B-011

# A Case Study of Formal Analysis Methods with Reasoning for Cryptographic Protocols

Jun Zheng[1] Yuichi Goto[1]

***Abstract***: Formal analysis method with reasoning is an alternative formal analysis method for cryptographic protocols. Three formal analysis methods with reasoning are proposed to detect the flaws related to confidentiality, authentication, fairness, non-repudiation and anonymity. However, there is no study to investigate the effectiveness of those three methods with a case study. To investigate the effectiveness of the three formal analysis methods with reasoning, this paper conducts a case study to analyze 30 cryptographic protocols with the methods. Results of the case study that one method is ineffective and the other two methods are effective to check the cryptographic protocols.

***Keywords***: Cryptographic protocols; Formal analysis; Formalization; Forward reasoning; Analysis

## 1. Introduction

A cryptographic protocol is a network protocol based on the theory of cryptography, through the combination of message, key and cryptographic algorithm to achieve the network environment of identity authentication, the exchange of session keys and other security objectives. With the development of network technology, the cryptographic protocol's flaws will cause huge losses to the network.

Formal analysis is used to find out the flaws of cryptographic protocols [4][11][12]. Formal analysis method with reasoning is an alternative formal analysis method for cryptographic protocols. Formal analysis method based on theorem proving system and model checking system can be regarded as "proving methods". The proving methods differs from the reasoning method in that the analysts do not need to enumerate the targets of analysis of a cryptographic protocol before doing formal analysis. Instead of the proving methods, the reasoning method uses the formalized *participants behaviors* and *intruder behaviors* of a cryptographic protocol as premises of forward reasoning. Through forward reasoning, all possible the participants and the intruder's activities in the protocol will be deduced. The analyst checks whether the deductive activity represented by the logical formulas are related to the flaw of security properties for protocols.

Three formal analysis methods with reasoning are proposed to detect the flaws related to confidentiality, authentication, fairness, non-repudiation and anonymity. However, there is no study to investigate the effectiveness of those three methods with a case study.

This paper shows a case study to verify the effectiveness of the proposed three formal analysis methods with reasoning. As the case study, we analyzed 30 cryptographic protocols by the three reasoning methods.

## 2. Basic Notions

A cryptographic protocol is a protocol that uses encryption to perform security-related functions. The security-related function is to prevent unauthorized entity access to information or the intentional but unauthorized destruction or alteration of that information.

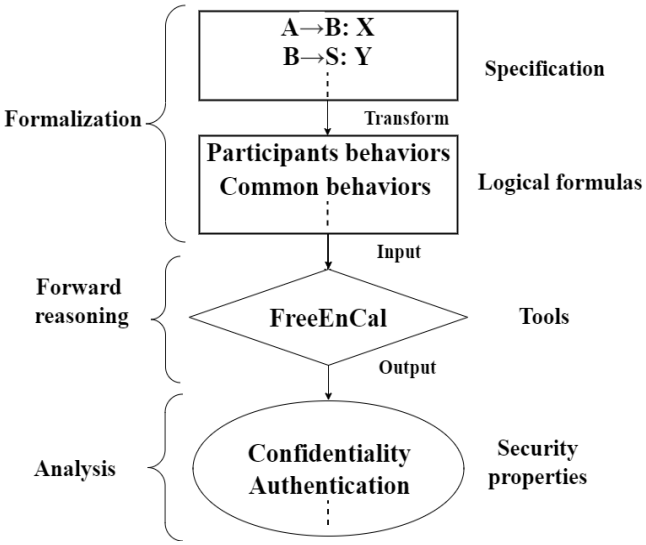


**Figure 1**. Overview of formal analysis method with reasoning

Security properties are used as a standard to determine whether the encryption protocol has flaw [17]. A cryptographic protocol that does not satisfy the security properties corresponding to the security requirements leads to the generation of flaws. Therefore, security properties are considered the criteria for determining whether flaws exist. The security properties of cryptographic protocols include confidentiality, authentication, fairness, non-repudiation, anonymity, and atomicity [17].

[1] Saitama University

## 3. Formal Analysis Method with Reasoning

Three formal analysis methods with reasoning were proposed. The first one is to detect flaws related to confidentiality and authentication proposed by Wagatsuma et al. (Wagatsuma method for short) [14][16]. The second one is to detect flaws related to non- repudiation, fairness and proposed by Yan et al. (Yan method for short) [18]. The final one is to detect flaws related to anonymity proposed by Wang et al. (Wang method for short) [15].

Figure 1 shows an overview of the formal analysis method with reasoning. The method consists of three phases: formalization, forward reasoning, and analysis.

In formalization phase, analysts formalize the behavior rules based on first-order predicate strong relevant logics [2] and transform specification into logical formulas. The logical formulas included the *participants behaviors*, *intruder behaviors*, *common behaviors*, *confirm behaviors* and *anonymous behaviors*. *Participants behavior* is referred to as a set of behavior rules for participant to send or receive data. *Intruder behavior* refers to the set of behavior rules of intruders, and the behavior of intruders is based on the Dolev-Yao model [5]. *Common behaviors* mainly describe implicit behaviors such as encryption or decryption behaviors of participants. *Confirm behavior* is the basis for the participants to judge whether the received message is correct or not. The *confirm behavior* is used to detect flaws related to non-repudiation and fairness in Yan method. *Anonymity behavior* provides the participants with the basis for judging whether the identity is protected or not. The *anonymity behavior* is used to detect flaws related to anonymity in Wang method.

The proposed methods give following predicates:

- *Start* (*p1, p2*)*: p1 and p2 start a communication process.*
- *Send* (*p1, p2, x*)*: p1 sends x to p2.*
- *Parti* (*p*)*: p is a participant of a protocol.*
- *Eq* (*x1, x2*)*: x1 and x2 are equal.*
- *Get* (*p, x*)*: p gets x.*
- *Recv* (*p, x*)*: p receives x.*

The proposed methods give following functions:

- *Data* (*x1 … xn*)*: A data set of sent and received.*
- *Enc* (*k, x1 … xn*)*: A data set that consists of encrypted*
- *Id* (*p*)*: Identifier of p.*
- *Nonce* (*p*)*: Nonce of p.*
- *Old* (*x*)*: Old data of x.*
- *Pk* (*p*)*: Public key of p.*
- *Plus* (*x*)*: Incremented data of x.*
- *Sig* (*p, x1 … xn*)*: A data set of signature.*
- *Symk* (*p1, p2*)*: p1 and p2 are symmetric key.*
- *Tstamp* (*p*)*: p is the timestamp.*

In forward reasoning phase, analysts obtain possible status and actitivies of participants and intruders in the target protocol by forward reasoning. In the three methods, forward reasoning is done automatically by using FreeEnCal [3].

Forward reasoning phase is different between Wagatsuma method and the other two methods. Forward reasoning is done one time in Yan and Wang method. In the two methods, analysts use participant behaviors, common behaviors, and anonymous behaviors as premise of forward reasoning, and obtain all possible activities of participants and final status of the target protocol. On the other hand, forward reasoning is done many times in Wagatsuma method. The operation is analysts put logical formulas of participants behaviors, common behaviors, and intruder behaviors into FreeEnCal. Based on the results of first forward reasoning, the analyst creates tampered data and then adding the tampered data to the logical formulas. Repeat the above operations until the final step of the cryptographic protocol.

In analysis phase, analysts analyze the deduced formulas in each result of forward reasoning. According to three reasoning methods, the targets of analyzing logical formulas are as follows.

In Wagatsuma method, the target of logical formulas include the intruder get the secret data, or any participant received the falsified data.

In Yan method, the target of logical formulas include participants who have confirmed the data they should receive, and also include participant has confirmed the target data, but the other has not.

In Wang method, the target of logical formulas is the participant protecting his identity in the protocol, and the other part does not protect the identity's data.

## 4. Case Study

### 4.1 Purpose and Conditions

The purpose of case studies is to confirm whether the three methods can apply various cryptographic protocols or not.

We can say that a formal analysis method with reasoning can be applied to a cryptographic protocol if the method satisfies the following conditions.

1) Analysts can formalize specification of the target protocol according to the method.
2) Analysts can detect flaws related to target security properties by the method if the flaws of the target protocol has been known.
3) Analysts cannot detect any flaw related to target security properties by the method if the target protocol does not have any flaws related to the target security properties.

In order to verify whether the three formal analysis methods with reasoning can be used in variety of cryptographic protocols, we analyzed 30 cryptographic protocols by using the three reasoning methods as a case study.

The protocols are as follows:

- F1: ISO/IEC 11770-2 Key Establishment Mechanism 1 to 6 [9]
- F2: ISO/IEC 11770-2 Key Establishment Mechanism 7 to 10 [9]
- F3: ISO/IEC 11770-2 Key Establishment Mechanism 12 to 13 [9]

- F4: ISO/IEC 11770-3 Key Agreement Mechanism 1 to 6 [8]
- F5: Kao Chow Authentication v1 to v3 [13]
- F6: Needham Schroeder Symmetric Key [12]
- F7: Amended Needham Schroeder Symmetric Key [12]
- F8: Lowe fixed version of Needham Schroeder Public Key [6]
- F9: Lowe modified Denning Sacco Shared Key [7]
- F10: Denning-Sacco Shared Key [7]
- F11: SKID 2 to 3 [1]

In this paper, we showed one of 30 analysis: The analysis of ISO/IEC 11770-2 key establishment mechanism 11 as a sample of this case study. The specification of ISO/IEC 11770-2 key establishment mechanism 11 is as follows.

*1)* $A \rightarrow S$ : $\{id(B), F\}\ Kas$

*2)* $S \rightarrow A$ : $\{id(A), F\}\ Kbs$

*3)* $A \rightarrow B$ : $\{id(A), F\}\ Kbs$

The communication according to the protocol is the following steps:

- In step 1, the participant *A* requests key translation by sending message to the *S* (key translation center *S*), The message {i*d*(*B*), *F*} is encrypted using the key *Kas* shared between *A* and *S*, where *id*(*B*) is the identifier of the participant *B* and *F* is a keying material made up of the target key *K*. After receiving the message, the *S* decrypt it to get F, attach the distinguishing identifier *id*(A), and encrypts both using the key *Kbs* to get {*F*, *A*} *Kbs*.
- In step 2, the *S* sends the generated message to *A*.
- In step 3, *A* transfers the received message to *B*. *B* decrypts the message, and checks whether *id*(A) is correct or not, and then obtains the key *K* from *F*.

In the formalization phase, at first, we translated the above specification to following logical formulas:

*1)* *Start* (*p1*, *p2*) →
*Send* (*p1*, *S*, *data*(enc(*symk*(*p1*, *S*), *id*(*p2*), *F*)))

*2)* *Recv* (*S*, *data*(enc(*symk*(*p1*, *S*), *id*(*p2*), *F*))) →
*Send* (*S*, *p1*, *data*(*enc*(*symk*(*p2*, *S*), *F*, *id*(*p1*))))

*3)* *Recv* (*p1*, *data*(*enc*(*symk*(*p2*, *S*), *F*, *id*(*p1*)))) →
*Send* (*p1*, *p2*, *data*(*enc*(*symk*(*p1*,*S*), *F*, *id*(*p1*))))

After that, we generated 31 logical formulas that represented *participants behaviors*, *common behaviors*, *confirm behaviors*, *and anonymous behaviors* from the specification according to the proposed three reasoning methods.

In the forward reasoning phase, we translated those 34 logical formulas into the data format for FreeEnCal, and then do forward reasoning by FreeEnCal. By forward reasoning, 1,058 logical formulas were deduced.

In the analysis phase, we checked whether there are logical formulas related to security properties. Based on Wagatsuma method, if intruders get original data and send tampered data, then the protocol does not satisfy confidentiality and authentication. But after the forward reasoning, we failed to create tampered data, so we cannot analyze ISO/IEC 11770-2 key establishment mechanism 11 by Wagatsuma method.

Based on Yan method, if all participants have confirmed the data they should receive, the cryptographic protocol has satisfying non-repudiation. In addition, if one participant deceives another participant, the other participant cannot confirm the received data, it indicates the protocol does not satisfy fairness. In the deduced formulas, we found that *Cof*(*A*, *B*, *id*(*A*)) was deduced, according to *confirm behaviors*, it means that the participant *A* can confirm that *B* has the responsibility of *id*(*A*), that is, *A* received the *id*(*A*). We also found that *Recv*(*B*, *data*(*enc*(*symk*(*B*, *S*), *F*, *id*(*A*))) which means that *B* cannot decrypt the message, so *B* cannot check whether *id*(*A*) is correct or not. From the above, if *B* can get the *id*(*A*), then the logical formula is *Recv*(*B*, *data*(*F*, *id*(*A*))), but *B* cannot get the *id*(*A*), so it does not satisfy non-repudiation. Furthermore, *A* receives *id*(*A*), but *B* does not receive *id*(*A*), the protocol also does not satisfy fairness.

Based on Wang method, if a participant protects the identity in the protocol, the other part does not protect the data of this identity, then this participant keeps anonymity. On the contrary, the identity data is protected by other participants, which means that the identity is leaked, so the protocol does not satisfy anonymity. In the result of case study, the formulas include ¬ *Anoy*(*S*, *id*(*A*)) was deducted, which means *A*'s identity is not protected, and *S* knows *A*'s identity information. And then, we found out formulas of *Anoy*(*B*, *id*(*A*)), which means participant *B* protects *A's* identity, so the *A*'s identity is leaked, and the protocol does not satisfy anonymity.

### 4.2 Results of the Case Study

**Table 1**. Comparison of the feasibility of the three methods

| Cryptographic Protocols | Three formal analysis method with reasoning | | |
|---|---|---|---|
| | Yan | Wang | Wagatsuma |
| F1 | ○ | ○ | — |
| F2 | — | — | — |
| F3 | — | — | — |
| F4 | ○ | ○ | — |
| F5 | — | — | — |
| F6 | ○ | ○ | — |
| F7 | ○ | ○ | — |
| F8 | ○ | ○ | — |
| F9 | ○ | ○ | — |
| F10 | ○ | ○ | — |
| F11 | ○ | ○ | — |

Table 1 shows all 30 cryptographic protocols were analyzed by the three reasoning methods. According to Table 1, the circled part is the successful analysis of 21 cryptographic protocols. The remaining 9 protocols could not be analyzed. The 9 cryptographic protocols cannot be analyzed because some concepts included in specification of those protocols cannot be formalized.

- *Ns→Ns'* (changed sequence number)
- *Ts →Ts'* (changed time stamp)
- *TVP* (time-variant parameter)
- *MAC* (message authentication code)
- *Dec* (*Nb*) (nonce - 1)

Current Yan and Wang methods do not provide formalization rule about such special data.

The result of case study shows that the method of Wagatuma is not effective. The reason is we tried to analyze cryptographic protocols based on the method of Wagatuma, but it is unclear how to create a new *intruder behavior* during the process of forward reasoning.

In summary, the method of Wagatsuma is ineffective. Method of Yan and Wang are applied to most cryptographic protocols, so they are effective.

## 5. Concluding Remarks

In this paper, we used three formal analysis methods with reasoning to do a case study of 30 cryptographic protocols. In the result of the case study, we use a table to summarize the three reasoning methods' effectiveness. Therefore, we point out which methods are ineffective and which are effective.

In this case study, the analyst needs to manually perform all operations except forward reasoning, which includes the logical translate part and creates some behavior parts according to the type of cryptographic protocol. Therefore, we cannot be sure that the results are all correct.

In future work, we need to continue to expand some functions and predicates of formalization. In addition, a fully automated development environment is needed to improve efficiency and accuracy.

## Reference

[1] Bruce, S.: Applied cryptography: protocols, algorithms, and source code in c, John Wiley and Sons, Inc, 1996.
[2] Cheng, J., Miura, J.: Deontic relevant logic as the logical basis for specifying, verifying, and reasoning about information security and information assurance, In: Proc. ARES 2016, pp. 601-608, 2006.
[3] Cheng, J., Nara, S., Goto, Y.: FreeEnCal: A forward reasoning engine with general-purpose. In: KES 2007. LNCS (LNAI), vol. 4693, pp. 444–452. 2007.
[4] Cortier, V., Kremer, S., Warinschi, B.: A survey of symbolic methods in computational analysis of cryptographic systems. Journal of Automated Reasoning, vol. 46, pp. 225-259, 2011.
[5] Dolev, D., Yao, A. C.: On the security of public key protocols, IEEE Transactions on Information Theory, vol. 29, pp. 198-208, 1983.
[6] Gavin, L.: An attack on the Needham-Schroeder public-key authentication protocol, Information Processing Letters, vol. 56, no.3, pp. 131–133, 1995.
[7] Gavin, L.: A family of attacks upon authentication protocols, Technical Report 1997/5, Department of Mathematics and Computer Science, University of Leicester, 1997.
[8] ISO/IEC.: ISO/IEC 11770 - 3: Information Technology — Security Techniques — Key Management – Part 3: Mechanisms Using Asymmetric Techniques, ISO/IEC, 2015.
[9] ISO/IEC.: ISO/IEC 11770 - 2: IT Security Techniques — Key Management – Part 2: Mechanisms Using Symmetric Techniques, ISO/IEC, 2018.
[10] Meadows, C.: Formal verification of cryptographic protocols: a survey. In: Proc. ICTAC, pp. 135-150, 1994.
[11] Meadows, C.: Formal methods for cryptographic protocol analysis: Emerging issues and trends. IEEE Journal on Selected Areas in Communications, vol. 21, pp. 44-54, 2003.
[12] Roger, M., Michael, D.: Using encryption for authentication in large network of computers, Communication of the ACM, vol. 21, no. 12, pp. 993–999, 1978.
[13] Steven, P., Miller, S.P., Neuman, B.C., Schiller, J.I., Saltzer, J.H.: Kerberos authentication and authorization system, Project Athena Technical Plan, 1987.
[14] Wagatsuma, K., Goto, Y., Cheng, J.: A formal analysis method with reasoning for key exchange protocols, IPSJ Journal, vol. 56, no.3, pp. 903-910, IPSJ, 2015.
[15] Wang, Y., Goto, Y.: An extension of formal analysis method with reasoning for anonymity, In: Proc. ACIIDS, vol. 12034, pp. 53-64, 2020.
[16] Yan, J., Wagatsuma, K., Gao, H., Cheng, J.: A formal analysis method with reasoning for cryptographic protocols. In: Proc. CIS 2016, pp. 566–570. 2016.
[17] Yan, J., Ishibashi, I., Goto, Y., Cheng, J.: A study on fine-grained security properties of cryptographic protocols for formal analysis method with reasoning, In: Proc. SmartWorld Congress 2018, pp. 210-215, 2018.
[18] Yan, J., Wang, Y., Goto, Y., Cheng, J.: An extension of formal analysis method with reasoning: a case study of flaw detection for non-repudiation and fairness. In editors, C2SI 2019, LNCS, vol. 11445, pp. 399–408. 2019.