment is weak and probabilistic concealment is desired to discuss the safety of cryptographic protocols.

All of the following four concepts of concealment are the refinements of the concept of probabilistic concealment.

3.2 Asymptotic concealment and information-theoretic concealment

Asymptotic concealment Suppose that the concealed data X is either x_1 or x_0 in probability 1/2. For an arbitrary polynomial p, there is a large number N such that, for any security parameter $n > N$ which is as large as the length of encryption key, in computation time of polynomial of n, for the computation result X', $|\Pr[X = X'] - 1/2|$ is smaller than $1/p(n)$.

Information-theoretic concealment When the concealed data X is either x_1 or x_0 in probability 1/2, even if the adversary observes any observable variables, both $\Pr[X = x_1]$ and $\Pr[X = x_0]$ are still exactly equal to 1/2 for the adversary.

The concept of asymptotic concealment is popular in the context of public-key cryptography, as in the book by Goldreich [5].

Information-theoretic concealment can be realised in the settings of some secret sharing schemes. One of them is Shamir's secret sharing scheme [10], although Shamir did not show information-theoretic concealment of his secret sharing scheme [8].

Not all secret sharing schemes realise information-theoretic concealment. Boyle et al. [3] discuss asymptotic concealment by a secret sharing scheme.

Information-theoretic concealment is stronger than asymptotic concealment is. Therefore, it is better to realise information-theoretic concealment than asymptotic concealment if it is possible. However, it is impossible to realise information-theoretic concealment and only asymptotic concealment is realisable in some settings, namely, the setting of public-key cryptography.

3.3 Computational concealment and Bayesian concealment

Computational concealment When the concealed data X is either x_1 or x_0 in probability 1/2, even if the adversary makes any computation using observable variables in the given computation power, the probability that the adversary guesses the collect value of X is equal to or very near to 1/2.

Bayesian concealment Even if the adversary observes any observable variables, the posterior distribution of the concealed variable is equal to its prior distribution.

We say that the data is concealed Bayesianly when the Bayesian concealment is realised.

If the probabilistic distribution of the observable variables are independent to that of the concealed data, then the concealed data is concealed Bayesianly.

The definition of computational concealment mentions both the concepts of computation and of probability, while the definition of Bayesian concealment mentions only the concept of probability.

3.4 Applicability

The following explanations around the last four concepts in the literature [9].

Two dichotomies are shown around the concept of probabilistic concealment; one dichotomy is asymptotic concealment versus information-theoretic concealment in Sect. 3.2, and the other is computational concealment versus Bayesian concealment in Sect. 3.3. The former one in Sect. 3.2 captures what phenomenon happens, and the latter one in Sect. 3.3 captures the method how to observe the phenomenon. We apply the method indicated by the dichotomy in Sect. 3.3 to observing the phenomenon indicated by the dichotomy in Sect. 3.2.

Not both methods are applicable to both phenomena. The concept of asymptotic concealment is essentially computational, and Bayesian concealment is not applicable to asymptotic concealment. Bayesian concealment is applicable to only information-theoretic concealment. On the other hand, computational concealment is applicable to both asymptotic concealment and information-theoretic concealment.

3.5 Merit of the concept of Bayesian concealment

As the merit of the concept of Bayesian concealment, the concept of Bayesian concealment captures probabilistic concealment more directly than computational concealment does. A formal system for proving computational concealment has to have some devices of computation theory as well as of probabilistic theory. The formal system by Takeuti and Adachi [10] has the undefined function symbol f which denote an arbitrary computation as well as the probabilistic modality. On the other hand, the formal system which we propose in Sect. 6 has only probabilistic predicates.

As the profit of using the concept of Bayesian concealment, the proof of the Bayesian concealment is more direct and easier to analyse than the proof of computational concealment is. Takeuti and Adachi [10] prove the computational concealment of the secret sharing scheme in Sect. 4.3. Although it proves the computational concealment explicitly, the proof uses Bayesian concealment implicitly. In Sect. 3.3 of the literature [10], they prove

$$\Pr[j = f'(x_1 + l_1, x_2 + l_2, \dots, x_k + l_k)] = \Pr[j = f'(x_1, x_2, \dots, x_k)].$$

In this expression, $f'(x_1 + l_1, x_2 + l_2, \dots, x_k + l_k)$ is a linear combination of the observable variables, and $f'(x_1, x_2, \dots, x_k)$ is independent to the secrets. Therefore, this expression implicitly meaning that the observable variables are independent to the secrets, that is, Bayesian concealment is realised here. Their proof of computational concealment is a little hard to analyse. However, in order to prove its information-theoretic concealment, it is sufficient to prove its Bayesian concealment, and it is not necessary to prove its computational concealment. It is much clearer to prove its Bayesian concealment than to prove its computational concealment.

4 Secret sharing system

4.1 Threshold secret sharing scheme

A typical secret sharing scheme realises the following situation. There are n persons, each of which has its own fragment of the secret, and t persons out of them together can restore the secret but $t - 1$ persons cannot. If it realises this situation, then it is called (n, t)-threshold secret sharing scheme.

4.2 Simple secret sharing scheme

We can construct a simple secret sharing system by a finite group G as below.

There are a dealer and two persons P_1 and P_2. The group G is open. There is a secret $X \in G$. The dealer chooses a fresh key Y from G, that is, the distribution of Y is even and independent to that of X. The dealer gives Y to a person P_1 and gives $Z = XY$ to another person P_2. The distribution of Z is also even, and X and Z is also independent, because of the following proposition. Neither P_1 nor P_2 alone can solve the value of X, because X is concealed Bayesianly both from Y and from Z. On the other hand, P_1 and P_2 in collaboration can solve the value of X as $X = ZY^{-1}$.

Proposition 1 *Let G be a finite group and X and Y be probabilistic variables over G. Suppose that the distribution of Y is even and independent to that of X. Put $Z = XY$. Then, the distribution of Z is even and independent to that of X.*

Proof For any $x, z \in G$, it holds that

$$\begin{aligned}\Pr[X = x, Z = z] &= \Pr[X = x, XY = z] = \Pr[X = x, Y = x^{-1}z] \\ &= \Pr[X = x] \cdot \Pr[Y = x^{-1}z] = \Pr[X = x]/|G|.\end{aligned}$$

On the other hand,

$$\begin{aligned}&\Pr[Z = z] = \Pr[XY = z] = \sum_{x\in G} \Pr[X = x, XY = z] = \sum_{x\in G} \Pr[X = x, Y = x^{-1}z] \\ &= \sum_{x\in G} \Pr[X = x] \cdot \Pr[Y = x^{-1}z] = \sum_{x\in G} (\Pr[X = x]/|G|) \\ &= \left(\sum_{x\in G} \Pr[X = x]\right)/|G| = 1/|G|.\end{aligned}$$

Therefore $\Pr[Z = z] = 1/|G|$ and $\Pr[X = x, Z = z] = \Pr[X = x] \cdot \Pr[Z = z]$. □

This is a (2, 2)-threshold secret sharing scheme.

4.3 Shamir's secret sharing scheme

Shamir [8] proposes (n, t)-threshold secret sharing scheme. We will show the construction of his (3, 3)-threshold secret sharing scheme as an example.

Take a finite field F of characteristic ≥ 5.

For a secret data $M \in F$, the dealer takes fresh variables $X_1, X_2 \in F$, that is, their distributions are even, and the distributions of them and M are independent.

The dealer calculates

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \begin{pmatrix} M \\ X_1 \\ X_2 \end{pmatrix}.$$

Then the dealer delivers the data Y_1, Y_2 and Y_3 to three persons P_1, P_2 and P_3 respectively.

By knowing all of Y_1, Y_2, Y_3, one can solve the equation system and obtain M. On the other hand, one cannot obtain M from only two of Y_1, Y_2, Y_3, because the degree of freedom is not enough and one cannot solve the equation system. Therefore, it is (3, 3)-threshold secret sharing scheme.

Shamir [8] discusses (n, t)-threshold secret sharing schemes for general n and t by using general Vandermonde's matrices.

Although Shamir shows only possibilistic concealment of this scheme, it is actually probabilistic concealment, as is shown by Takeuti and Adachi [10].

5 Formal systems in previous studies

There are several previous studies which propose formal systems to prove concealment of cryptographic protocol. We point out two of them.

One is the study by Takeuti and Adachi [10] which proposes the formal logical system which proves the information-theoretic concealment of Shamir's secret sharing scheme. The other is the study by Abadí and Rogaway [1] which proposes the formal system which can show asymptotic concealment of cryptographic protocols with an encryption function.

5.1 Previous system for the secret sharing scheme

Takeuti and Adachi [10] prove its computational concealment of the secret sharing scheme in Sect. 4.3 by using its Bayesian concealment.

In this secret sharing scheme, the secret is M, the random seeds are X_1 and X_2, and the observable variables are Y_1, Y_2 and Y_3. They prove the following fact. Suppose that a party knows only two of the three observable variables, namely, Y_1 and Y_2. Then for an arbitrary function f, the distribution of the result of the calculation $f(Y_1, Y_2)$ is independent to that of M. In other words, the variable M is concealed Bayesianly from Y_1 and Y_2. By using this fact, they prove computational concealment of M from Y_1 and Y_2.

The logical system is a little heavy, since it has modal operators for denoting probability as well as full propositional logical connectives. The proof is also a little heavy to analyse.

In order to assure the probabilistic concealment, it is sufficient to prove Bayesian concealment and it is not necessary to prove computational concealment. In order to prove only Bayesian concealment, we can simplify the system and the proof much more.

5.2 Previous system for the cryptographic protocol with an encryption function

Abadí and Rogaway [1] propose the formal system which can show asymptotic concealment of cryptographic protocols with an encryption function. The system is to derive a term from terms. The system is quite simple.

The terms are defined by the following grammar:

$$M ::= X \mid (M, M) \mid \{M\}_M \mid M^{-1} \quad \text{where } X \text{ is a variable.}$$

The derivation rules are the follows:

$$M, M' \vdash (M, M'), \quad (M, M') \vdash M, \quad (M, M') \vdash M',$$
$$M, K \vdash \{M\}_K, \quad \{M\}_K, K^{-1} \vdash M.$$

They [1] prove that this system enjoys soundness and completeness, where soundness means that, if $M_1, M_2, \dots, M_n \vdash M$ is derivable in this system, then M is obtained from $M_1, M_2, \dots, M_n$, and completeness means that, if $M_1, M_2, \dots, M_n \vdash M$ is not derivable in this system, then M is concealed from $M_1, M_2, \dots, M_n$.

For example, one asserts that X is concealed from $\{X\}_K$ because X is not derived from $\{X\}_K$.

6 Formal system

6.1 Overview

We propose a formal system which proves Bayesian concealment. The targets of this system are formulae without logical connectives. In order to deal with Bayesian concealment, it is necessary to state evenness and independency of probabilistic distribution. Hence the system has the predicates which denote evenness and independency, thus the system targets not terms but formulae. However, this system does not have logical connectives. Therefore, this system is a little more complicated than the system by Abadí and Rogaway [1], but not so as the system by Takeuti and Adachi [10].

We prove the soundness of this system. Its completeness is unknown. Even if it is not complete, the system which proves useful theorems is useful.

We fix a finite field where secret sharing scheme is calculated. Its reason is the same as that in the study by Takeuti and Adachi [10], which states as below.

The secret sharing scheme uses a finite field. In order to deal with general fields, the formal logical system must have a general theory of finite fields, which is a kind of complicated. We would like to divide the problem into two parts: one is that of probability and the other problem is that of general finite fields. In this paper we discuss only probability. Therefore, we fix a particular finite field.

6.2 Syntax

We fix a finite field F.

There are only finite probabilistic variables.

Terms are defined as the following syntax:

$$t ::= X \mid e \mid t + t \mid t \cdot t \mid t^{-1}.$$

where X is a probabilistic variable and $e \in F$.

Formulae are in the following forms:

$$t = t', t \neq t', E(t) \text{ and } I(t_t, t_2, \dots, t_n).$$

A formula $E(t)$ denotes that the distribution of t is even. A formula $I(t_t, t_2, \dots, t_n)$ denotes that the distributions of $t_1, t_2, \dots, t_{n-1}$ and t_n are independent.

A term t is said to be made of $t_1, t_2, \dots, t_n$ when t is a term generated from only $t_1, t_2, \dots, t_n$ and some $e_1, e_2, \dots, e_m \in F$ with only $+, \cdot$ and $(-)^{-1}$.

6.3 Semantics

An assignment ω assigns an element $e \in F$ to each probabilistic variable. Note that there are only finite assignments, because probabilistic variables are finite and F is also finite.

The value $\llbracket t \rrbracket_\omega \in F$ of a term t under an assignment ω is defined in the ordinary way as follows:

$$
\begin{aligned}
&\llbracket X \rrbracket_\omega = \omega(X) \quad \text{where } X \text{ is a probabilistic variable,}\\
&\llbracket e \rrbracket_\omega = e \quad \text{where } e \in F,\\
&\llbracket t + t' \rrbracket_\omega = \llbracket t \rrbracket_\omega + \llbracket t' \rrbracket_\omega,\\
&\llbracket t \cdot t' \rrbracket_\omega = \llbracket t \rrbracket_\omega \cdot \llbracket t' \rrbracket_\omega,\\
&\llbracket t^{-1} \rrbracket_\omega = \llbracket t \rrbracket_\omega^{-1} \quad \text{when } \llbracket t \rrbracket_\omega \neq 0, \text{ and } \llbracket t^{-1} \rrbracket_\omega = 0 \text{ when } \llbracket t \rrbracket_\omega = 0.
\end{aligned}
$$

We define $\llbracket 0^{-1} \rrbracket_\omega = 0$ in order to make $\llbracket - \rrbracket$ a total function over terms, although 0^{-1} is undefined in mathematics.

The probability space here is $(\Omega, \mathscr{B}, \mu)$ where the underlying set Ω is the set of all the assignment of elements in F to probabilistic variables, the Borel family $\mathscr{B}$ is the power set of Ω, and μ is a probability measure over $\mathscr{B}$.

In the following text, the notation $\Pr[t_1 = t'_1, t_2 = t'_2, \dots, t_n = t'_n]$ denotes

$$\mu(\{\omega \in \Omega | \llbracket t_1 \rrbracket_\omega = \llbracket t'_1 \rrbracket_\omega, \llbracket t_2 \rrbracket_\omega = \llbracket t'_2 \rrbracket_\omega, \dots, \llbracket t_n \rrbracket_\omega = \llbracket t'_n \rrbracket_\omega\}).$$

For a formula ϕ, the truth value $\llbracket \phi \rrbracket_\mu \in \{\mathsf{true}, \mathsf{false}\}$ is defined as follows:

$$
\begin{aligned}
&\llbracket t = t' \rrbracket_\mu = \mathsf{true} \iff \llbracket t \rrbracket_\omega = \llbracket t' \rrbracket_\omega \quad \text{for each } \omega \in \Omega,\\
&\llbracket t \neq t' \rrbracket_\mu = \mathsf{true} \iff \llbracket t \rrbracket_\omega \neq \llbracket t' \rrbracket_\omega \quad \text{for each } \omega \in \Omega,\\
&\llbracket E(t) \rrbracket_\mu = \mathsf{true} \iff \Pr[t = e] = 1/|F| \quad \text{for each } e \in F,\\
&\llbracket I(t_1, t_2, \dots, t_n) \rrbracket_\mu = \mathsf{true}\\
&\qquad \iff \Pr[t_1 = e_1, t_2 = e_2, \dots, t_n = e_n] = \prod_{i=1,2,\dots,n} \Pr[t_i = e_i]\\
&\qquad \text{for each } (e_1, e_2, \dots, e_n) \in F^n.
\end{aligned}
$$

One can calculate both of $\llbracket t = t' \rrbracket_\mu$ and $\llbracket t \neq t' \rrbracket_\mu$ because Ω is finite. Note that $\llbracket t = t' \rrbracket_\mu$ and $\llbracket t \neq t' \rrbracket_\mu$ are independent to μ.

We say ϕ is valid and write $\models \phi$ when $\llbracket \phi \rrbracket_\mu = \mathsf{true}$ for any μ.

6.4 Inference rules

The inference rules are listed below:

Rule 1. $\vdash t = t'$ where $[\![t = t']\!]_\mu = \mathsf{true}$,
Rule 2. $\vdash t \neq t'$ where $[\![t = t']\!]_\mu = \mathsf{true}$,
Rule 3. $t = t', \phi(t) \vdash \phi(t')$,
Rule 4. $I(t_1, t_2, \dots, t_n) \vdash I(t'_1, t'_2, \dots, t'_m)$ where $\{t'_1, t'_2, \dots, t'_m\} \subset \{t_1, t_2, \dots, t_n\}$,
Rule 5. $\vdash I(t)$,
Rule 6. $I(t_1, t_2, \dots, t_n) \vdash I(t_1, t_2, \dots, t_n, e)$ where $e \in F$,
Rule 7. $I(t_1, t_2, \dots, t_n, t'_1, t'_2, \dots, t'_m) \vdash I(t_1, t_2, \dots, t_n, t')$. where t' is made of $t'_1, t'_2, \dots, t'_m$,
Rule 8. $E(t), I(t, t_1, t_2, \dots, t_n) \vdash I(t + t', t_1, t_2, \dots, t_n)$. where t' is made of $t_1, t_2, \dots, t_n$,
Rule 9. $E(t), I(t, t'), t' \neq 0 \vdash E(t \cdot t')$.

6.5 Soundness

We show the soundness of the logical system in this section.

Theorem 1 *Suppose $\phi_1, \phi_2, \dots, \phi_n \vdash \phi$ and $\vDash \phi_i$ for each $i = 1, 2, \dots, n$. Then $\vDash \phi$.*

Proof The proof is done by showing that each rule above preserves the validity.
Rules 1, 2 and 5: They follow from the definition directly.
Rules 3, 4 and 6: Easy.
Rule 7: It follows from Lemma 1.
Rule 8: It follows from Lemma 2.
Rule 9: It follows from Lemma 3. □

In the proofs of the following lemmata, in order to distinguish from comparison of the values of terms, we use the symbol $\equiv$ to denote that two are of the same form, that is, we write $t \equiv t'$ to denote that the term t is the same term as t'.

Lemma 1 *Let $\bar{t}$ be the sequence $t_1, t_2, \dots, t_m$ and $\bar{t}'$ be the sequence $t'_1, t'_2, \dots, t'_m$. If $\vDash I(\bar{t}', \bar{t})$ and u is a term made of $\bar{t}$, then $\vDash I(\bar{t}', u)$.*

Proof Let $x_1, x_2, \dots, x_n$ be variables.

Because u is a term made of $\bar{t}$, there is some term $u_*(x_1, x_2, \dots, x_n)$ which is made of $x_1, x_2, \dots, x_n$ such that $u \equiv u_*(\bar{t})$.

For $e \in F$, the set $u_*^{-1}(e) \subset F^n$ is defined as

$$u_*^{-1}(e) = \{(e_1, e_2, \dots, e_n) | e = u_*(e_1, e_2, \dots, e_n)\}.$$

As the assumption, for any $e_1, e_2, \dots, e_n, e'_1, e'_2, \dots, e'_m$ in F, it holds that

$$\begin{aligned}&\Pr[t_1 = e_1, t_2 = e_2, \dots, t_n = e_n, t'_1 = e'_1, t'_2 = e'_2, \dots, t'_m = e'_m]\\&= \left(\prod_{i=1,2,\dots,n} \Pr[t_i = e_i]\right) \cdot \prod_{i=1,2,\dots,m} \Pr[t'_i = e'_i].\end{aligned}$$

Let $e, e'_1, e'_2, \dots, e'_m$ be arbitrary elements in F. Then,

$$\begin{aligned}&\Pr[t'_1 = e'_1, t'_2 = e'_2, \dots, t'_m = e'_m, u = e]\\&= \sum_{(e_1,e_2,\dots,e_n)\in u_*^{-1}(e)} \Pr[t_1 = e_1, t_2 = e_2, \dots, t_n = e_n, t'_1 = e'_1, t'_2 = e'_2, \dots, t'_m = e'_m]\\&= \sum_{(e_1,e_2,\dots,e_n)\in u_*^{-1}(e)} \left(\prod_{i=1,2,\dots,n} \Pr[t_i = e_i]\right) \cdot \prod_{i=1,2,\dots,m} \Pr[t'_i = e'_i]\\&= \left(\prod_{i=1,2,\dots,m} \Pr[t'_i = e'_i]\right) \cdot \sum_{(e_1,e_2,\dots,e_n)\in u_*^{-1}(e)} \prod_{i=1,2,\dots,n} \Pr[t_i = e_i]\\&= \left(\prod_{i=1,2,\dots,m} \Pr[t'_i = e'_i]\right) \cdot \Pr[u = e].\end{aligned}$$

Therefore $\models I(\bar{t}', u)$. □

Lemma 2 *Let $\bar{t}$ be the sequence $t_1, t_2, \dots, t_n$. If $\models E(t)$, $\models I(t, \bar{t})$ and u is a term made of $\bar{t}$, then $\models I(t + u, \bar{t})$.*

Proof Let $x_1, x_2, \dots, x_n$ be variables.

Because u is a term made of $\bar{t}$, there is some term $u_*(x_1, x_2, \dots, x_n)$ which is made of $x_1, x_2, \dots, x_n$ such that $u \equiv u_*(\bar{t})$.

For $e \in F$, the set $u_*^{-1}(e) \subset F^n$ is defined as

$$t_*^{-1}(e) = \{(e_1, e_2, \dots, e_n) | e = u_*(e_1, e_2, \dots, e_n)\}.$$

As the assumption, $\Pr[t = e] = 1/|F|$ for each $e \in F$.

As the assumption, for any $e, e_1, e_2, \dots, e_n$ in F, it holds that

$$\begin{aligned}&\Pr[t = e, t_1 = e_1, t_2 = e_2, \dots, t_n = e_n]\\&= \Pr[t = e] \cdot \prod_{i=1,2,\dots,n} \Pr[t_i = e_i] = \left(\prod_{i=1,2,\dots,n} \Pr[t_i = e_i]\right)/|F|.\end{aligned}$$

Let $e, e_1, e_2, \dots, e_n$ be arbitrary elements in F. Then,

$$
\begin{aligned}
&\Pr[t+u=e, t_1=e_1, t_2=e_2, \ldots, t_n=e_n] \\
&\quad = \sum_{e' \in F} \Pr[t+u=e, u=e', t_1=e_1, t_2=e_2, \ldots, t_n=e_n] \\
&\quad = \sum_{e' \in F} \Pr[t=e-e', u=e', t_1=e_1, t_2=e_2, \ldots, t_n=e_n] \\
&\quad = \sum_{e' \in F} \Pr[t=e-e', u_*(e_1, e_2, \ldots, e_n)=e', t_1=e_1, t_2=e_2, \ldots, t_n=e_n] \\
&\quad = \sum_{e' \in F} \sum_{(e_1, e_2, \ldots, e_n) \in u_*^{-1}(e')} \Pr[t=e-e', t_1=e_1, t_2=e_2, \ldots, t_n=e_n] \\
&\quad = \sum_{e' \in F} \sum_{(e_1, e_2, \ldots, e_n) \in u_*^{-1}(e')} (\Pr[t_1=e_1, t_2=e_2, \ldots, t_n=e_n]/|F|) \\
&\quad = \left(\sum_{e' \in F} \sum_{(e_1, e_2, \ldots, e_n) \in u_*^{-1}(e')} \Pr[t_1=e_1, t_2=e_2, \ldots, t_n=e_n] \right) / |F| \\
&\quad = \left(\sum_{e' \in F} \Pr[u_*(e_1, e_2, \ldots, e_n)=e', t_1=e_1, t_2=e_2, \ldots, t_n=e_n] \right) / |F| \\
&\quad = \left(\sum_{e' \in F} \Pr[u=e', t_1=e_1, t_2=e_2, \ldots, t_n=e_n] \right) / |F| \\
&\quad = \Pr[t_1=e_1, t_2=e_2, \ldots, t_n=e_n])/|F| = \left(\prod_{i=1,2,\ldots,n} \Pr[t_i=e_i] \right) / |F| \\
&\quad = \Pr[t=e] \cdot \prod_{i=1,2,\ldots,n} \Pr[t_i=e_i].
\end{aligned}
$$

Therefore $\models I(t+u, \overline{t})$. □

Lemma 3 *If* $\models E(t), \models I(t, t')$ *and* $\models t' \neq 0$, *then* $\models E(t \cdot t')$.

Proof It holds $\Pr[\phi, t'=0]=0$ because $\models t' \neq 0$.

Let e be an arbitrary element in F. Then,

$$\begin{aligned}
\Pr[tt' = e] &= \sum_{e' \in F} \Pr[tt' = e, t' = e'] \\
&= \left(\sum_{e' \in F - \{0\}} \Pr[tt' = e, t' = e'] \right) + \Pr[tt' = e, t' = 0] \\
&= \sum_{e' \in F - \{0\}} \Pr[t = ee'^{-1}, t' = e'] = \sum_{e' \in F - \{0\}} \Pr[t = ee'^{-1}] \Pr[t' = e'] \\
&= \sum_{e' \in F - \{0\}} (\Pr[t' = e'] / |F|) = \left(\sum_{e' \in F - \{0\}} \Pr[t' = e'] \right) / |F| \\
&= \left(\left(\sum_{e' \in F - \{0\}} \Pr[t' = e'] \right) + \Pr[t' = 0] \right) / |F| = \left(\sum_{e' \in F} \Pr[t' = e'] \right) / |F| = 1/|F|.
\end{aligned}$$

□

7 Proof of Bayesian concealment in secret sharing scheme

In this section we prove Bayesian concealment of the secret sharing system of Sect. 4.3 in the formal system of Sect. 6.

In the secret sharing system of Sect. 4.3, there are probabilistic variables M, X_1, X_2, Y_1, Y_2 and Y_3. The variable where M is a secret, The variables X_1 and X_2 are fresh variables, that is, the distributions of X_1 and X_2 are even and M, X_1 and X_2 are independent, The variables Y_1, Y_2 and Y_3 are calculated as

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \begin{pmatrix} M \\ X_1 \\ X_2 \end{pmatrix}.$$

Although one can calculate M from all of Y_1, Y_2 and Y_3, it is concealed Bayesianly from two of them.

We show the formal proof of the Bayesian concealment of M from Y_1 and Y_2.

1. $I(M, X_1, X_2) \cdots$ Assumption.
2. $E(X_1) \cdots$ Assumption.
3. $E(X_2) \cdots$ Assumption.
4. $Y_1 = M + X_1 + X_2 \cdots$ Assumption.
5. $Y_2 = M + 2X_1 + 4X_2 \cdots$ Assumption.
6. $I(M, M + X_1 + X_2, X_2) \cdots$ By Rule 8 from 1 and 2.
7. $I(M, M + X_1 + X_2, X_2 + (M + X_1 + X_2) - M/2) \cdots$ By Rule 8 from 3 and 6.
8. $I(M, M + X_1 + X_2, 2(X_2 + (M + X_1 + X_2) - M/2)) \cdots$ By Rule 7 from 7.
9. $I(M, M + X_1 + X_2, M + 2X_1 + 4X_2) \cdots$ By Rule 1 from 8.
10. $I(M, Y_1, Y_2) \cdots$ By Rule 3 from 4, 5 and 9.

Therefore, it is proved that the probabilistic distributions of M, Y_1 and Y_2 are independent, that is, M is concealed Bayesianly from Y_1 and Y_2.

This proof is the inverse way of row reduction to solve the equation system. The concealment of Shamir's secret sharing system depends on the unsolvability of the linear equation system. Thus, the proof of its concealment follows the steps of solving the linear equation system. While the proof in the literature [10] uses the inverse matrix, the proof in this study follows the inverse way of row reduction step by step.

8 Future work

We proposed a formal logical system which proves the Bayesian concealment. Our system shows which operations in field theory preserve the evenness and the independency of probabilistic distributions. Therefore, our system proves the concealment of only the cryptographic protocols based on fields theory. Especially, this system is applied to only one example which is the concealment of Shamir's secret sharing scheme. To apply this system to more examples is a future work.

9 Related works

As is explained in Sect. 5.2, Abadí and Rogaway [1] define a formal system which proves one can computed a term from other terms, and show the completeness of the system for a computational model. Their system targets not formulae but a terms. Its completeness yields that if a term is not derived from the set of other terms, then the term is concealed from the person who knows only the set of terms. The concealment which is proved here is asymptotic concealment.

In their theory, the impossibility of derivation yields concealment. Hence its completeness is necessary. On the other hand, our system derives the independency of terms which implies the concealment. Hence its soundness is sufficient and its completeness is not required.

As is explained in Sect. 5.1, Takeuti and Adachi [10] propose a formal logical system which proves the probabilistic concealment of Shamir's secret sharing scheme. Their system has full Boolean logical connectives and modal operators for denoting probability. The system is a little heavy, and the proof is a little hard to analyse. On the other hand, our system in this study has no logical symbols and the proof is easy to analyse.

Affeldt et al. [2] implement probabilistic theory in the general logical system Coq, and develop the theory of conditional probability. The theory of conditional probability can describe independency of events, therefore it can deal with Bayesian concealment. They regard probabilistic theory as a special case of measure theory. The implementation does not use probabilistic variables but uses the functions represented by propositional variables, that is, they use the expression $\mu\{\omega \in \Omega | f_X(\omega) = x\}$ instead of $\Pr[X = x]$. They use probabilistic variables in informal expressions, but do not give formal expressions with probabilistic variables.

Some studies on formal systems for probability discuss modal logic for probabilistic transitions. One of them is the literature [6] by Aviad Heifetz and Philippe Mongin. They axiomatise modal logic for probabilistic transitions and prove the soundness and completeness of the axiomatisation. The logic for probabilistic transitions cannot write independency of events, therefore it cannot deal with Bayesian concealment.

Dougherty and Guttman [4] define a formal theory of fields in order to prove the security of a modification of Diffie–Hellman key exchange protocol against man-in-the-middle attack. The result is not a direct theorem of the formal system but a conclusion of a discussion of informal logic with an aid of formal theory.

Acknowledgements The author is grateful to Prof. Yasuyuki Tsukada for discussions and comments. The author is in dept to anonymous referees for advice and comments.

References

1. Abadí, M., Rogaway, P.: Reconciling two views of cryptography (the computational soundness of formal encryption). J. Cryptol. **15**, 103–127 (2002)
2. Affeldt, R., Garrigue, J., Saikawa, T.: Reasoning with conditional probabilities and joint distributions in Coq. Comput. Softw. **37**(3), 79–95 (2020)
3. Boyle, E., Gilboa, N., Ishai, Y., Lin, H., Tessaro, S.: Foundations of homomorphic secret sharing. In: Karlin, A.R. (ed.) 9th Innovations in theoretical computer science conference (ITCS 2018), Leibniz international proceedings in informatics (LIPIcs), vol. 94, pp. 21:1–21:21. Schloss Dagstuhl–Leibniz-Zentrum fúr Informatik (2018)
4. Dougherty, D.J., Guttman, J.D.: An algebra for symbolic Diffie–Hellman protocol analysis. In: Palamidessi, C., Ryan, M. (eds.) Trustworthy global computing. TGC 2012. Lecture Notes in Computer Science, vol. 8191, pp. 164–181. Springer, Berlin (2012)
5. Goldreich, O.: Foundations of Cryptography, vol. I. Cambridge University Press, Cambridge (2008)
6. Heifetz, A., Mongin, P.: Probability logic for type spaces. Games Econ. Behav. **35**, 31–53 (2001)
7. O'Neill, K.R., Halpern, J.Y.: Secrecy in multiagent systems. ACM Trans. Inf. Syst. Secur. **12**(5), 1–47 (2003)
8. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
9. Takeuti, I.: Bayesian concealment. In: Adachi, T. (ed.) Algebraic System, Logic, Language and Related Areas in Computer Science II, RIMS Kôkyûroku. Kyoto University, Kyoto (2021, to appear)
10. Takeuti, I., Adachi, T.: Formalisation of probabilistic concealment. Jpn. J. Ind. Appl. Math. **36**(2), 473–495 (2019)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.