1 Introduction of Cryptographic Protocols

Abstract Cryptographic protocols are communication protocols which are designed to provide security assurances of various kinds, using cryptographic mechanisms. This chapter gives a brief introduction of cryptographic protocols and the reason why we study these protocols.

A protocol consists of a set of rules (conventions) which determine the exchange of messages between two or more participants. Cryptographic protocols, also called security protocols, use cryptographic primitives in communication protocols to provide information security, such as confidentiality, authentication, integrity or nonrepudiation, in an insecure network. Encryption schemes, digital signatures, hash functions, and random number generations are among the cryptographic primitives which may be utilized to build cryptographic protocols.

Example 1.1 (A cryptographic protocol) Alice is an initiator who wants to establish a secure session between herself and the responder Bob with the aid of a trusted third party Trent, as shown in Fig. 1.1. Alice seeks to establish this connection with Bob by selecting a nonce N_A at random and sending it to Trent, and Trent returns the nonce N_A along with a selected new session key k_{AB} encrypted under the long-term key K_{AS} (shared between Alice and

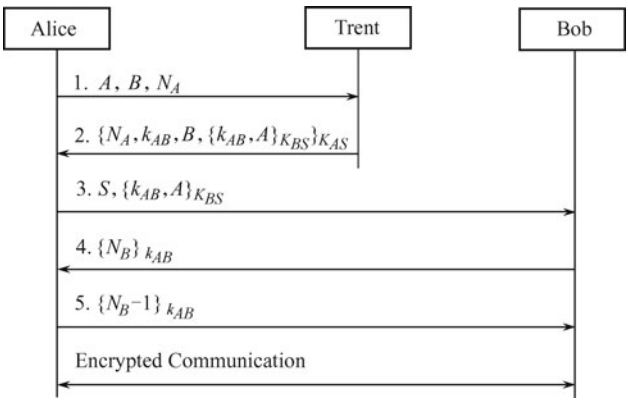

Fig. 1.1 Example of a cryptographic protocol.

L. Dong et al., *Cryptographic Protocol*

Trent) and K_{BS} (shared between Bob and Trent) respectively. A successful run of this protocol does achieve the establishment of the shared key k_{AB} exclusively between Alice and Bob except Trent, then k_{AB} can be used for the subsequent communication between Alice and Bob.

1.1 Information security and cryptography

Over the ages, information was typically stored and transmitted on paper, whereas much of it now resides on magnetic media and is transmitted via computer networks. As we all know, it is much easier to copy and alter information stored and transmitted electronically than that on paper. Information security intends to provide security services for information in digital form. Information security objectives include confidentiality, data integrity, authentication, non-repudiation, access control, availability, fairness and so on. Computer and network security research and development focus on the first four general security services, from which other security services, such as access control, and fairness can be derived[1–5]. Many terms and concepts in this book are from Ref. [1] which is well addressed. For strict or inquisitive readers, please refer to book [1] for detailed information.

— Confidentiality is a service used to keep the content of information from all but those authorized to have it. That is, the information in a computer system or transmitted information cannot be comprehended by unauthorized parties. Secrecy is a term synonymous with confidentiality and privacy.
— Data integrity is a service which addresses the unauthorized modification of data. Modification includes creating, writing, deleting, changing, changing status, and delaying or replaying of transmitted messages.
— Authentication is a service related to identification, including entity authentication and data origin authentication. Entity authentication ensures that the identity of the party entering into a communication is not false. Data origin authentication ensures that the origin of information itself is not false. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed). In many applications, entity authentication is to allow resource usage to be tracked to identified entities.
— Non-repudiation is a service which prevents an entity from denying previous commitments or actions. A procedure involving a trusted third party is needed to resolve the dispute where an entity may deny that certain commitments were made or certain actions were taken. Commonly used fairness security in electronic commerce protocols can be derived from non-repudiation.
— Access control is a service which addresses the authorization of a party to access information resources. Only authorized parties may access the

information resources of the target system. To gain access to an information resource (e.g., computer account, printer, or software application), the user enters a (userid, password) pair, and explicitly or implicitly specifies a resource; here userid is a claim of identity, and password is the evidence supporting the claim. The system checks to see if the password matches corresponding data it holds for that userid, and if the stated identity is authorized to access the resource. Demonstration of knowledge of this secret (by revealing the password itself) is accepted by the system as corroboration of the entity's identity.

— Availability is a service which addresses the availability of the information resources, when they are needed, to authorized parties in a computer system.

— Fairness is a service to keep each honest protocol participant to have sufficient evidence (through acquisition of corroborative evidence) to solve the argumentation between or among parties, which may arise in or after a protocol run. It is the most important security service in a electronic commerce protocol.

Cryptography is to study mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. It is about the prevention and detection of cheating and other malicious activities. Cryptographic skills are the most common technical means of providing information security. Often the objectives of information security cannot solely be achieved through cryptographic primitives and protocols alone, but require procedural techniques and abidance of laws to achieve the desired security result[1].

1.2 Classes of cryptographic protocols

A cryptographic protocol is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective. Cryptographic protocols involving message exchanges require precise definition of both the messages to be exchanged and the actions to be taken by each party. Cryptographic protocols may be typically divided into four main categories, depending on the security objectives of the cryptographic protocol:

1.2.1 Authentication protocol

It is a protocol to provide one party some degree of assurance regarding the identity of another with whom it is purportedly communicating. An identification or an entity authentication technique assures one party (through

acquisition of corroborative evidence) of both: the identity of a second party involved, and that the second party was active at the time the evidence was created or acquired. Authentication protocol typically involves no meaningful messages other than the claim of being a particular entity. Authentication protocol could be broadly subdivided into unilateral entity authentication protocol, and mutual entity authentication protocol. Examples include Woo-Lam protocol[6], Zero knowledge proofs of identify[7] and Okamoto protocol[8].

— Unilateral entity authentication protocol, also called unilateral authentication protocol, is a protocol to assure a corroborated identity of a second party and that this party is active at the protocol run.
— Mutual entity authentication protocol, also called mutual authentication protocol, is a protocol to assure corroborated identities of both protocol parties and that they are active at the protocol run. Mutual authentication may be obtained by running any of the unilateral authentication mechanisms twice.

1.2.2 Key establishment protocol

It is a protocol to establish shared secrets, which are typically called or used to derive session keys. Key establishment is any process whereby a shared secret key becomes available to two or more parties for subsequent cryptographic use. Ideally, a session key is an ephemeral secret, i.e., the one whose use is restricted to a short time period such as a single telecommunications connection (or session), after which all trace of it is eliminated. While privacy of keying material is a requirement in key establishment protocols, source authentication is also typically needed. Encryption and signature primitives may respectively be used to provide these properties. Key establishment protocol can be broadly subdivided into key agreement protocol and key transport protocol.

— Key transport protocol is a key establishment technique with which one party creates or otherwise obtains a secret value, and securely transfers it to the other(s) as a session key.
— Key agreement protocol is a key establishment technique in which a session key is derived by two (or more) parties as a function of information contributed by or associated with each of these, (ideally) so that no party can predetermine the resulting value.
— Authenticated key establishment protocol is a protocol to establish a shared secret with a party whose identity has been (or can be) corroborated. Examples include Needham-Schroeder public-key protocol[9], IKE (Internet Key Exchange) protocol[10], Kerberos authentication protocol[11], X.509 protocol[12], DASS (Distributed Authentication Security Protocol)[13], etc.

1.2.3 Electronic commerce protocol

It is a protocol to provide secure electronic trades over network for two (or more) parties. The focuses of electronic commerce protocols are fairness and non-repudiation. Examples include SET (Secure Electronic Transaction)[14], IKP (Internet Keyed Payments)[15], etc.

1.2.4 Secure multi-party protocol

It is a protocol to assure secure collaborated run of computation for any parties of the protocol run in a distributed system. Examples include group key exchange protocols, multi-party authentication protocols, electronic vote protocols over net, electronic bid protocols, electronic cash protocols etc.

In the literature of cryptographic protocols, authentication protocols are commonly used to refer to both authentication protocols and key establishment protocols, and this is the case in this book.

1.3 Security of cryptographic protocols

An active adversary (perhaps by co-working with his friends distributed over an open communication network) is capable of intercepting, modifying, or injecting messages, and is good at doing so by impersonating other protocol principals. Even in the existence of active adversaries and communication errors, a secure cryptographic protocol should meet all claimed objectives. As for a key establishment protocol, this should include being operational, providing both secrecy and authenticity of the key, and being resilient. A key establishment protocol is operational (or compliant) if, in the absence of active adversaries and communications errors, honest participants who comply with its specification always complete the protocol having computed a common key and having knowledge of the identities of the parties with whom the key is shared. Key authenticity implies that the identities of the parties sharing the key are understood and corroborated, thus addressing impersonation and substitution. A key establishment protocol is resilient if it is impossible for an active adversary to mislead honest participants as to the final outcome[1].

Cryptographic protocols, such as authentication or authenticated key-establishment protocols, are difficult to design and debug. For example, IEEE 802.11 wired equivalent privacy (WEP) protocol[16], which is used to protect link-layer communications from eavesdropping and other attacks, has several serious security flaws. Anomalies and shortcomings have also been discovered in standards and proposed standards for Secure Sockets Layer[17], the later

IEEE 802.11i wireless authentication protocols[18], Kerberos[11], and others.

A successful attack on an authentication or authenticated key establishment protocol usually does not refer to breaking a cryptographic algorithm, e.g., via complexity theory-based cryptanalysis technique. Instead, it usually refers to adversary's unauthorized and undetected acquisition of cryptographic credential or nullification of cryptographic service without breaking a cryptographic algorithm. Of course, this is due to an error in protocol design, not the one in the cryptographic algorithm[3].

Here is a taxonomy of the possible attack types: message replay attack, man-in-the-middle attack, parallel session attack, reflection attack, interleaving attack, attack due to type flaw, attack due to name omission, attack due to misuse of cryptographic services, etc. We cannot exhaust all possible types of attacks even we could list all known attacks or attacks we can imagine, since the ability of an adversary is always developing. Furthermore, viewing from a lower-layer (the network layer) communication protocol, it actually does not require very sophisticated techniques for an adversary to mount various types of attacks. Hence, cryptographic protocols, especially authenticated protocols and key establishment protocols, are readily to contain security flaws, even under the great care of experts in the field.

The main objective of this section is to show the delicate nature of cryptographic protocols, especially authenticated protocols and key establishment protocols.

Example 1.2 (Needham-Schroeder public-key protocol) The Needham-Schroeder public-key protocol[9] provides mutual entity authentication and key transport for both parties, as shown in Fig. 1.2. The transported symmetric keying materials N_A and N_B may serve both as nonces for entity authentication and session key parts for further secure communication use. Combination of the resulting shared key parts allows computation of a joint key to which both parties contribute.

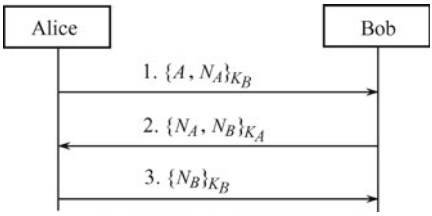

Fig. 1.2 Needham-Schroeder public-key protocol.

Notation

$\{Y\}_{K_X}$ denotes public-key encryption (e.g., RSA) of data Y using party X's public key K_X; $\{Y_1, Y_2\}_{K_X}$ denotes the encryption of the concatenation of Y_1 and Y_2. A stands for Alice, B for Bob, and I for the active adversary Malice. N_A and N_B are secret symmetric keying materials chosen by Alice and Bob, respectively.

Premise

K_A is Alice's public key, K_B is Bob's public key, and Alice and Bob possess each other's authentic public key. If this is not the case, while each party has an authentic certificate carrying its own public key, one additional message is required for certificate transport.

Actions

1) A randomly chooses a nonce N_A and sends B Message 1.

2) B recovers N_A upon receiving Message 1, and randomly chooses a nonce N_B and returns Message 2 to A.

3) Upon decrypting Message 2, A checks if the key material N_A recovered agrees with that sent in Message 1. (Provided N_A has never been previously used, this gives A both entity authentication of B and assurance that B knows this key). A sends B Message 3.

4) Upon decrypting Message 3, B checks if the key N_B recovered agrees with that sent in Message 2. A session key can be computed as $f(N_A, N_B)$ using an appropriate publicly known non-reversible function f.

Thus, a successful run of this protocol does achieve the establishment of the symmetric keying materials N_A and N_B, which are shared secrets exclusively between Alice and Bob. Further notice that since both parties contribute to these shared secrets recently, they are confident about the freshness of N_A and N_B. A and B trust the randomness of the secrets N_A and N_B since they are from a large space, which can be used to initialize a shared secret key $f(N_A, N_B)$ for subsequent secure communication between Alice and Bob.

Unfortunately, the Needham-Schroeder public-key protocol is vulnerable to an attack discovered by Lowe in 1995[19]. In the attack of Low, Malice intercepts the messages sent by (or to) Alice and Bob in Messages 1, 2, and 3, and replaces them with his own version. The following example is the attack.

Example 1.3 (Attack on Needham-Schroeder public-key protocol) The attack (see Fig. 1.3) involves two simultaneous runs of the protocol. In the first

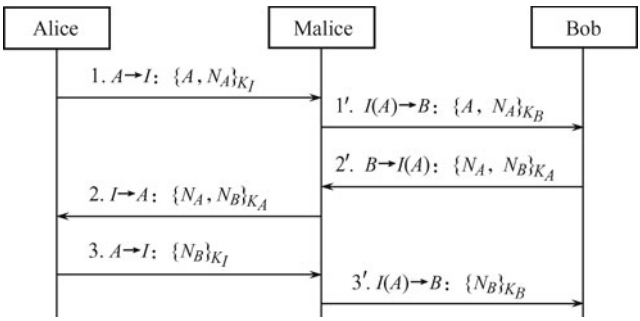

Fig. 1.3 Attack on Needham-Schroeder public-key protocol.

run (steps 1, 2, 3), Alice establishes a valid session with Malice; in the second run (steps $1'$, $2'$, $3'$), Malice establishes a bogus session with Bob by impersonating Alice. At last, Bob believes that Alice (in deed, it is Malice) has correctly established a session with him and they shared exclusively the secret nonces N_A and N_B.

Premise

Suppose that Malice has the public keys of all the protocol participants in his possession.

Actions

1) In step 1, Alice starts to establish a normal session with Malice, sending him a nonce N_A.

2) In step $1'$, via replaying the nonce N_A to Bob, Malice tries to establish a bogus session with Bob by impersonating Alice.

3) In step $2'$, Bob responds to Alice (Malice indeed) by selecting a new nonce N_B and returning it back along with N_A. Malice intercepts this message, but he cannot decrypt it because it is encrypted under Alice's public key.

4) In step 2, Malice therefore seeks to use Alice's private key to do the decryption for him, by forwarding the message to Alice; note that this message is of the form expected by Alice in the first run of the protocol.

5) In step 3, Alice decrypts the message to obtain N_B, and returns N_B to Malice (encryption under Malice's public key), thus completing the first run of the protocol.

6) In step $3'$, Malice decrypts Message 3 to obtain N_B using Malice's private key, and then constructs Message $3'$ and sends it to Bob by impersonating Alice, thus completing the second run of the protocol.

We can imagine the following consequences of this attack. Malice may include the shared nonces which suggest a session key within a subsequent message, and Bob will believe that the encrypted message using this session key originates from Alice.

Example 1.4 (Revised Needham-Schroeder public-key protocol) Figure 1.4 illustrates a revised Needham-Schroeder public-key protocol which is designed to enhance the security by indicating Alice's identity in Message 3. Alice assures Bob that N_A and N_B are exclusively symmetric keying ma-

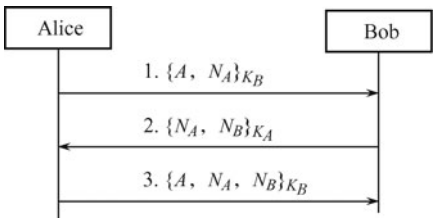

Fig. 1.4 A revise on Needham-Schroeder public-key protocol.

terials between Alice and Bob by explicitly indicating Alice's identity and encrypting Message 3 using Bob's public key.

Actions

1) Upon receiving Message 2, Alice should be assured that she is talking to Bob, since only Bob could be able to decrypt Message 1 to obtain N_A and this must have been done after her action of sending the nonce N_A out (a recent action).

2) Upon receiving Message 3, Bob should be assured that he is talking to Alice, since only Alice could be able to decrypt Message 2 to obtain N_B (a recent action). Bob should also be assured that N_A and N_B are exclusively symmetric keying materials between Alice and Bob since they are transmitted with the explicit identity of Alice, and only Bob could decrypt Message 3.

However, the revised protocol with security enhanced is not secure indeed. It could also be compromised by the attack discovered by Lowe[20].

Example 1.5 (Attack on the revised Needham-Schroeder public-key protocol) The new attack involves two simultaneous runs of the protocol, as shown in Fig. 1.5. In the first run (steps 1, 2, 3), Alice establishes a valid session with Malice; in the second run (steps $1'$, $2'$, $3'$) Malice tries to establish a bogus session with Bob by impersonating Alice. At last, Bob believes that Alice has correctly established a session with himself and they shared exclusively the nonces N_A and N_B. However, N_A and N_B are known by Malice.

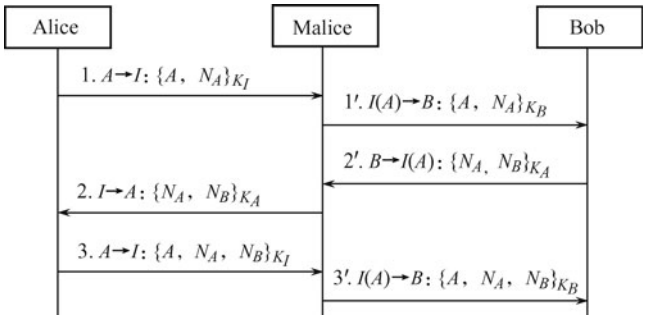

Fig. 1.5 Attack on the revised Needham-Schroeder public-key protocol.

Cryptographic protocols often comprise only a few messages, and protocol construction might seem a simple task. However this is clearly deceptive in practice, and the example we have shown above is an illustration.

1.4 Motivations of this book

Authentication protocols are the most commonly used cryptographic protocols and they are important in real world applications. Many and various

protocols have been proposed to provide authentication and key establishment security[1–18]. Although many of these protocols may seem relatively simple, in comparison with more complex distributed systems, they are subtle to design and very easily compromised, as we have witnessed in the above section.

Furthermore, authentication protocols are not only notoriously error-prone, and the flaws of these protocols are very difficult to detect. The current version of the Internet key exchange (IKE) protocol for Internet security is proved to be not secure as it promised, even after many years' protocol development by the committee of highly experienced computer security experts[21]. Many protocols have shown to be flawed even a long time after they were published. For example, the Needham-Schroeder public-key authentication protocol was found flawed by Lowe in 1995, seventeen years after its publication[9, 19].

The question of whether the security of an authentication protocol or an authenticated key establishment protocol is adequate has been extensively studied, with a large body of approaches proposed, including [20, 22 – 34] etc., and these approaches have played a very important role in protocol security analysis. While this book will introduce a new idea, which is more operational in practice, on how to uncover flaws in cryptographic protocols, the uncovering procedure can be done in a short time, by even a communication engineer without deep cryptographic knowledge background.

In this book, we will discuss the topic of the security of cryptographic protocols, especially that of authentication protocols. Our study of cryptographic protocol security in this book covers a wide range of topics in the subject with in depth discussions. Especially, we will put forward a novel idea, security analysis based on trusted freshness, which will indicate when a cryptographic protocol is secure, why a cryptographic protocol is flawed, and how to achieve the security of a cryptographic protocol. Security analysis based on trusted freshness is a new idea but not only a concrete means or formalism for analyzing the security of a cryptographic protocol. While it is an operational idea which can be easily employed by even a communication engineer without deep cryptographic background, and it can be utilized by information security researchers to invent systematic approaches (i.e., formal methods) for developing correct cryptographic protocols, or to invent formal approaches and automation tools for analyzing the security of existing cryptographic protocols.

This book includes 9 chapters. In Chapter 2, we will introduce some background knowledge of cryptography related to cryptographic protocols, and we will further study the principles to design cryptographic protocols in Chapter 3. Informal security analysis mechanisms, and reasons why taxonomy attacks on authentication protocol exist are in Chapter 4, and case studies of several protocols for real world applications are in Chapter 5. Formal definition of some security properties, formalism approaches of protocol security analysis, and design approaches to the development of correct authentication proto-

cols are in Chapters 6, 7, and 8. Chapter 9 introduces automated verification approaches to authentication protocols.

References

[1] Menezes A, van Oorschot P, Vanstone S (1996) Handbook of Applied Cryptography. CRC Press, New York

[2] Goldreich O (2003) Foundations of Cryptography. Cambridge University Press, New York

[3] Mao W (2004) Modern Cryptography: Theory and Practice. Prentice Hall, New Jersey

[4] Stallings W (2006) Cryptography and Network Security: Principles and Practice, 4th edn. Prentice Hall, New Jersey

[5] Stinson DR (2003) Cryptography: Theory and Practice, 2nd edn. CRC Press, New York

[6] Woo TYC, Lam SS (1992) Authentication for Distributed Systems. Computer 25(1): 39 – 52

[7] Feige U, Fiat A, Shamir A (1987) Zero Knowledge Proofs of Identify. In: STOC'87 Proceedings of the Nineteenth Annual ACM symposium on Theory of computing, New York, 25 – 27 May 1987

[8] Okamoto T (1993) Provably Secure and Practical Identification Schemes and Corresponding Signature Scheme. In: CRYPTO'92 Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara 16 – 20 Aug 1992. Lecture notes in computer science, vol 740, pp 31 – 53, Springer

[9] Needham RM, Schroeder MD (1978) Using Encryption for Authentication in Large Network of Computers. Communication of the ACM 21(12): 993 – 999

[10] Harkins D, Carrel D (1998) The Internet Key Exchange Protocol (IKE), RFC 2409. http://www.ietf.org/rfc/rfc2409.txt. Accessed Dec 2005

[11] Miller SP, Neuman BC, Schiller JI, Saltzer JH (1987) Kerberos Authentication and Authorization System. Paper Presented at the Project Athena Technical Plan Section E.2.1. MIT, Boston

[12] CCITT (1987) CCITT Draft Recommendation X.509. The Directory-Authentication Framework (Version 7), New York

[13] Kaufman C (1993) Distributed Authentication Security Service, RFC 1507. http://www.ietf.org/rfc/rfc1507.txt. Accessed Sept 1993

[14] SET. Secure Electronic Transaction. The SET Standard Specification. http://www.setco.org/set-specifications. Accessed May 1997

[15] IBM Zurich Laboratory (1995) Internet Keyed Payments Protocol (IKP). http://www.zurich.ibm.com /Technology/Security/extern/ecommerce/spec. Accessed 30 June 1995

[16] ANSI/IEEE Std 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Sept 1999

[17] Freier AO, Karlton P, Kocher PC (1996) The SSL Protocol Version 3.0. http://wp.netscape.com/eng/ssl3/draft302.txt. Accessed 18 Nov 1996

[18] IEEE Std 802.11i-2004. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements. July 2004

[19] Lowe G (1995) An Attack on the Needham-Schroeder Public Key Authentication Protocol. Information Processing Letters 56(3): 131 – 133

[20] Lowe G (1996) Breaking and Fixing the Needham-Schroeder Public-key Protocol Using FDR. In: TACAS'96 Proceedings of the 12th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Passau, 27 – 29 Mar 1996. Lecture Notes in Computer Science (Lecture Notes in Software Configuration Management), vol 1055, pp 147 – 166, Springer

[21] Kaufman C (2005) Internet Key Exchange (IKEv2) Protocol, RFC 4306. http://tools.ietf.org/html/rfc4306. Accessed Dec 2005

[22] Canetti R, Krawczy H (2001) Analysis of Key-exchange Protocols and Their Use for Building Secure Channels. In: EUROCRYPT'01 Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, Innsbruck, 6 – 10 May 2001. Lecture Notes in Computer Science, vol 2045, pp 453 – 474, Springer

[23] Burrows M, Abadi M, Needham R (1990) A Logic of Authentication. ACM Transactions on Computer Systems 8(1): 18 – 36

[24] Gong L, Needham R, Yahalom R (1990) Reasoning About Belief in Cryptographic Protocols. In: Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, Oakland, 7 – 9 May 1990

[25] Syverson PF, Oorschot PCV (1994) On Unifying Some Cryptographic Protocol Logics. In: Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy, Oakland, 16 – 18 May 1994

[26] Lowe G (1999) Towards a Completeness Result for Model Checking of Security Protocols. Journal of Computer Security 7(2 – 3): 89 – 146

[27] Goldwasser S, Micali S (1984) Probabilistic Encryption. Journal of Computer and System Sciences 28(2): 270 – 299

[28] Bellare M, Rogaway P (1993) Entity Authentication and Key Distribution. In: CRYPTO'93 Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, 22 – 26 Aug 1993. Lecture Notes in Computer Science, vol 773, pp 232 – 249, Springer

[29] Blanchet B (2006) A Computationally Sound Mechanized Prover for Security Protocols. In: Proceedings of the 2006 IEEE Symposium on Security and Privacy, Berkeley/Oakland, 21 – 24 May 2006

[30] Datta A, Derek A, Mitchell JC, Roy A (2007) Protocol Composition Logic (PCL). Electronic Notes in Theoretical Computer Science 172: 311 – 358

[31] Canetti R, Herzog J (2006) Universally Composable Symbolic Analysis of Mutual Authentication and Key-exchange Protocols. In: Theory of Cryptography Conference Proceedings of TCC2006, New York, 4 – 7 Mar 2006

[32] Qing SH (2003) Design and Logical Analysis of Security Protocols. Journal of Software, 14(7): 1301 – 1309 (in Chinese)

[33] Qing SH (2003) Twenty Years Development of Security Protocols Research. Journal of Software 14(10): 1740 – 1752 (in Chinese)

[34] Feng DG, Fan H (2003) Security Protocol Theory and Method. Science Press, Beijing (in Chinese)