Bayesian Concealment

竹内泉
Takeuti Izumi
AIST

Abstract. There are many concepts of concealment in the context of cryptographic protocols. This study proposes the concept of Bayesian concealment as the counter part of the concept of computational concealment, and states the merit of the concept of Bayesian concealment in proving the concealment.

1 Introduction

There are many concepts of concealment proposed and discussed in the context of cryptographic protocols [1]. The words of concealment is explained in the literature [2] as follows.

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 shares 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 shares a secret key e^{ab}. It takes too much time for an eavesdropper to obtain the secret key e^{ab} even if it knows the 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.

That is the explanation in the literature [2].

Most literatures discuss computational concealment, in which the concealment is defined as it is impossible or too hard to calculate the secret from observable variables. On the other hand, we can define the concealment as the posterior distribution of the secret is equal to the prior distribution of the secret when the observable variables are observed. We call this concealment Bayesian concealment. We put the formal definitions of computational concealment and Bayesian concealment in Subsection 2.3.

2 Concepts of Concealment

In this section we list three pairs of concepts of concealment.

2.1 Probabilistic 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 case 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 literature [1]. The concept of possibilistic concealment is called concealment under a non-probabilistic argument in the literature [2], which states that concealment under a probabilistic argument is stronger than under a non-probabilistic argument.

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

2.2 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 literature [3]

Information-theoretic concealment can be realised in the settings of some secret sharing schemes. One of them is Shamir's secret sharing scheme [2], although Shamir did not show information-theoretic concealment of his secret sharing scheme [5].

Not all secret sharing schemes realise information-theoretic concealment. The literature [4] discusses asymptotic concealment by a secret sharing scheme.

2.3 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.

3 Applicability

The previous section, two dichotomies are shown around the concept of probabilistic concealment; one dichotomy is asymptotic concealment versus information-theoretic concealment in Subsection 2.2, and the other is computational concealment versus Bayesian concealment in Subsection 2.3. The former one in Subsection 2.2 captures what phenomenon happens, and the latter one in Subsection 2.3 captures the method how to observe the phenomenon. We apply the method indicated by the dichotomy in Subsection 2.3 to observing the phenomenon indicated by the dichotomy in Subsection 2.2.

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.

	Asymptotic concealment	Information-theoretic concealment
Computational concealment	applicable	applicable
Bayesian concealment	NOT	applicable

4 Merit of the Concept of Bayesian Concealment

In comparing to the concept of computational concealment, the merit of the concept of Bayesian concealment is to be easy to prove the concealment. In the literature [2] the computational concealment of Shamir's secret sharing scheme is proved in the formal logical system by using its Bayesian concealment. The formal proof of it 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 mush clearer to prove its Bayesian concealment than to prove its computational concealment.

Acknowledgement

The author is grateful to Tsukada Yasuyuki and Yamamura Akihiro for their comments.

References

[1] Kevin R. O'Neill and Joseph Y. Halpern, Secrecy in Multiagent Systems, ACM Trans. Inf. Syst. Secur., Vol. 12, Num. 5, pp1–47, 2003.

[2] Izumi Takeuti and Tomoko Atachi, Formalisation of Probabilistic Concealment, Japan J. Indust. Appl. Math., Vol. 36, Num. 2, pp473–495, 2019.

[3] Oded Goldreich, Foundations of Cryptography Volume I, Cambridge University Press, 2008.

[4] Elette Boyle, Niv Gilboa, Yuval Ishai, Huijia Lin and Stefano Tessaro, Foundations of Homomorphic Secret Sharing, Anna R. Karlin eds, 9th Innovations in Theoretical Computer Science Conference (ITCS 2018), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 94, pp21:1–21:21, Schloss Dagstuhl–Leibniz-Zentrum fúr Informatik, 2018.

[5] Adi Shamir, How to Share a Secret, Commun. of the ACM, Vol. 22 Num. 11, pp612–613, 1979.