http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (6): 1068-1091, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1068.1091

A Survey on Analysis of Selected Cryptographic Primitives and Security Protocols in Symbolic Model and Computational Model

Bo Meng
School of Computer, South-Center University for Nationalities, MinYuan Road No. 708, HongShan Section, Wuhan, Hubei, China, 430074

Abstract: Security protocols and cryptographic primitive play a very important role in information security world. People have paid a serious attention to the methods to verify security properties in security protocols and cryptographic primitives. From 1980's two distinct approaches: Symbolic approach and computational approach have been proposedd for it. Recently, significant advances have been made in verification on security properties in security protocols and cryptographic primitives and these two approaches. In this study we survey the existing results on the fields including symmetric encryption, public key encryption, digital signature, hush function, secrecy, key cycles, information flow, secrecy, automatic proof, deniable authentication protocol, electronic payment protocol and internet voting protocol in symbolic model and computational model. The survey processes in two lines: One line follows the trace of emergence and developments of verification on security properties in security protocols and cryptographic primitives. The other line is to discuss what methods are usedd and how to verify these security properties during the developments. Finally we give the existing results on verification on security properties in security protocols and cryptographic primitives in symbolic model and computational model.

Key words: Security property, verification, review, protocol security

INTRODUCTION

Security protocols and cryptographic primitive play a very important role in information security world. It can be usedd to achieve many security targets including privacy, authentication and confidentiality, integrity and so on in unsecure environment with passive or active adversary. In the last several decades all kinds of security protocols, for example, authentication protocol, electronic payment protocol, key distribution protocol, electronic voting protocol and deniability encryption protocol are proposedd. But how to prove the security goals of security protocols and cryptographic primitives is a changeling issue. Since 1980's two distinct approaches: Symbolic approach and computational approach are proposedd to verify the security properties of security protocols and cryptographic primitives. Each approach is that: Firstly the abilities of adversary and the participants are assumed and modeled, then the formal definitions of security properties or security goals are presenteded, finally the analyzed security protocols and cryptographic primitives are modeled and is analyzed with the correspondence language and tool according to the formal definitions of security properties.

In symbolic approach, based on the work of Dolev and Yao, messages are terms of algebra and the cryptographic primitives are assumed ideally secure. Hence the results of proof are not clear and unpractical in a way. But owning to that the abstraction is ideal it is more amenable to automated proof methods. For such kinds of semantics a body of work on automatic protocol analysis exists (Cortier *et al*., 2006; Meadows, 2003; Meng, 2009d) for a survey. However, these surveys pay little attention on the status of analysis of deniable authentication protocols, electronic payment protocols and internet voting protocols with/without automatic tool in symbolic approach and computational approach. In computational approach based on complexity and probability the attacker is modeled a probabilistic polynomial-time Turing machine and a protocol is an unbounded number of copies of probabilistic polynomial-time Turing machine. Security is assessed in active or passive attacker. If an adversary can win an attack game with non-negligible probability, then a pre-defined computational assumption is invalid. Hence the results of proof are clear and practical. Yet the proof in computational model is long and highly error prone. So development of automatic verifier in computational model is an emergency mission and is a hard problem. Cortier *et al.* (2010) discussed the existing results in computational model. They give a survey that could act as a quick reference for researchers who want to

contribute to the field, want to make used of existing results, or just want to get a better picture of what results already exist. Yet in their survey on analysis of security protocols including deniable authentication protocols, electronic payment protocols and internet voting protocols in computational approach is not got serious attention.

So in this survey we discus the state-of-art of verification of selected cryptographic primitives and security protocols especially including deniable authentication protocols, electronic payment protocols and internet voting protocols. The main contributions of this study are sunmarized as follows:

- The state-of-art of verification of security protocols including information flow, deniable authentication protocols electronic payment protocols and internet voting protocols in symbolic model and computational model are discussed in detail
- The status in quo of verification of cryptographic primitives including symmetric encryption, public key encryption, digital signature, hush function, secrecy etc in computational model are presenteded
- In symbolic model the verification of security protocols have make a great development in automatic tools. However, the automatic tools which are usedd to verify the cryptographic primitives and security protocols in computational model are at the beginning stage. So development of automatic verifier in computational model is an emergency mission. At the same time the verification on implementation of security protocols and cryptographic primitives with automatic tools should be got a serious attention owning to its great significance in real world

Verification of security protocols and cryptographic primitives: Two important approaches to the verification of security protocols are known under the general names of symbolic and computational, respectively. In the symbolic approach, originating from the study of Dolev and Yao (1983) messages are terms of algebra and the cryptographic primitives are ideally secure; in the computational approach, growing out of the study of Goldwasser and Micali (1984) messages are bitstrings and the cryptographic primitives are secure with overwhelming probability. This means for example, that in the symbolic approach only who knows the secret key can decrypt a ciphertext while in the computational approach the probability to decrypt a ciphertext without knowing the secret key is negligible. Indeed while the symbolic approach is more amenable to automated proof methods, the computation approach can be more realistic. Recently a significant amount of effort has been made in order to link both approaches and profit from the advantages of each of the two worlds. In order to combine the profit from the advantages of each of the two communities is a changeling issue whether the symbolic approach is sound with respect to the computational approach, need to address. The seminal study of Abadi and Rogaway (2002) address the chandelling issue in the context of passive adversaries while the study of Micciancio and Warinschi (2004a) deals with it in the context of active adversaries. Table 1 describes the difference between symbolic model and computational model .In the following first the art of status of symbolic approach is introduced and then the computational approach is discussing in detail.

Table 1: The difference between symbolic model and computational model

	Formal approach	Computational model
Message	terms	bitstrings
Encryption	idealized	algorithem
Adversary	idealized	Anypolynomial algorithm
Secrecy property	Reachability-based property	Indistingability
Guarantees	unclear	Strong
Proof	automatic	By hand and error-prone

Goal: Proving propertities at the bitstring level using existing symbolic models

SYMBOLIC APPROACH

Symbolic approach is based on Dolev-Yao model (Dolev and Yao, 1983) which relies on a formal model: bitstrings are abstracted by formal expressions, the attacker is any formal process and security properties, such as anonymity, can be expressed by the observational equivalence of processes. This model is much simpler: There is no coin tossing, no complexity bounds and the attacker is given only a fixed set of primitive operations. Therefore, it is easy that security proofs become much simpler and can sometimes be mechanized. However, the drawback is that we may be miss some attack becaused the model might be too rough. For such kinds of semantics a body of study on automatic protocol analysis exists (Cortier *et al*., 2006; Meadows, 2003; Meng, 2009d) for a survey. However, these surveys pay little attention on the status of analysis of deniable authentication protocols, electronic payment protocols and internet voting protocols with/without automatic tool in symbolic approach.

The development of symbolic approach has started in 1980s (Dolev and Yao, 1983). This field matured considerably in the 1990s. Some of the methods rely on rigorous but informal framestudys, sometimes supporting sophisticated complexity-theoretic definitions and arguments. Other methods rely on formalisms specially tailored for this task. However, other methods are based on communicating sequential processes (Hoare, 1985); BAN logic (Burrows *et al*., 1989); strand space (Fabrega *et al*., 1998), spi calculus (Abadi and Gordon,

1997), murϕ (Mitchell *et al*., 1997; Kessler and Neumann, 1998), applied pi calculus (Abadi and Fournet, 2001).

Symbolic model has been successfully applied to find problems in the design of security protocols. Moreover, verification methods based on the symbolic model have become efficient and robust enough to be deployed for the analysis of even large security protocols (He *et al*., 2005; Backes *et al*., 2006; Butler *et al*., 2006; Kailar, 1996; Meng *et al*., 2005; Jonker and De Vink, 2006; Delaune *et al*., 2006; Meng, 2007a, 2008, 2009a, 2011a; Meng *et al*., 2010a). Owning to the abstraction ideally of cryptography, symbolic methods are often quite effective; a fairly abstract view of cryptography often suffices in the design, implementation and analysis of security protocols. Symbolic methods enable relatively simple reasoning and also benefit from substantial study on proof methods and from extensive tools support, for example, SMV, NRL, Casper, Isabelle, Athena, Revere and SPIN (Maggi and Sisto, 2002), Brutus, ProVerif (Blanchet, 2001), Scyther (Joseph and Cremers, 2006) Coq. Some of the automatic tools have been usedd to analyze commercial protocols (Blanchet, 2008; Abadi *et al*., 2007; Backes *et al*., 2008; Bhargavan *et al*., 2008; Gerling *et al*., 2008; Meng *et al*., 2010a; Meng, 2011a).

Deniable authentication protocol: Deniable authentication protocols allow a Sender to authenticate a message for a receiver, in a way that the receiver can not convince a third party that such authentication ever took place. Deniable authentication has two characteristics that differ from traditional authentication: One is that only the intended receiver can authenticate the true source of a given message; the other is that the receiver can not provide the evidences to prove the source of the message to a third party. A practical secure deniable authentication protocol should have the following properties: Completeness or authentication, strong deniability; Weak deniability, security of forgery attack, security of impersonates attack, security of compromising session secret attack, security of man-in-the-middle attack.

In symbolic approach, Meng (2009b) proposed a framestudy of strong and weak deniability based on Kessler and Neumann logic. After that, the framestudy is applied to analyze the deniability of two typical deniable authentication protocols: Fan *et al*. (2002) propsed interactive deniable authentication protocol and Mengs non-interactive deniable authentication protocol (Meng, 2009c). In the next section we review the formal definition of strong deniability and weak deniability.

Formal definition of strong deniability: If a deniable authentication protocol satisfies the following conditions at the same time, we agree that the deniable authentication protocol has non-strong-deniability, otherwise has strong deniability.

Condition one:

$$\{\text{Prove believes canprove } \{\text{Authority said Sender}\} \text{ to J until t}\}$$

The condition one shows that prover has Senders legal identification,Sender_ID, that is issued by the legal authority, not by other illegal party.

Condition two:

$$\{\text{Prove believes canprove } \{\text{Sender said Message}\} \text{ to J until t}\}$$

The condition two shows that the prover certainly Sender sends a message to receiver.

Condition three:

$$\left\{\text{prover believes prover canprove}\left\{\begin{matrix}\text{sender said Relatioship between}\\ \text{Sender\_ID and Message}\end{matrix}\right\}\text{to J until t}\right\}$$

The condition three shows that the Sender who has the Sender_ID , not other Sender with Sender_ID, sends a special message, or the Sender who has the Sender_ID sends other message.

Proving rule P7:

$$\left\{\begin{matrix}\left[\text{prover believes prover canprove } \{\text{Authority said Sender\_ID}\} \text{ to J until t}\right]\\ \wedge\left[\text{prover believes prover canprove } \{\text{sender said Message}\} \text{ to J until t}\right]\wedge\\ \left[\begin{matrix}\text{prover believes prover canprove}\\ \{\text{sender said Relatioship between Sender\_ID and Message}\}\text{to J until t}\end{matrix}\right]\end{matrix}\right\}$$

The P7 rule shows that if the prover assure the Senders identification Sender_ID and can get a message and can prove the message is generated by the Sender who has the legal identification Sender_ID, he can prove Sender said or can generate the evidence of non-strong-deniability which means that the deniable authentication protocol has the non-strong-deniability, otherwise has strong deniability.

Formal definition of weak deniability: If a deniable authentication protocol satisfies the following conditions at the same time, we agree that the deniable authentication protocol has not weak deniability, otherwise has weak deniability.

Condition one:

$$\{\text{receiver believes receiver canprove } \{\text{Authority said Sender\_ID}\} \text{ to J until t}\}$$

The condition one shows that receiver has Senders legal identification, Sender_ID, that is issued by the legal authority, not by other illegal party.

Condition two:

{receiver believes receiver canprove {Sender said Message} to J until t}

The condition two shows that the prover certainly the Sender sends a special message.

Condition three:

$$\left\{\text{reveiver believes reveiver canprove}\left\{\begin{matrix}\text{sender said Relatioship between}\\ \text{Sender\_ID and Message}\end{matrix}\right\}\text{to J until t}\right\}$$

The condition three shows that the Sender who has Sender_ID, not other Sender with Sender_ID, sends a special message, or the Sender who has the Sender_ID sends other message.

Proving rule P8:

$$\left\{\begin{matrix}\left[\text{reveiver believes reveiver canprove }\{\text{Authority said Sender\_ID}\}\text{ to J until t}\right]\\ \wedge\left[\text{reveiver believes reveiver canprove }\{\text{sender said Message}\}\text{ to J until t}\right]\wedge\\ \left[\begin{matrix}\text{reveiver believes reveiver canprove}\\ \{\text{sender said Relatioship between sender\_ID and Message}\}\text{to J until t}\end{matrix}\right]\end{matrix}\right\}$$
$$\rightarrow \text{reveiver believes reveiver canprove}$$
$$\{\text{sender said Evidence of non-weak-deniability}\}\text{ to J until t}$$

The P8 rule shows that if the receiver assure the Senders identification Sender_ID and can get a special message and can prove the special message is generated by the Sender who has the legal identification Sender_ID, he can generate the evidence of non-weak-deniability which means that the deniable authentication protocol has non-weak-deniability, otherwise has weak deniability.

Electronic payment protocol: The practical secure electronic payment protocol should have the following properties: Accountability, atomicity, anonymity, non-repudiation and fairness. These secure properties play important roles in implementation of secure transactions over the public Internet. A lot of electronic payment protocols for example, SOCPT (Meng and Xiong, 2004) Virtual Credited Card, SET, Ikp, VCPT, CyberCoin, DigiCash, eCoin, MilliCent, NetCash, NetBill, FSTC, CAFÉ, Agora, Mondex, MiniPay, NetCents, PayWord, LMCCPP and NetPay are proposedd.

In symbolic approach, Kailar (1996) is probably the first who proposed a modal logic to reason about accountability in electronic payment protocol. Kailars definition of accountability is concerned with the ability to prove the association of an originator with some action to a third party without revealing any private information to the third party. The party who can prove such a statement is called a prover whereas the third party who is convinced of the proof is called a verifier. Kailar employs the modal operator CanProve to formalize the concept of accountability i.e., Prover CanProve ϕ to Verifier where Prover and Verifier stand for prover and verifier, respectively and ϕ stands for a general statement about some action. However, Kailars logic is not suitable for analyze the real-world e-commerce protocols becaused of the following two reasons: Firstly, Kailars logic can analyze the signed plain message only. Messages in real-world ecommerce protocols are not just signed plain messages but they often are multiply encrypted and/or hashed messages which are signed Secondly, Kailars logic does not reason about verifiers at all. Van Herreweghen (2001) points out that reasoning about verifiers is essential for analyzing real-world e-commerce protocols. It should be noted also that Kailars definition for accountability is general in that the actions that are associated with an originator can be of any kinds.

Following Kailar (1996) and Kessler and Neumann (1998) employ a modal logic to reason about the accountability. However, Kessler and Neumann (1998) provide an alternative definition of the modal operator CanProve by means of sending messages. Its goal to show the accountability is to show Prover believes Prover CanProve ϕ to Verifier. One way to show that Prover believes Prover CanProve ϕ to Verifier holds is for Prover to believe that Prover can convince Verifier to believe ϕ by sending some messages that Prover has to Verifier. Thus, this logic offers reasoning about both provers beliefs and verifiers beliefs and in particular, provers beliefs about verifiers beliefs.

Based on Kessler and Neumann (1998) logic, Kungpisdan and Permpoontanalarp (2001) provide a modal logic which is an extension and a simplification of Kessler and Neumanns logic. It employs the concept of provable authorization in the presented of private information. In order to solve disputes, a prover wants to send only the necessary information to prove some statements to a judge who acts as a verifier without revealing the unnecessary private information. With this concept, prover can prove the statement without revealing private information to verifier. They extend Kessler and Neumanns (1998) logic in two main aspects. Firstly, they provide axioms for the accountability of multiply encrypted and/or hashed messages which are signed in order to resolve disputes. Secondly, proposed axioms fordealing with the used accountability to specify

and analyze the goals of electronic commerce protocols. With it they analyze SET and iKP protocol. They argue that the analysis of two kinds of accountability shows that SET lacks of both kinds of accountability beacused of its message format that combines price and OD with in the same hash Hash (price, OD). When proving money accountability, prover is required to send both price and OD which are the inputs of hash, to verifier in order to prove price. Prover is also required to reveal price to verifier in order to prove goods accountability. Proving money accountability in iKP is successful beacused price and OD are separated with applying hash function. Verifier cannot infer OD beacused it is hashed. However, iKP has problem when proving goods accountability. In order to prove OD, prover is required to reveal price to verifier.

Van Herreweghen (2001) proposed informal description of authorization and gives an analysis of SET and iKP. The analysis shows that the Customer in a SET transaction has no secure receipt of payment. A comparison shows the equivalent version of iKP to provide more complete evidence than SET. The analysis is not formal since it is done without using any formal logic. However, the analysis is presenteded partly in rule-based styles.

Meadows and Syverson (1998) presented a formal specification of requirements for the payment portion of the SET protocol by introducing transaction vectors, projections thereon and the vector agreement. Their specification is expressed by NRL language. But they do not analyze SET protocol with NRL. Bella *et al.* (2006) used Isabelle to analyze the complete Purchase protocols of SET and find that owning to the lack of explicitness in the dual signature makes some agreement properties fail: It is impossible to prove that the Cardholder meant to send his credit card details to the very payment gateway that receives them. Lu *et al.* (2009) used SMV to analyze the authentication, confidentiality and integrity of a variant of SET. They also talked about its lacks, for example how to deal with transaction records and give their suggestions. Shaikh and Devane (2010) used AVISPA to analyze the authentication, confidentiality and secrecy of the SET protocol. It is shown that these securities hold within the established security of PKI. Panti *et al.* (2003) proposed a methodology for verifying security requirements of electronic payment protocols by means of model checking. They extended correspondence property to not only used for authentication but also confidentiality and integrity. At the same time they analyze a variant of SET with NuSMV and discover two attacks that allow a dishonest usedr to purchase a good debiting the amount to another usedr. Meng and Zhang (2005) also introduced generally formal definition of accountability in electronic transaction based on Kessler and Neumann (1998) logic and the SET protocol is analyzed with its framestudy. It results show that it has the properties of money accountability and goods accountability. They also think that the analysis of SET by Kungpisdan and Permpoontanalarp (2001) is worth discussing.

Table 2: The requirements of money accountability

	Requirements	Owner
Auth (C-M)	(C, M, Amount, ref) $\sigma(K_C^-(C, M, Amount, ref))$	M
Auth (M-C)	(M, C, Amount, ref), $\sigma(K_M^-(M, C, Amount, ref))$	C
Auth (C-A)	(C, A, Amount, ref) $\sigma(K_C^-(C, A, Amount, ref))$	A
Auth (A-C)	(A, C, Amount, ref) $\sigma(K_A^-(A, C, Amount, ref))$	C
Auth (M-A)	(M, A, Amount, ref) $\sigma(K_M^-(M, A, Amount, ref))$	A
Auth (A-M)	(A, M, Amount, ref) $\sigma(K_A^-(A, M, Amount, ref))$	M

Table 3: The requirements of goods accountability

	Requirements	Owner
(1)	(C, M, OD, ref'), $\sigma(K_c^-(C, M, OD, ref))$	M
(2)	(M, C, OD, ref'), $\sigma(K_M^-(M, C, OD, ref))$	C

Meng *et al.* (2005) used Kessler and Neumann (1998) logic to prove the soundness of the requirements and analyze SOCPT protocol with the framestudy. The requirements of money accountability are listed in Table 2 and 4.The requirements of goods accountability are listed in Table 3 and 5. They argue that after an execution of the electronic payment protocol, if the results reach to the requirements of money accountability, the electronic payment protocol has the property of money accountability. If the results reach to the requirements of goods accountability, the electronic payment protocol has the property of goods accountability. C stands for Customer. M stands for Merchant. A stands for Acquirer. OD stands for Order Description. $\sigma K_c(C, M, Amount, ref)$ means the results of the digital signature of (C, M, Amount, ref) under the private key K_c by customer. Their results show that SOCPT protocol has money accountability and goods accountability.

Internet voting protocol: The practical secure internet voting protocol should have basic properties including privacy, completeness, soundness, unreusability, fairness eligibility and invariableness and expanded properties including universal verifiability, receipt-freeness and coercion-resistance. Internet voting protocol play a key role in internet voting system. Especially receipt-freeness and coercion-resistance are the key properties in internet voting protocol.

We survey the symbolic proof on receipt-freeness and coercion-resistance. The survey processes in two different lines. The first line follows the trace of emergence and developments of formal proof on security properties. The second line is to analyze what formal methods are usedd during symbolic proof.

Table 4: Kessler and Neumann logic notations description of money accountability

Definition	Kessler and Neumann'logic notation description	Owner
Ayth (C-M)	M believes M canprove {C said (C, M, Amount, ref)}to J until t	M
Ayth (M-C)	C believes C canprove {M said (C, M, Amount, ref)}to J until t	C
Ayth (C-A)	A believes A canprove {C said (C, A, Amount, ref)}to J until t	A
Ayth (A-C)	C believes C canprove {A said (C, A, Amount, ref)}to J until t	C
Ayth (M-A)	A believes A canprove {M said (M, A, Amount, ref)}to J until	A
Ayth (A-M)	M believes M canprove {P said (M, A, Amount, ref)}to J until t	M

Table 5: Kessler and Neumaun'logic notations description of goods accountability

Definition	Kessler and Neumann'logic notation description	Owner
(1)	M believes M canprove {C said (M, C, OD, ref)}to J until t	M
(2)	C believes C canprove {M said (C, M, OD, ref)}to J until t	C

Delaune *et al.* (2006) have done a path breaking study on proposing the formal definition of receipt-freeness and coercion-resistance based on applied pi calculus. Their formal model is based on Dolev-Yao abstraction. They formalize receipt-freeness as an observational equivalence. The idea is that if the attacker can not find if arbitrary honest voters V_A and V_B exchange their votes, then in general he can not know anything about how V_A (or V_B) voted. This definition is robust even in situations where the result of the election is such that the votes of V_A and V_B are necessarily revealed. They also assume that the voter cooperates with the coercer by sharing secrets but the coercer cannot interact with the voter to give her some prepared messages. At the same time they used adaptive simulation to formalize coercion-resistance. The ideas of this definition is that whenever the coercer requests a given vote on the left-hand side then V_B can change his vote according to the right-hand side and counterbalance the outcome. However, we need to avoid the case where $V' = V_A\{c/v\}^{c_1,c_2}$ letting vote V_B vote α. Therefore, we require that when we apply a context C, intuitively the coercer, requesting $V_A\{c/v\}^{c_1,c_2}$ to vote c, V' in the same context votes α. There may be circumstances where V' may need not to cast a vote that is not. In the case of coercion-resistance, the coercer is assumed to communicate with Alice during the protocol and can prepare messages which she should send during the election process. Their formal definition of coercion-resistance base on the informal definition: A voter can not cooperate with a coercer to prove to him that she voted in a certain way. The voting protocol (Lee *et al.*, 2003) is analyzed with their formal model. Meng (2008) also applies their formal model to analyze the protocol (Meng, 2007b). Kremer and Ryan (2005) applies the applied pi calculus to analyze the voting protocol (Fujioka *et al.*, 1992). They formalize three properties, fairness, eligibility and privacy.

Yet Jonker and De Vink (2006) point out that the formal model (Delaune *et al.*, 2006) offers little help to identify receipts when receipts are presented. Hence they presented a new formal method which useds the process algebra, to analyze receipts based on their informal definition: A receipt r is an object that proves that a voter v cast a vote for candidate c. This means that a receipt r has the following properties: (R1) r can only have been generated by v. (R2) r proves that v chose candidate c. (R3) r proves that v cast her vote. Jonker and De Vink provide a generic and uniform formalism that captures a receipt. Symbolic model of Jonker and De Vink (2006) is also simpler than symbolic model of Delaune *et al.* (2006) They used the formalism to analyze several voting protocols. Meng (2007b) analyzes receipt-freeness of the protocols (Fujioka *et al.*, 1992; Cramer *et al.*, 1997; Acquisti, 2004) based on formalism (Jonker and De Vink, 2006).

About definition of receipt proposed by Jonker and De Vink (2006), Meng (2009d) argues that it is worth discussing. Firstly about (R1) r can only have been generated by v, in some voting protocol one part of receipt is generated by the authority, not generated by voter. Secondly, they give the following auxiliary receipt decomposition functions: "α: Rcpt $\rightarrow$AT" which extracts the authentication term from a receipt. Authentication term should be the identification of voter. Thirdly the author does not prove the generic and uniform formalism that is right in their study. Finally they used a special notion, it difficult to used and generalize it. Hence Meng gives a formal logic framestudy for receipt-freeness based on V. Kessler and H. Neumann logic (Kessler and Neumann, 1998) and apply it to analyze the voting protocol (Fujioka *et al.*, 1992).

Knowledge based logics have been also used in the studies of Jonker and Pieters (2006), Baskar *et al.* (2007) and Van Eijck and Orzan (2007) to formally analyze the security properties of e-voting protocol. Jonker and Pieters (2006) formalize the concept of receipt-freeness from the perspective of a anonymity approach in epistemic logic which offers among others, the possibility to write properties allowing to reason about the knowledge of an agent a of the system with respect to a

proposition p. They classify receipt-freeness into two types: Weak receipt-freeness and strong receipt-freeness. Weak receipt-freeness implies that the voter can not prove to the vote buyer that she sent message m during the protocol, where m is the part of a message representeding the vote. Here, no matter what information the voter supplies to the vote buyer, any vote in the anonymity set is still possible. In other words, for all possible votes, the vote buyer still suspects that the voter cast this particular vote; or: The vote buyer is not certain she did not cast this vote. Baskar *et al.* (2007) give the formal definition of secrecy, receipt-freeness, fairness, individual verifiability based on knowledge based logic and analyze receipt-freeness of the voting protocol (Fujioka *et al*., 1992). Van Eijck and Orzan (2007) used dynamic epistemic Logic to model security protocols and properties, in particular anonymity properties. They apply it to the voting scheme (Fujioka *et al*., 1992) and find the three phases should be strictly separated, otherwise anonymity is compromised. Talbi *et al.* (2008) used ADM logic to specify fairness, eligibility, individual verifiability and universal verifiability and analyze the voting protocol (Fujioka *et al*., 1992). Their goal is to verify these properties against a trace-based model.

Groth (2004) evaluated the voting scheme based on homomorphic threshold encryption with univeral composability framestudy. He formalizes the privacy, robustness, fairness and accuracy.

Backes *et al.* (2008) model formalized key properties including the soundness, receipt-freeness and coercion-resistance in remote internet voting protocol with applied pi calculus. It mainly models the soundness, receipt-freeness and coercion resistance. In Backes *et al.* (2008) model, the voter are classified into three types of voter: Honest voter, corrupted voter and ad-hoc voter. Honest voter are issued an identity by an issuer authority and behave according to the protocol specification. Corrupted voter will register and then simply output all their registration credentials on a public channel, thus the coercer and vote buyer can impersonate him in order to mount any sort of attack. Ad-hoc voters can behave arbitrarily; they do not necessarily follow the protocol but are also not necessarily corrupted. Backes *et al.* (2008) model formalized soundness with the events including, beginvote (id, v), endvote (v), startid (id) and startcorid (id). The events in the soundness property are also usedd later in the modeled processes. Beginvote (id, v) starts the voting phase for a voter with id and the intention to vote for v whereas endvote (v) is the tallying of this vote. startid (id) and indicate the start of the registration phase for an eligible voter or an corrupted voter with id. The receipt-freeness models that the voter V′ does not only vote v′ as a regular voter but additionally used V^{fake} to generate fake secrets, casts an extra vote using them and provides a receipt of this invalid voting and deal with that an additional voter k that votes with fake registration secrets in case the voter 'i' complies with the request of the coercer and simply abstains if 'i' cheats the vote buyer by casting a vote with fake secrets.In order to formalize coercion-resistance, the process called Extractor is introduced. Extractor plays an important role in formalization of coercion-resistance which extracts the vote the coercer casts on behalf of Extractor and tallies it directly. Extractor depends on the construction of the particular electronic voting protocol and has to be provided by the usedr. Meng *et al.* (2010a) used Backes *et al.* (2008) model to analyze Meng *et al.* (2010b) protocol with automatic tool ProVerif , a resolution-based mechanized theorem prover for security protocols. The result is that it has coercion resistance. But it has not soundness becaused ProVerif found an attack on soundness. Then the improvement of Meng *et al.* (2010b) protocol is proposedd and also modeled in applied pi calculus and automatically analyzed in ProVerif. The result is that the improvement of protocol has soundness. At the same time Meng (2011a) used Backes *et al.* (2008) model to analyze Acquisti (2004) protocol in applied PI calculus with ProVerif. The result is that Acquisti (2004) protocol has the soundness and coercion-resistance in some conditions. Meng *et al.* (2010c) used Backes *et al.* (2008) model to analyze Meng (2009e) protocol with automatic tool ProVerif . They found that Meng (2009e) protocol has coercion resistance. But it has not soundness becaused ProVerif found an attack on soundness. Then the improvement of Meng (2009e) protocol is proposedd and also modeled in applied pi calculus and automatically analyzed in ProVerif. The improvement of Meng (2009e) protocol has soundness. To our best knowledge, the first automated analysis of Meng (2009e) protocol, Meng *et al.* (2010b) protocol and Acquisti (2004) protocol for an unbounded number of honest and corrupted voters is finished.

COMPUTATIONAL MODEL

In order to prove the security of cryptographic primitives and security protocols, there are two different approaches usedd. The most famous approach, among the cryptographic world, is the proved security in the reductionist sense (Bellare, 1997). Adversaries are

modeled as a probabilistic polynomial-time Turing machine and a protocol is an unbounded number of copies of probabilistic polynomial-time Turing machine which try to win a game, specific to the cryptographic primitive/protocol and to the security notion to be satisfied. The computational security is achieved by rules: If an adversary can win such an attack game with non-negligible probability, then a well-defined computational assumption is invalid. As a consequence, the actual security relies on the sole validity of the computational assumption. For signature schemes, the adversary tries to forge a new valid message-signature pair while it is able to ask for the signature of any message of its choice (Goldwasser *et al*., 1988). Similarly, for encryption, the adversary chooses two messages and one of them is encrypted. Then the goal of the adversary is to guess which one has been encrypted (Goldwasser and Micali, 1984) with a probability significantly better than one half. Again, several oracles may be available to the adversary according to the kind of attack. One can see in these security notions that computation time and probabilities are of major importance: An unlimited adversary can always break them with probability one; or in a shorter period of time, an adversary can guess the secret values, by chance and thus win the attack game with possibly negligible but non-zero probability. Security proofs in this framestudy consist in showing that if such an adversary can win with significant probabilit, within reasonable time, then a well-defined problem can be broken with significant probability and within reasonable time too. Such an intractable problem and the reduction will quantify the security of the cryptographic protocol. The adversary can be categorized into two types: Passive adversary and active adversary. Passive adversary can eavesdrops on communication between honest parties. Active adversary is assumed to control the netstudy and can schedule the communications and send fake messages. Note that in both models it is assumed that the adversary has complete control of the netstudy: he can intercept, send and block messages. In symbolic models, the adversary can build new messages using a predefined symbolic inference rules. For example, he can recover the plaintext from ciphertext only if he has the proper decryption key. In computational models a potential adversary can perform arbitrary computations while tampering with the protocol, provided it takes a polynomial time. In particular, this assumption captures the possibility that the adversary may try to guess secrets. An additional distance between the symbolic and the computational models is in how security properties are specified. For example, secrecy is usually stated in symbolic models as a reachability property while in computational models, it is formalized as the indistinguishability of adversary views. Cortier *et al*. (2010) discussed the existing results in computational model. They give a complete survey that could act as a quick reference for researchers who want to contribute to the field, want to make used of existing results, or just want to get a better picture of what results already exist. Yet in their survey on analysis of security protocols including deniable authentication protocols, electronic payment protocols and internet voting protocols in computational approach is not got serious attention.

Computational soundness: In their path breaking study, Abadi and Rogaway (2000) gave the links between the world of symbolic method and computational model. They finish the changeling issue that under which conditions messages that are equivalent in symbolic model are also equivalent in computational model with an example of symmetric encryption in a passive adversary that eavesdrops on communication. Their study shows that it is possible to employ the formal tools and methods devoted to the symbolic approach to directly obtain computational security guarantees. The crucial implication is that such guarantees can be obtained without making used of the typical computational proofs. For example, security properties are defined as indistinguishability in computational model: The protocol is secure if, for any adversary, the probability that adversary gets an advantage is negligible. A typical example is the anonymity property, by which an attacker should not be able to distinguish between two netstudys in one of which identities have been switched. The difficulty in such computational security notions lies in the problem of obtaining detailed proofs: They are in general unmanageable and it is hard to be verified by automatic tools.

Following the seminal study of Abadi and Rogaway (2000), Micciancio and Warinschi (2002, 2004b) analyze the completeness of the Abadi-Rogaway logic of encrypted expressions and considered various extensions of the basic logic that allow to model realistic encryption functions that do not hide the length of the message being transmitted and complex protocols of distributed programs communicating over a synchronous netstudy. They get the result that the Abadi-Rogaway logic of indistinguishability for cryptographic expressions is not complete and giving a example of a secure encryption function and a pair of expressions, such that the distributions associated to the two expressions are computationally indistinguishable but equality cannot be proved within the logic. They also introduce a definition of confusion freeness and prove that the Abadi-Rogaway

logic is sound and complete whenever the encryption scheme that is usedd is confusion free. In addition, they consider a refinement of the logic that overcomes certain limitations of the original proposal, allowing for encryption functions that do not hide the length of the message being sent.

Horvitz and Gligor (2003) introduce the two different conditions under which indistinguishability in the computational setting implies equivalence in the formal. One is weak key-authenticity tests for expressions which are a necessary condition and the other is confusion-freeness which is a sufficient condition on the computational encryption scheme. They introduce the new completeness rule of weak key-authenticity tests for expressions that is strictly weaker than the rule confusion-freeness with symmetric encryption.

Laud and Corin (2004) gave an extension of the study of Abadi and Rogaway which mainly constituted by considering the used of composed, non-atomic keys in the encryption operator of the formal language. They provide a computational interpretation for expressions that allow it establish the computational soundness of formal encryption with composed keys.

Herzog (2003, 2005) and Herzog *et al*. (2003) proposed a soundness theorem that shows that if the public key encryption is plaintext-aware then the computational adversary cannot construct the interpretation of any formal message that the formal adversary cannot construct.

Baudet *et al*. (2005, 2009) proposed a general framestudy for comparing formal and computational models in the presence of a passive attacker. In contrast to other studys, they do not consider a fixed set of primitives but aim at results for arbitrary equational theories. They define the notions of soundness and faithfulness of a cryptographic implementation with respect to equality, static equivalence and (non-) deducibility. Soundness holds when a formal notion of security has a computational interpretation. Applying the framestudy they get the soundness results for static equivalence with the exclusive OR and the soundness of symmetric encryption and lists. The result is similar in spirit to the one of Abadi and Rogaway (2000). However, but the difference is that the deterministic, length-preserving, symmetric encryption schemes-also known as pseudo-random permutations or ciphers are considered while Abadi and Rogaway (2000) consider probabilistic, symmetric encryption.

Key cycles: Key cycles play an important role in the context of computational soundness. An encryption cycle is a sequence of keys where each key is encrypted under the next one and the last key is encrypted under the first one. Becaused in symbolic models where such cycles do not caused any insecurity questions with key-cycle but in the computational model where standard security definitions do not guarantee security with key-cycles.

Laud (2002) introduced a definition of the strengthened attacker for the symbolic model to address the key-cycles. His result show that no matter whether these expressions contain key-cycles or not, if two formal expressions look the same to this attacker, then the distributions of bit-strings corresponding to these two expressions look the same for the adversaries in the computational model. At the same time, he proves that if two formal expressions do not contain key-cycles, then they look the same to the strengthened attacker, if and only if the look the same to the normal attacker. Laud's solution provides soundness in the presence of key-cycles but does so by strengthening attacker for the symbolic model in other words, weakening the notion of formal equivalence. It is assumed that key-cycles somehow always break the encryption and the formal adversary is strengthened so as to be always able to know inside the encryptions of a key-cycle. Adao *et al*. (2005) think that the price of Laud (2002) paid is too high. They get the soundness in the presence of key-cycles not by weakening encryption in the formal model but by strengthening it in the computational one. They get the soundness in the presence of key-cycles by using the notion of key-dependent message security for public key cryptosystem. Cortier and Zalinescu (2006) proved that for detecting the generation of key cycles during the execution of a protocol in the presence of an intruder for a bounded number of sessions, it is a NP-complete decision procedure. Comon-Lundh *et al*. (2010) used the constraint system approach to provide an NP-complete decision procedure for detecting the generation of key cycles during the execution of a protocol, in the presence of an intruder, for a bounded number of sessions.

Datta *et al*. (2005, 2006) have designed a computationally sound logic that enables them to prove computational security properties using a logical deduction system which is based on a variant of computational version of Protocol Composition Logic. The framestudy can be usedd to prove security properties of key exchange protocols in the computational model.

Corin and Hartog (2006) used a probabilistic Hoare-style logic for formalizing game-based cryptographic proofs and give elaborately in full detail a proof of security of El Gamal by reducing the semantic security of the cryptosystem to the hardness of solving the Decisional Diffie-Hellman problem.

Garcia and van Rossum (2008) extend the well-known Abadi-Rogaway logic with probabilistic hashes and give a precise semantic interpretation to it using Canetti's oracle hashes. These are probabilistic polynomial-time hashes that hide all partial information. They also show that under appropriate conditions that the encryption algorithm is type-0 secure or IND-CPA on the encryption scheme, this interpretation is computationally sound and complete. It can be usedd to port security results from the formal world to the computational world when considering passive adversaries. At the same time they point that while considering active adversaries, they have shown that the security definition for oracle hashing is not strong enough.

Bresson *et al.* (2007) used their generalization of DDH to extend the celebrated computational soundness result of Abadi and Rogaway (2000) with exponentiation and Diffie-Hellman-like keys. They show that how to extend the notion of Decisional Diffie-Hellman assumption into (P, Q) -DDH assumption in order to capture the information that is leaked through exponentiation which are essentially linear dependencies between the various exponents.

Kremer and Mazare (2010) introduced a symbolic model to analyze protocols that used a bilinear pairing between two cyclic groups. This model consists in an extension of the Abadi-Rogaway logic and the logic is still computationally sound: Symbolic indistinguishability implies computational indistinguishability. With the symmetric encryption scheme has to satisfy indistinguishability against chosen-plaintext attacks and the bilinear mapping has to satisfy the bilinear decisional Diffie-Hellman assumption.

Information flow: Laud (2001, 2003) firstly proposed a programming language to analyze the secure information flow in the presence of a probabilistic polynomial time adversary without key-cycles. The programming language contains assignment, loops, conditional, sequential composition and application of some operators. Laud (2003) designed an automatic analysis for protocols using shared-key encryption, with passive adversaries. Laud (2004) extends it to active adversaries but with only one session of the protocol. Laud (2005) designs a type system for proving security protocols in the computational model. This type system handles shared- and public-key encryption, with an unbounded number of sessions. This system relies on the Backes-Ptzmann-Waidner library. Laud and Vene (2005) presented a novel type system for checking the security of information flow in programs containing operations of symmetric encryption. The type system studys directly in the computational model and is correct with respect to the complexity-theoretic security definitions of the encryption primitive. Askarov *et al.* (2006) proposed an abstract model for cryptographically masked flows. This model considers an imperative programming language with key generation, encryption and decryption as distinguished operations. In the concrete semantics, corresponding to the real-world implementations of the language, the encryption operation is probabilistic. He also gives a type system for checking whether a program satisfies the non-interference property in the cryptographically masked flows. Based on the study of Askarov *et al.* (2006), Laud (2008) gets a reasonable set of conditions and then proposeds a simpler abstract model that is nevertheless no more restrictive than the cryptographically masked flows together with these conditions for soundness.

Secrecy: Secrecy in the computational model is usually defined as a confidentiality property while in the formal model it may also be a confidentiality property but more commonly is an integrity property. The adversary may learn partial information about the secret messages in the computational model. Cortier and Warinschi (2005) established that symbolic integrity and secrecy proofs are sound with respect to the computational model. Janvier *et al.* (2005a, b) applied the idea to introduce a security criterion that allows it to combine asymmetric and symmetric key cryptography as well as signature and hashing. Then they give a proof of correctness of the Dolev-Yao model for protocols that may combine asymmetric and symmetric encryption schemes, signature schemes as well as hash functions. Laud (2004) presented a technique for static analysis, correct with respect to complexity-theoretic definitions of security, of cryptographic protocols for checking whether these protocols satisfy confidentiality properties. The protocol is transformed in an automated way in the view of the adversary does not change distinguishably. The transformation is based on the security definitions of the cryptographic primitives which demand the indistinguishability of certain two oracles-parts of the protocol that behave as the real oracle may be replaced by the ideal oracle. If one can transform out all syntactic accesses to the secret payloads then the payloads are secure.

In active adversaries: Reconciliation approaches taking into account also active adversaries have mostly considered asymmetric primitives and/or integrity properties. Guttman *et al.* (2001) are one of the first to consider authentication in the presence of active adversaries in two models. Their approach was different

from the later ones in that the security definitions in the computational model were not complexity-theoretical but information theoretical, so the obtained security guarantee was stronger than usual. The cost for this added strength was the length of the shared secrets. They also pioneered the technique of translating a protocol run in the computational model, after it had finished, to a run in the formal model and showing that if that run would not have been possible in the formal model then something which should happen only with a negligible probability must have happened in the run in the computational model. The approach was developed further by Micciancio and Warinschi (2004a) the idea is to show that any concrete trace is the image of a symbolic trace. They related the formal and computational traces for protocols using symmetric encryption. They considered logics that allow to model realistic encryption functions that do not hide the length of the message being transmitted and complex protocols of distributed programs communicating over a synchronous netstudy. All these logics are both sound and complete when the encryption scheme usedd to implement the protocols satisfies the appropriate notion of security of indistinguishability and confusion-freeness. In other words, the patterns associated to two programs by these logics are equivalent if and only if no probabilistic polynomial time adversary can distinguish the messages transmitted by one or the other protocol with non-negligible advantage. Cortier and Warinschi (2005) showed that there exist automatic analyses for the formal model that carry directly over to the computational model. They provided that soundness of secrecy and signatures implemented using an existentially unforgeable scheme under chosen message attacks. Janvier *et al.* (2005a) extend Micciancio and Panjwani (2005) and proposed a computational soundness theorem for the symbolic analysis of cryptographic protocols which extends an analogous theorem of Abadi and Rogaway to a scenario where the adversary gets to see the encryption of a sequence of adaptively chosen symbolic expressions. They point that if the encryption scheme is IND-CCA and the signature scheme is UNF-CCA, an adversary behavior follows the formal model with overwhelming probability. At the same time they also proposed a theorem that allows proving equivalences between security criterion and some of its sub-criteria.

Canetti (2001) introduced universal composability based on probabilistic polynomial-time interacting Turing machines. The universal composability relation involves a real protocol and ideal functionality to be compared, a real and ideal adversary and an environment. The real protocol realizes the ideal functionality if, for every attack by a real adversary on the real protocol, there exists an attack by an ideal adversary on the ideal functionality, such that the observable behavior of the real protocol under attack is the same as the observable behavior of the ideal functionality under attack. Each set of observations is performed by the same environment. In other words, the system consisting of the environment, the real adversary and the real protocol must be indistinguishable from the system consisting of the environment, the ideal adversary and the ideal functionality. The scheduling of a system of processes is sequential in that only one process is active at a time, completing its computation before another is activated. The default process to be activated, if none is designated by process communication, is the environment. Canetti and Herzog (2004) had defined the abstract functionality for certified public key encryption which allows them to relate the integrity properties satisfied by protocols with bounded number of runs using only asymmetric encryption in formal and computational models. Canetti and Herzog (2006) showed how a Dolev-Yao-style symbolic analysis can be usedd to prove security properties of protocols (including authentication) within the framestudy of universal composability (Canetti, 2001) for a restricted class of protocols using public-key encryption as only cryptographic primitive. They also used the framestudy of time bounded task-PIOAs (Probabilistic Input/Output Automata) for proving cryptographic protocols in the computational model (Canetti *et al.*, 2006). This framestudy allows them to combine probabilistic and non-deterministic behaviors.

Lincoln *et al.* (1998) had given a computational semantics for a variant of polynomial-time processes calculus where probabilistic choice replaces non-determinism everywhere. They have usedd a form of process equivalence, where an environment directly interacts with the real and ideal protocol. The idea is that security is defined by requiring that a real system that supposedly implements some cryptographic system is as secure as an ideal version of the protocol/primitive. The computational model in this study is a probabilistic polynomial-time processes calculus that allows concurrent execution of independent processes. The process equivalence relation usedd in particular to prove authentication properties gives rise to a relation between protocols and ideal functionalities by allowing a simulator to interact with the ideal functionality, resulting in a relation called strong simulatability. They have also devised a formal proof system for this calculus but it does not seem to be amenable for automatic deduction. Mateus *et al.* (2003) proposed a probabilistic polynomial-time process calculus for analyzing cryptographic protocols and used it to derive compositionality properties of protocols in the presence of computationally

bounded adversaries. His approach is based on the intuition that security properties of a protocol P may be expressed by means of existence of an idealized protocol Q such that for any adversary M, the interactions between M and P have the same ob servable that for any adversary M, the interactions between M and P have the same observable behavior as the interactions between M and Q. Ramanathan *et al.* (2004) used a probabilistic polynomial-time process calculus designed for specifying security properties as observational equivalences to develop a form of bisimulation that justifies an equational proof system. This proof system is sufficiently powerful to derive the semantic securityof ElGamal encryption from the Decision Diffie-Hellman assumption and vice versa. Mitchell *et al.* (2005) presented the process calculus which is a variant of CCS, with bounded replication and probabilistic polynomial-time expressions allowed in messages. The process calculus can be usedd to expressing probabilistic polynomial-time protocol steps, a specification method based on a compositional form of equivalence and a logical basis for reasoning about equivalence. They prove that evaluation of any process expression halts in probabilistic polynomial time and define a form of asymptotic protocol equivalence that allows security properties to be expressed using observational equivalence, a standard relation from programming language theory that involves quantifying over all possible environments that might interact with the protocol. They also develop a form of probabilistic bisimulation and used it to establish the soundness of an equational proof system based on observational equivalences. Kusters *et al.* (2008) gave a detailed review and analysis and comparison of the different existed framestudy.

Based on the new indistinguishability-based security definition for commitment schemes in the presence of adaptive adversaries, apply novel generic construction for a non-malleable commitment scheme based on one-way trapdoor permutations which is secure with respect to our new definition and has some additional properties such as being non-interactive, perfectly binding and reusable which makes it of independent interest, Galindo *et al.* (2008) gave a sound interpretation of symbolic commitments in the Dolev-Yao model while considering active adversaries.

Automatic proof: Barthe *et al.* (2004) provided a machine-checked account of the Generic Model and the Random Oracle Model the proof assistant Coq. The Generic Model and the Random Oracle Model provide non-standard computational models in which one may reason about the probability and computational cost of breaking a cryptographic scheme.

Laud (2004) gave symmetric encryption in automatic analyses for confidentiality against active adversaries and presenteds a technique for static analysis, correct with respect to complexity-theoretic definitions of security, of cryptographic protocols for checking whether these protocols satisfy confidentiality properties.

Backes and Pfitzmann (2004) and Backes *et al.* (2003a, b) had designed an abstract cryptographic library including symmetric and public-key encryption, message authentication codes, signatures and nonce and shown its soundness with respect to computational primitives, under arbitrary active adversary. This framestudy shares some limitations with the computational soundness results, for instance the exclusion of key cycles and the fact that symmetric encryption has to be authenticated. It relates the computational model to a non-standard version of the Dolev-Yao model, in which the length of messages is still presented. Backes and Pfitzmann (2005) related the computational and formal notions of secrecy in the framestudy of this library. Sprenger *et al.* (2006) used this framestudy for a computationally-sound machine-checked proof of the Needham-Schroeder-Lowe protocol. Laud (2005) presented a type system for checking secrecy of messages handled by protocols based on the Backes-Pfitzmann-Waidner library for cryptographic operations. The type system is similar to the Abadi-Blanchet type system for asymmetric communication and can be usedd to show that the protocol preserves the secrecy of input messages. They develop a language which is similar to the spi-calculus but has a completely deterministic semantics for expressing protocols, handling symmetric encryption and unbounded number of sessions. Backes and Laud (2006) develop an automatic tool based on Backes-Pfitzmann-Waidner library. The tool can reason about a comprehensive language for expressing protocols, in particular handling symmetric encryption and asymmetric encryption and it produces proofs for an unbounded number of sessions in the presence of an active adversary. The tool have enjoys cryptographic soundness in the strong sense of blackbox reactive simulatability/UC which entails that secrecy properties proven by our tool are automatically guaranteed to hold for secure cryptographic implementations of the analyzed protocol, with respect to the more fine-grained cryptographic secrecy definitions and adversary models.

Blanchet (2008) proposed a probabilistic polynomial calculus based on computational model. In this calculus, messages are bitstrings and cryptographic primitives are functions operating on bitstrings. Blanchet calculus is adapted from the pi calculus and its semantics is purely probabilistic (no non-determinism). All processes run in polynomial time: polynomial number of copies of

processes and length of messages on channels bounded by polynomials. Blanchet calculus has been carefully designed to make the automated proof security protocols. Blanchet calculus consists of terms and processes.

CryptoVerif (Blanchet, 2008) is a mechanized prover which supported Blanchet calculus in computational model. CryptoVerif does not rely on soundness results for symbolic model but directly automate the proofs made in cryptography, based on sequences of games. It can directly prove security properties of cryptographic protocols in the computational model in which the cryptographic primitives are functions on bit-strings and the adversary is a polynomial-time Turing machine. It can proves secrecy properties and that events can be executed only with negligible probability, also it can handles various cryptographic primitives, for example, MACs, stream and block ciphers, public-key encryption, signatures, hash functions. CryptoVerif studys for N sessions with an active adversary. It can also give a bound on the probability of an attack (exact security). CryptoVerif runs either automatically or interactively, in which case it receives guidance from the usedr for selecting transformations. In a recent case study, CryptoVerif is usedd to verify: FDH signature scheme (Blanchet and Pointcheval, 2006), PKINIT for Kerberos (Jaggard *et al.* 2007) Verification Protocol Implementations in ML (Bhargavan *et al.*, 2007) a model of the Basic and Public-Key Kerberos protocol (Blanchet *et al.*, 2008) Verification Protocol Implementations for TLS (Bhargavan *et al.*, 2008), Diffie-hellman protocol (Blanchet, 2009), deniable authentication protocol (Meng, 2011b, Meng and Shao, 2010; Meng *et al.*, 2011c), electronic payment protocols (Meng, 2011c; Meng *et al.*, 2011a, b).

Deniable authentication protocols: Deniable authentication protocols allow a Sender to authenticate a message for a receiver, in a way that the receiver can not convince a third party that such authentication (or any authentication) ever took place. Deniable authentication has two characteristics that differ from traditional authentication: One is that only the intended receiver can authenticate the true source of a given message; the other is that the receiver can not provide the evidences to prove the source of the message to a third party. A practical secure deniable authentication protocol should have the following properties: Completeness or authentication, strong deniability, weak deniability, security of forgery attack, security of impersonate attack, security of compromising session secret attack, security of man-in-the-middle attack.

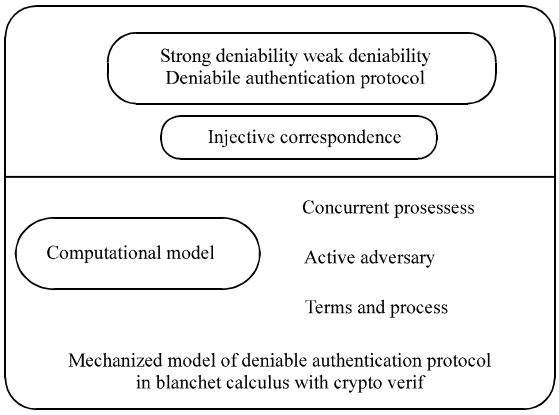

Fig. 1: Analysis model of deniable authentication protocols with Blanchet calculus

In computational model, Meng and Shao (2010) used term, process and correspondence assertion in Blanchet calculus to model the security properties included strong deniability and weak deniability and deniable authentication protocol and proposed the first mechanized framestudy of deniable authentication protocols in computational model with active adversary. The strong deniability and weak deniability are expressed by non-injective or injective correspondence. The mechanized framestudy can be usedd to automatic analyze the security properties including strong deniability and weak deniability of interactive deniable authentication protocols and non-interactive deniable authentication protocols with CryptoVerif. Fig. 1 describes the analysis model of deniable authentication protocols with Blanchet calculus.

Meng and Shao (2010) described automatic model of strong deniability and weak deniability. Meng and Shao automatic model used Blanchet calculus to model the strong deniability and weak deniability.

Generally deniable authentication protocol includes three roles, Sender which is initiator, receiver which is responder and third party, representeded by Sender, Receiver and Thirdparty, respectively. We assume that Sender plays only on the role of the initiator, Receiver plays only the role of responder, Thirdparty play only on the prover. The deniable authentication protocol consists of a sequence of messages exchanged between the Sender and the Receiver and the Receiver and Thirdparty and Sender and Receiver. In deniable authentication protocol Sender can authenticate a message for Receiver, in a way that the can not Receiver convince a Thirdparty that such authentication (or any authentication) ever took place. Deniable authentication protocol has two characteristics that differ from traditional authentication protocol. One is that only the intended Receiver can

authenticate the true source of a given message. The other is that the Sender can not provide the evidences to prove the source of the message to a third party at some condition and the Receiver can provide the evidences to prove the source of the message to a third party. The ability of adversary is defined in the previous section. It can control the channel channelSR between Sender and Receiver. It can not control the channels: ChannelST and channelRT. At the same time the adversary is a probabilistic polynomial-time attacker.

Definition DAP: A secure deniable authentication protocol with session functions sessionid and sessionid′ process DAP for any probabilistic polynomial-time adversary:

$$DAP = Initprosess;(!^{isender\le n}\,SenderProcess\,|!^{ireceiver\le n}\,ReceiverProcess\,|!^{ithirdpartry\le n}\,ThirdpartyProcess)$$

Such that:

- If the adversary just send Receiver to Senderprocess as the first message and relays faithfully between process Senderprocess and process Reciverprocess, then process Reciverprocess finishes with Sender and process Senderprocess finishes with Receiver
- With overwhelming probability, there exists an injective function that maps each index I of a process Senderprocess that finished with Receiver to the index i of a process Receiverprocess with intended principle Sender such that sessioner sessioner′

$$sessioner'(x_1[i],x_2[i],\cdots,x_1[i]) = sessioner'(z_1[i'],z_2[i'],\cdots,z_1[i'])$$

- With overwhelming probability, there exists an injective function that maps each index I of a process Receiver Process that finished with Sender to the index i of a process Sender process that finished with sessioner such that

$$sessioner'(x_1[i],x_2[i],\cdots,x_1[i]) = sessioner'(z_1[i'],z_2[i'],\cdots,z_1[i'])$$

- If the adversary just send Thirdparty to Receiverprocess as the first message and relays faithfully between Thirdparty and Receiverprocess, then Thirdpartyprocess finishes with Receiver and Receiverprocess finishes withThirdparty.
- With overwhelming probability, there exists an injective function that maps each index Thirdparty process of a process that finishes with Receiver to the index i of a process ReceiverProcess finishes with Thirdparty such that

$$sessioner'(p_1[i]) = sessioner'(q_1[i])$$

In the above definition of DAP the injective correspondence can be instead by non-injective correspondence.

The condition one describes the communications between Sender and Receiver without adversary. It deal with Receiver authenticate Sender. The condition two and three describe that Sender has a distinct session with Receiver and Receiver has the same session with Sender with overwhelming probability.

The condition four describes the communications between Receiver and Thirdparty without adversary. It deal with Thirdparty authenticate Receiver. The condition five describes that Receiver has a distinct session with intended principle Thirdparty and Thirdparty has the same session with Receiver with overwhelming probability.

Definition of strong deniability: The purpose of strong deniability is to protect the privacy of Sender. After execution of the deniable authentication protocol the Sender can deny to have ever authenticated anything to Receiver. If the prover (Receiver or the any other party) wants to prove that the Sender have authenticated messages to Receiver, they must provide all the relevant evidence. The Sender can provide his secret information to the Thirdparty. A adversary model in strong deniability: When discussing the strong deniability, in addition the adversary has the ability in previous section, we always also suppose that the Sender and the Receiver cooperate with the judge or the prover or the any other party which means that the Sender and the Receiver provide all the transcripts of the message in the deniable authentication protocol to them.

If DAP satisfies the condition one and four in:

$$\text{inj-event}(\text{whole}_{Sender}(Receiver,x)) \Rightarrow \text{inj-event}(\text{whole}_{Receiver}(Sender,x))$$

$$\text{inj-event}(\text{whole}_{Thirdparty}(Receiver,x)) \Rightarrow \text{inj-event}(\text{whole}_{Thirdparty}(Sender,x))$$

definition DAP and DAP′ satisfies the correspondence and with public variables V = ϕ, then DAP is a secure deniable authentication protocol with session functions (sessionid and sessionid′) in a adversary model in strong deniability. In the above definition of DAP the injective correspondence can be instead by non-injective correspondence.

Definition of weak deniability: The purpose of weak deniability is to protect the privacy of Sender. After

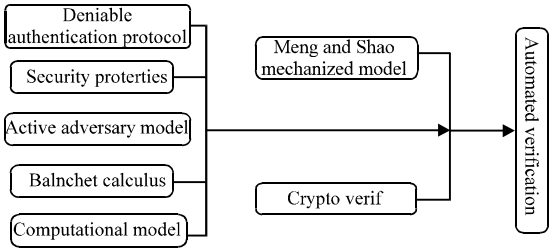

Fig. 2: Model of automatic verification of deniable authentication protocols

execution of the deniable authentication protocol the Receiver can prove to have spoken to Sender but not the content of what the Sender authenticated in a way that the Receiver can not convince a third party that such authentication. If the Receiver want to prove that the Sender have authenticated messages to Receiver, he must provide the evidence related to the thing. An adversary model in weak deniability: When discussing the weak deniability, in addition the adversary has the ability in previous section; we always suppose that only the Receiver generates the evidence that the Sender have authenticated messages to Receiver. Receiver can not get the secret information of the Sender, for example the private key of Sender. Receiver can provide his secret information to the Thirdparty.

If DAP′ satisfies the condition one in definition DAP and DAP′ satisfies the correspondence:

$$\text{inj-event}\left(\text{whole}_{\text{Sender}}\left(\text{Receiver}, x\right)\right) \Rightarrow \text{inj-event}\left(\text{whole}_{\text{Receiverr}}\left(\text{Sender}, x\right)\right)$$

$$\text{inj-event}\left(\text{whole}_{\text{Thirdparty}}\left(\text{Receiver}, x\right)\right) \Rightarrow \text{inj-event}\left(\text{whole}_{\text{Thirdparty}}\left(\text{Sender}, x\right)\right)$$

and with public variables V = ϕ, then DAP is a secure deniable authentication protocol with session functions (sessionid and sessionid′) in a adversary model in weak deniability. In the above definition of DAP the injective correspondence can be instead by non-injective correspondence.

Meng (2011b) and Meng *et al.* (2011c) used Meng and Shao automatic model to automatically prove two typical deniable authentication protocols, Fan *et al.* (2002) interactive deniable authentication protocol and Meng non-interactive deniable authentication protocol, are analyzed in the computational model and the proposedd framestudy with mechamized tool Crypto Verif. Fan *et al.* (2002) deniable authentication protocol which is based on the Deffie-Hellman key agreement protocol, has weak deniability and resist person-in-the-middle attack usedd the digital certificate issued by the Certification Authority. The result of analysis show that (Fan *et al.*, 2002) interactive deniable authentication protocol has weak deniability but not strong deniability which is consist to the claim in itsstudy. Meng (2009c) protocol (is a secure non-interactive deniable authentication protocol based on discrete logarithm problem. It claims that it is secure and has properties including completeness, strong deniability, weak deniability, security of forgery attack, security of impersonate attack, security of compromising session secret attack and security of man-in-the-middle attack. The result of analysis shows that Meng non-interactive deniable authentication protocol has weak and strong deniability which is consist to the claim in its study. To our knowledge, they are conducting the first automatic analysis in computational model of Fan *et al.* (2002) interactive deniable authentication protocol and Meng non-interactive deniable authentication protocol in active adversary. Figure 2 describes the model of automatic verification of deniable authentication protocols.

Electronic payment protocol: The practical secure electronic payment protocol should have the following properties: accountability, atomicity, anonymity, non-repudiation and fairness. These secure properties play important roles in implementation of secure transactions over the public Internet. Electronic commerce protocol useds the cryptographic technologies to confirm the security of parties in the electronic commerce. A lot of electronic payment protocols ,for example, SOCPT (Meng and Xiong, 2004), Virtual Credited Card, SET, Ikp, VCPT, CyberCoin, DigiCash, eCoin, MilliCent, NetCash, NetBill, FSTC, CAFÉ, Agora, Mondex, MiniPay, NetCents, Payword, LMCCPP, Netpay are proposedd.

In computational model, Backes and Durmuth (2005) presented the first cryptographically sound Dolev-Yao-style security proof of iKP protocol by hand. The payment protocol is a slightly simplified variant of the 3KP payment protocol and comprises a variety of different security requirements ranging from basic ones like the impossibility of unauthorized payments to more sophisticated properties like disputability. They show that the payment protocol is secure against arbitrary active attacks, including arbitrary concurrent protocol runs and arbitrary manipulation of bitstrings within polynomial time if the protocol is implemented using provably secure cryptographic primitives. Although they achieve security under cryptographic definitions, their proof does not have to deal with probabilistic aspects of cryptography and is hence within the scope of current proof tools. The reason is that they only exploit a Dolev-Yao-style cryptographic library with a provably secure cryptographic implementation.

Meng *et al.* (2011a) used the term, process and correspondence assertion in Blanchet calculus to model

money accountability and goods accountability and electronic payment protocol, after that they proposed the first mechanized framestudy of electronic payment protocols in computational model with active adversary. The money accountability and goods accountability are expressed by non-injective or injective correspondence. This mechanized framestudy can be usedd to automatically analyze money accountability and goods accountability of electronic payment protocols with Crypto Verif. An automic model of money and goods accountability by Meng *et al.* (2011a) is reviewed as follows:

A probabilistic polynomial-time attacker has full control of the communications channels channelCA between the customer and acquirer, channelCM between the customer and the merchant and channelMA between the merchant and the acquirer: It can listen to all the transmitted information, decide what messages will reach their destination and when change these messages at will or inject its own generated messages. The formalism representeds this ability of the attacker by letting the adversary be the one in charge of passing messages from one party to another. The attacker also controls the scheduling of all protocol events including the initiation of protocols and message delivery. The electronic payment protocols are in a context in which the honest participants are willing to run sessions with the adversary. That is mean the adversary is an active attacker in the channel channelCA, channelCM and channelMA.

Generally electronic payment protocol includes three roles, customer, merchant and acquirer, representeded by customer, Merchant and Acquirer, respectively. The electronic payment protocol consists of a sequence of messages exchanged between Customer and Merchant, Merchant and acquirer, customer and acquirer. In secure electronic payment protocol customer can authenticate a payment message for customer in some way; customer can authenticate an receipt of payment message for acquirer in some way; acquirer can authenticate an message which means he requested to deduct money from his account for acquirer in some way; acquirer can authenticate an receipt which means that he is requested to deduct money from customer's account for customer in some way; Merchant can authenticate a payment message to him for acquirer in some way; acquirer can authenticate a message which means that acquirer transferred money to Merchant's account for Merchant in some way.

In electronic payment protocol EPP, Meng *et al.* (2011a) automatic model assumes that the first messages is sent by Merchant to Customer, then the information related to payment is sent to Merchant and Acquirer. After that the payment response information is sent to Customer and Merchant by Acquirer. It also assumes that EPP consists of odd number of rounds i Merchant between and Customer, rounds m between Merchant and Acquirer, rounds n between Acquirer and Merchant. It also assumes that the first message of rounds i is from Merchant to Customer, the first message of rounds n is from Customer to Acquirer and the first message of rounds n is from Customer to Acquirer. So that the 1-th message of EPP is from Merchant to Customer.The m-th message is from Merchant to Acquirer. The n-th message is from Customer to Acquirer.

In the following we review the definition of money accountability and goods accountability in Meng *et al.* (2011a) automatic model.

Definition of money accountability: Generally in electronic payment protocols one type is that the customer first pays the money then the merchant sends the goods to customer. The other is that the merchant first sends the goods to customer and then the customer pays the money. Meng *et al.* (2011a) automatic model is based on the first category.

If EPP′ is a SEPP and EPP′ satisfies that: $\text{endevent}_{PI}(\text{Marchent-Customer})$, $\text{endevent}_{PI}(\text{Acquirerr-Customer})$ and $\text{endevent}_{PI}(\text{Acquirerr-Marchent})$ are true; at the same time EPP' also satisfies that the following correspondence:

$$\text{endevent}_{PI}(\text{Merchant-Customer-}) \Rightarrow \text{benginevent}_{PI}(\text{Customer-Merchant})$$

$$\text{endevent}_{PI}(\text{Acquirer-Customer}) \Rightarrow \text{benginevent}_{PI}(\text{Customer-Acquirer})$$

$$\text{endevent}_{PI}(\text{Acquirer-Merchant}) \Rightarrow \text{benginevent}_{PI}(\text{Merchant-Acquirer})$$

With public variables V = ϕ, then EPP is SEPP with session functions (sessionid and sessionid′) with money accountability.

Definition of goods accountability: In order used the correspondence to model the goods accountability, electronic payment protocols is classified into two categories: One is that the customer agrees on order description, then the merchant agrees on it; the other is that merchant agrees on order description, then the customer the order description. Meng *et al.* (2011a) automatic model is based on the first category.

If EPP' is a SEPP and EPP′ satisfies that endevent_{PI} (Marchent-Customer) is true, at the same time $\text{endevent}_{OD}(\text{Marchent-Customer}) \Rightarrow \text{enginevent}_{OD}$ (Customer) satisfies the correspondence:

$$\text{endevent}_{OD}(\text{Merchant-Customer}) \Rightarrow \text{enginevent}_{OD}(\text{Customer-Merchant})$$

with public variables V = ϕ, then EPP is a SEPP with session functions (sessionid and sessionid′) with goods accountability.

Meng (2011c) and Meng *et al.* (2011b) apply the previous model based on Blanchet calculus in computational model with active adversary for automatically analysis of 3KP and SOCPT electronic payment protocol. iKP is also credit-card based ecommerce payment protocol. 3KP protocol is one of the families of iKP electronic payment protocols and consists of customer who will make the payment, merchant who will receive the money and acquirer which will withdraw the money from the account of customer to account of merchant. The protocol step of iKP is similar to that of SET. iKP is a family of protocol in that it consists of three types of protocol which depends on the number of certificate of the engaging party. The technologies applied by 3KP protocol mainly include symmetric encryption, asymmetric encryption, hash function and digital signature. It useds symmetric techniques and asymmetric techniques to guarantee data confidentiality and used digital signature to implement message integrity, consistency and accountability. SOCPT is based on analysis of most existing online payment protocols. It is of security, accountability, atomicity, partial anonymity, non-repudiation and fairness. The technologies applied by SOCPT mainly include symmetric techniques, asymmetric techniques, hash function and digital signature and so on. Symmetric techniques and asymmetric techniques is usedd to guarantee data confidentiality and used digital signature to implement message integrity, consistency and non-repudiation, used dual signature to separate order information and personal finical information. The analysis itself is performed by automatic tool CryptoVerif developed by Blanchet. The result shows that 3KP and SOCPT electronic payment protocol has money accountability and goods accountability which are consistent with its claim. To our knowledge, he has conducted the first automatic analysis in computational model of 3KP and SOCPT electronic payment protocol in active adversary.

CONCLUSION

Security protocols and cryptographic primitives play a very important role in information security world. People have paid a serious attention on the methods to verification of its security properties. From 1980's two distinct approaches: Symbolic approach and computational approach are proposedd. Each approach is that: firstly the abilities of adversary and the participants are assumed and modeled, then the formal definitions of security properties is presenteded, finally the analyzed security protocol and cryptographic primitives are modeled and analyzed with the correspondent language and tool according to the formal definitions of security properties. In symbolic approach, based on the study of Dolev and Yao, messages are terms of algebra and the cryptographic primitives are ideally secure. Hence the results of proof are not clear and unpractical in a way. But owning to the abstraction in high level it is more amenable to automated proof methods. In computational approach the attacker is modeled a probabilistic polynomial-time Turing machine and a protocol is an unbounded number of copies of probabilistic polynomial-time Turing machine. Hence the results of proof are clear and practical. Recently, great advances have been made in verification on security properties in security protocols and cryptographic primitives and these two approaches.

In this study we survey the existing results on the fields including symmetric encryption, public key encryption, digital signature, hush function, secrecy, key cycles, information flow, secrecy, automatic proof, deniable authentication protocol, electronic payment protocol, internet voting protocol in symbolic model and computational model. The survey processes in two lines: one line follows the trace of emergence and developments of verification on security properties in security protocols and cryptographic primitives£®The other line is to discuss what methods are usedd and how to verify these security properties during the developments. Table 6-12 give the analysis results of

Table 6: Part one of the analysis results of security protocols and cryptographic primitives in computational model. "✓" means the item is right

	Abadi and Rogaway (2002)	Micciancio and Warinschi (2002, 2004b)	Laud and Corin (2004)	Horvitz and Gligor (2003)	Herzog (2003, 2005) Herzog *et al.* (2003)	Datta *et al.* (2005, 2006)
Symmetric encryption	✓	✓	✓	✓		
Public key encryption					✓	
plaintext-aware					✓	
KDM security						
Composed keys		✓				
Confusion-freeness			✓			
Weak key-authenticity						
With key-cycles	✓					
Passive adversary	✓	✓	✓	✓	✓	
Active adversary						✓

Table 7: Part two of the analysis results of security protocols and cryptographic primitives in computational model. "✓" means the item is right

	Corin and Hartog (2006)	Laud (2001)	Laud (2003)	Laud (2004)	Laud (2005)	Laud and Vene (2005)	Askarov *et al.* (2006)
Symmetric encryption			✓	✓			
Public key encryption	✓						
Information folw		✓				✓	✓
Digitial signature							
Security protocol			✓		✓		
Passive adversary		✓					
Active adversary				✓			

Table 8: Part three of the analysis results of security protocols and cryptographic primitives in computational model. "✓" means the item is right.

	Laud (2008)	Cortier and Warinschi (2005)	Janvier *et al.* (2005a, 2005b)	Laud (2004)	Garcia and van Rossum (2008)	Bresson *et al.* (2007)	Baudet *et al.* (2005, 2009)
Symmetric encryption			✓		✓		
Public key encryption			✓				
Hush function			✓				
Information folw	✓						
Digitial signature			✓				
Integrity and secrecy		✓					
Security protocol				✓			
(P, Q) -DDH assumption						✓	
General framework					✓		✓
Passive adversary					✓		✓

Table 9: Part four of the analysis results of security protocols and cryptographic primitives in computational model. "✓" means the item is right

	Backes and Pfitzmann (2004)	Backes and Pfitzmann (2005)	Sprenger *et al.* (2006)	Laud (2005)	Backes and Laud (2006)	Guttman *et al.* (2001)	Cortier and Warinschi (2005)	Backes *et al.* (2003a,b)
Digitial signature								
Integrity and secrecy								
Security protocol			✓	✓				
Automatic tool					✓			
Authentication								
Secrecy						✓		
An abstract cryptographic library	✓	✓					✓	✓
Active adversary	✓	✓	✓	✓	✓	✓	✓	✓

Table 10: Part five of the analysis results of security protocols and cryptographic primitives in computational model. "✓" means the item is right

	Micciancio and Warinschi (2004a)	Janvier *et al.* (2005a)	Laud (2004)	Canetti (2001)	Canetti and Herzog (2006)	Lincoln *et al.* (1998)
Symmetric encryption			✓			
Public key encryption						
Security protocol		✓			✓	
Universal composability		✓		✓		✓
Polynomial-time processes calculus						✓
Authentication	✓					
Active adversary	✓	✓	✓	✓	✓	✓

Table 11: Part six of the analysis results of security protocols and cryptographic primitives in computational model. "✓" means the item is right

	Mateus *et al.* (2003)	Ramanathan *et al.* (2004)	Mitchell *et al.* (2005)	Galindo *et al.* (2008)	Cortier *et al.* (2006)	Blanchet (2007)	Barthe *et al.* (2004)
Symmetric encryption						✓	
Public key encryption						✓	
Hush function						✓	
Information folw						✓	
Digitial signature						✓	
Commitments				✓			
Security protocol	✓	✓	✓		✓	✓	
Polynomial-time processes calculus	✓	✓	✓			✓	
Automatic tool					✓		✓
Active adversary	✓	✓	✓	✓	✓	✓	✓

Table 12: Part seven of the analysis results of security protocols and cryptographic primitives in computational model. ✓ means the item is right

	Blanchet and Pointcheval (2006)	Jaggard *et al.* (2007)	Bhargavan *et al.* (2007)	Blanchet *et al.* (2008)	Bhargavan *et al.* (2008)	Blanchet (2009)	Meng *et al.* (2011a, b, c)	Meng and Shao (2010)	Meng (2011b, c)	Backes and Dumuth (2005)
Digitial signature		✓								
Security protocol		✓	✓	✓	✓	✓	✓	✓	✓	✓
Active adversary	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

security protocols and cryptographic primitives in computational model. means the item is right. In symbolic model the verification of security protocols have make a great development in automatic tools. However, the automatic tools which are usedd to verify the cryptographic primitives and security protocols in computational model are at the beginning stage. The verification on implementation of security protocols and cryptographic primitives with automatic tools should be got a serious attention owning to its great significance in real world.

ACKNOWLEDGMENT

This study was supported in part by Natural Science Foundation of The state Ethnic Affairs Commission of PRC under the grants No: 10ZN09, titled Research on the Provably Secure Remote Internet Voting Protocols without Physical Constrains, conducted in Wuhan, China from 1/1/2011 to 30/12/2011.

REFERENCES

Abadi, M. and A.D. Gordon, 1997. A calculus for cryptographic protocols: The spi calculus. Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, April 1-4, Switzerland, New York, pp: 36-47.

Abadi, M. and C. Fournet, 2001. Mobile values, new names and secure communication. Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, London, UK., March 2001, ACM New York, USA., pp: 104-115.

Abadi, M. and P. Rogaway, 2000. Reconciling two views of cryptography (the computational soundness of formal encryption). Proceedings of the 1st IFIP International Conference on Theoretical Computer Science, (IFIPTCS'00), Sendai, Japan, pp: 1-34.

Abadi, M. and P. Rogaway, 2002. Reconciling two views of cryptography (The computational soundness of formal encryption). J. Cryptol., 15: 103-127.

Abadi, M., B. Blanchet and C. Fournet, 2007. Just fast keying in the pi calculus. ACM Trans. Inf. Syst. Security 10: 9-9.

Acquisti, A., 2004. Receipt-free homomorphic elections and write-in voter verified ballots. Technical Report 2004/105, International Association for Cryptologic Research, May 2, 2004 and Carnegie Mellon Institute for Software Research International, CMU-ISRI-04-116, 2004. http://www. heinz.cmu. edu/~acq uisti /papers/acquisti-.

Adao, P., G. Bana, J. Herzog and A. Scedrov, 2005. Soundness of formal encryption in the presence of key-cycles. Proc. 10th Eur. Symp. Res. Comput. Security, 3679: 374-396.

Askarov, A., D. Hedin and A. Sabelfeld, 2006. Cryptographically-masked flows. Proc. 13th Int. Static Anal. Symp., 4134: 353-369.

Backes, M. and B. Pfitzmann, 2004. Symmetric encryption in a simulatable dolev-yao style cryptographic library. Proceedings of the 17th IEEE Computer Security Foundations Studyshop, June 28-30, IEEE Computer Society Washington, DC, USA., pp: 204-204.

Backes, M. and B. Pfitzmann, 2005. Relating symbolic and cryptographic secrecy. IEEE Trans. Dependable Secure Comput., 2: 109-123.

Backes, M. and M. Durmuth, 2005. A cryptographically sound dolev-yao style security proof of an electronic payment system. Proceedings of the 18th IEEE Computer Security Foundations Studyshop, June 20-22, Aix-en-Provence, France, pp: 78-93.

Backes, M. and P. Laud, 2006. Computationally sound secrecy proofs by mechanized flow analysis. Proceedings of the Studyshop on Formal and Computational Cryptography, November 2006, Alexandria, Virginia, USA., pp: 370-379.

Backes, M., B. Pfitzmann and M. Waidner, 2003a. A composable cryptographic library with nested operations. Proceedings of the 10th ACM conference on Computer and Communications Security, Oct. 27-30, Washington, DC., USA., pp: 220-230.

Backes, M., B. Pfitzmann and M. Waidner, 2003b. Symmetric authentication within a simulatable cryptographic library. Proc. ESORICS, 2808: 271-290.

Backes, M., C. Hritcu and M. Maffei, 2008. Automated verification of remote electronic voting protocols in the applied Pi-calculus. Proceedings of the 21st IEEE Computer Security Foundations Symposium, June 23-25, IEEE Computer Society, Washington, DC, pp: 195-209.

Backes, M., I. Cervesato, A.D. Jaggard, A. Scedrov and J.K. Tsay, 2006. Cryptographically sound security proofs for basic and public-key kerberos. ESORICS, 4189: 362-383.

Barthe, G., J. Cederquist and S. Tarento, 2004. A machine-checked formalization of the generic model and the random oracle model. IJCAR, 3097: 385-399.

Baskar, A., R. Ramanujam and S.P. Suresh, 2007. Knowledge-based modelling of voting protocols. Proceedings of the 11th Conference on theoretical Aspects of Rationality and Knowledge, June 25-27, Brussels, Belgium, pp: 62-71.

Baudet, M., V. Cortier and S. Kremer, 2005. Computationally sound implementations of equational theories against passive adversaries. Proc. Automata Languages Prog., 3580: 652-663.

Baudet, M., V. Cortier and S. Kremer, 2009. Computationally sound implementations of equational theories against passive adversaries. Inform. Comput., 207: 496-520.

Bella, G., F. Massacci and L.C. Paulson, 2006. Verifying the SET purchase protocols. J. Automated Reasoning, 36: 5-37.

Bellare, M., 1997. Practice-oriented provable security. ISW, 1561: 1-15.

Bhargavan, K., R. Corin and C. Fournet, 2007. Crypto-verifying protocol implementations in ML. Proceedings of the Studyshop on Formal and Computational Cryptography-FCC 2007. http://www.msr-inria.inria.fr/projects/sec/fs2cv/draft.pdf.

Bhargavan, K., R. Corin, C. Fournet and E. Zalinescu, 2008. Cryptographically verified implementations for TLS. Proceedings of the 15th ACM Conference on Computer and Communications Security, Oct. 27-31, Alexandria, Virginia, USA., pp: 459-468.

Blanchet, B. and D. Pointcheval, 2006. Automated security proofs with sequences of games. Proceedings of the 27th IEEE Symposium on Security, August 2006, LNCS, Santa Barbara, CA, Springer Verlag, pp: 537-554.

Blanchet, B., 2001. An efficient cryptographic protocol verifier based on prolog rules. Proceedings of the 14th IEEE studyshop on Computer Security Foundations, June 11-13, Cape Breton, Novia Scotia, Canada, pp: 82-82.

Blanchet, B., 2008. A computationally sound mechanized prover for security protocols. IEEE Trans. Dependable Secure Comput., 5: 193-207.

Blanchet, B., 2009. Diffie-hellman in cryptoverif. http://www.di.ens.fr/~blanchet/talks/FormaCrypt09-DH.pdf.

Blanchet, B., A.D. Jaggard, A. Scedrov and J. Tsay, 2008. Computationally sound mechanized proofs for basic and public-key kerberos. Proceedings of the ACM Symposium on Information, Computer and Communications Security, March 2008, Tokyo, Japan, pp: 87-99.

Bresson, E., Y. Lakhnech, L. Mazare and B. Warinschi, 2007. A generalization of DDH with applications to protocol analysis and computational soundness. Adv. Cryptol. CRYPTO, 4622: 482-499.

Burrows, M., M. Abadi and R. Needham, 1989. A logic of authentication. SIGOPS Oper. Syst. Rev., 23: 1-13.

Butler, F., I. Cervesato, A.D. Jaggard, A. Scedrov and C. Walstad, 2006. Formal analysis of Kerberos 5. Theoretical Comput. Sci., 367: 57-87.

Canetti, R. and J. Herzog, 2004. Universally composable symbolic analysis of cryptographic protocols (the case of encryption-based mutual authentication and key exchange). Cryptology ePrint Archive: Report 2004/334, 22 Feb. 2005. http://eprint.iacr.org/2004/334.

Canetti, R. and J. Herzog, 2006. Universally composable symbolic analysis of mutual authentication and key exchange protocols. Theory Cryptography, 3876: 380-403.

Canetti, R., 2001. Universally composable security: A new paradigm for cryptographic protocols. Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, Oct. 14-17, Las Vegas, Nevada, pp: 136-136.

Canetti, R., L. Cheung, D. Kaynar, M. Liskov, N. Lynch, O. Pereira and R. Segala, 2006. Time-bounded task-PIOAs: Aframestudy for analyzing security protocols. Distributed Comput., 4167: 238-253.

Comon-Lundh, H., V. Cortier and E. Zalinescu, 2010. Deciding security properties for cryptographic protocols. application to key cycles. ACM Trans. Comput. Logic, 11: 1-42.

Corin, R. and J. den Hartog, 2006. A probabilistic hoare-style logic for game-based cryptographic proofs. Automata Languages Programming, 4052: 252-263.

Cortier, V. and B. Warinschi, 2005. Computationally sound, automated proofs for security protocols. Programming Languages Syst., 3444: 140-140.

Cortier, V. and E. Zalinescu, 2006. Deciding key cycles for security protocols. Logic Programming Artificial Intell. Reasoning, 4246: 317-331.

Cortier, V., S. Delaune and P. Lafourcade, 2006. A survey of algebraic properties used in cryptographic protocols. J. Comput. Secur., 14: 1-43.

Cortier, V., S. Kremer and B. Warinschi, 2010. A survey of symbolic methods in computational analysis of cryptographic systems. J. Automated Reasoning, 10.1007/s10817-010-9187-9

Cramer, R., R. Gennaro and B. Schoenmakers, 1997. A secure and optimally efficient multi-authority election scheme. Lect. Notes Comput. Sci., 1233: 103-118.

Datta, A., A. Derek, J.C. Mitchell, V. Shmatikov and M. Turuani, 2005. Probabilistic polynomial-time semantics for protocol security logic. Automata Languages Programming, 3580: 16-29.

Datta, A., A. Derek, J.C. Mitchell and B. Warinschi, 2006. Computationally sound compositional logic for key exchange protocols. Proceedings of the 19th IEEE Studyshop on Computer Security Foundations, July 05-07, IEEE Computer Society Washington, DC, USA., pp: 321-334.

Delaune, S., S. Kremer and M.D. Ryan, 2006. Coercion-resistance and receipt-freeness in electronic voting protocol. Proceedings of 19th IEEE Computer Security Foundations Studyshop, July 5-7, Venice, Italy, pp: 28-42.

Dolev, D. and A. Yao, 1983. On the security of public-key protocols. IEEE Trans. Inform. Theory, 29: 198-208.

Fabrega, F.J.T., J.C. Herzog and J.D. Guttman, 1998. Strand space: Why is a security protocol correct? Proceedings of the IEEE Symposium on Security and Privacy, May 3-6, ACM, USA., pp: 160-171.

Fan, L., C.X. Xu and J.H. Li, 2002. Deniable authentication protocol based on Diffie–Hellman algorithm. Elect. Lett., 38: 705-706.

Fujioka, A., T. Okamoto and K. Ohta, 1992. A practical secret voting scheme for large-scale elections. Proceedings of the Studyshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, December 13-16, Springer-Verlag, London, UK., pp: 244-251.

Galindo, D., F.D. Garcia and P. van Rossum, 2008. Computational soundness of non-malleable commitments. Proceedings of the 4th Information Security Practice and Experience Conference, (ISPEC'08), Sydney, Australia, pp: 361-376.

Garcia, F.D. and P. van Rossum, 2008. Sound and complete computational interpretation of symbolic hashes in the standard model. Theoretical Comput. Sci., 394: 112-133.

Gerling, S., D. Jednoralski and X.Y. GU, 2008. Towards the verification of the civitas remote electronic voting protocol using proverif. http://www.infsec.cs.uni-sb.de/teaching/WS07/Seminar/reports/civitas-proverif.pdf.

Goldwasser, S. and S. Micali, 1984. Probabilistic encryption. J. Comput. Syst. Sci., 28: 270-299.

Goldwasser, S., S. Micali and R.L. Rivest, 1988. A digital signature scheme secure against adaptative chosen-message attacks. SIAM J. Comput., 17: 281-308.

Groth, J., 2004. Evaluating security of voting schemes in the universal composability framestudy. Applied Cryptography Netstudy Security, 3089: 46-60.

Guttman, J., D. Thayer, F. Javier and L.D. Zuck, 2001. The faithfulness of abstract protocol analysis: message authentication. Proceedings of the 8th ACM conference on Computer and Communications Security, Nov. 05-08, Philadelphia, PA, USA., pp: 186-195.

He, C., M. Sundararajan, A. Datta, A. Derek and J.C. Mitchell, 2005. A modular correctness proof of IEEE 802.11i and TLS. Proceedings of the 12th ACM Conference on Computer and Communications Security, Nov. 07-11, Alexandria, VA, USA., pp: 2-15.

Herzog, J., 2003. A computational interpretation of dolev-yao adversaries. Proceedings of the 3rd IFIP WG1.7 Studyshop on Issues in the Theory of Security, (WITS'03). http://citeseerx.ist.psu .edu/viewdoc /sunımary?doi=10.1.1.94.2941.

Herzog, J., 2005. A computational interpretation of Dolev-Yao adversaries. Theor. Comput. Sci., 340: 57-81.

Herzog, J., M. Liskov and S. Micali, 2003. Plaintext awareness via key registration. Lecture Notes Comput. Sci., 2729: 548-564.

Hoare, C.A., 1985. Communicating Sequential Processes. Prentice-Hall, Inc., USA.

Horvitz, O. and V.D. Gligor, 2003. Weak key authenticity and the computational completeness of formal encryption. Lecture Notes Comput. Sci., 2729: 530-547.

Jaggard, A.D., A. Scedrov and J. Tsay, 2007. Computationally sound mechanized proof of PKINIT for kerberos. Proceedings of the Studyshop on Formal and Computational Cryptography-FCC 2007. http://dimacs.rutgers.edu/~adj/Research/papers/jst 07fcc.pdf.

Janvier, R., Y. Lakhnech and L. Mazare, 2005a. (De)Compositions of cryptographic schemes and their applications to protocols. Cryptology ePrint Archive, Report 2005/020, 1 Feb. 2005. http://eprint.iacr.org/2005/020.pdf.

Janvier, R., Y. Lakhnech and L. Mazare, 2005b. Completing the picture: Soundness of formal encryption in the presence of active adversaries. Lecture Notes Comput. Sci., 3444: 172-185.

Jonker, H.L. and E.P. De-Vink, 2006. Formalising receipt-freeness. Proceedings of the 9th International Conference on Information Security, Aug. 30-Sept. 2, Samos Island, Greece, pp: 476-488.

Jonker, H.L. and W. Pieters, 2006. Receipt-freeness as a special case of anonymity in epistemic logic. Proceedings of the IAVoSS Studyshop on Trustworthy Elections, June 29-30, 2006, Cambridge, UK. http://doc.utwente.nl/65116/.

Joseph, C. and F. Cremers, 2006. Scyther-semantics and verification of security protocols. http://alexandria.tue.nl/extra2/200612074.pdf.

Kailar, R., 1996. Accountability in electronic commerce protocols. IEEE Trans. Software Eng., 22: 313-328.

Kessler, V. and H. Neumann, 1998. A sound logic for analysing electronic commerce protocols. Proceedings of the 5th European Symposium on Research in Computer Security, Sept. 16-18, London, UK., pp: 345-360.

Kremer, S. and L. Mazare, 2010. Computationally sound analysis of protocols using bilinear pairings. J. Comput. Security, 18: 999-1033.

Kremer, S. and M.D. Ryan, 2005. Analysis of an electronic voting protocol in the applied Pi calculus. Lect. Notes Comput. Sci., 3444: 186-200.

Kungpisdan, S. and Y. Permpoontanalarp, 2001. Practical reasoning about accountability in electronic commerce protocols. Proceedings of the 4th International Conference on Information Security and Cryptology, (ISC'01), Seoul, South Korea, pp: 135-174.

Kusters, R., A. Datta, J.C. Mitchell and A. Ramanathan, 2008. On the relationships between notions of simulation-based security. J. Cryptol., 21: 492-546.

Laud, P. and R. Corin, 2004. Sound computational interpretation of formal encryption with composed keys. Lecture Notes Comput. Sci., 2971: 55-66.

Laud, P. and V. Vene, 2005. A type system for computationally secure information flow. Lecture Notes Comput. Sci., 3623: 365-377.

Laud, P., 2001. Semantics and program analysis of computationally secure information flow. Lecture Notes Comput. Sci., 2028: 77-91.

Laud, P., 2002. Encryption cycles and two views of cryptography. Proceedings of the 7th Nordic Studyshop on Secure IT Systems, (SITS'02), USA., pp: 85-100.

Laud, P., 2003. Handling encryption in an analysis for secure information flow. Lecture Notes Comput. Sci., 2618: 159-173.

Laud, P., 2004. Symmetric encryption in automatic analyses for confidentiality against active adversaries. Proceedings of IEEE Symposium on Security and Privacy, (SOSP'04), Berkeley, California, pp: 71-85.

Laud, P., 2005. Secrecy types for a simulatable cryptographic library. Proceedings of the 12th ACM Conference on Computer and Communications Security, Nov. 07-11, ACM, New York, pp: 26-35.

Laud, P., 2008. On the computational soundness of cryptographically masked flows. Proceedings of the 35th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, (POPL'08), Canada, pp: 337-348.

Lee, B., C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, 2003. Providing receipt-freeness in mixnet-based voting protocols. http://caislab.icu.ac.kr/Paper/paper_files/2003/ICISC03/mnvoting-final-icisc20.pdf.

Lincoln, P., J. Mitchell, M. Mitchell and A. Scedrov, 1998. A probabilistic poly-time framestudy for protocol analysis. Proceedings of the 5th ACM Conference on Computer and Communications Security, Nov. 02-05, San Francisco, California, United States, pp: 112-121.

Lu, S., J. Zhang and L. Luo, 2009. The automatic verification and improvement of SET protocol model with SMV. Proceedings of the International Symposium on Information Engineering and Electronic Commerce, May 16-17, Ternopil, Ukraine, pp: 433-436.

Maggi, P. and R. Sisto, 2002. Using SPIN to verify security properties of cryptographic protocols. Proceedings of the 9th International SPIN Studyshop on Model Checking of Software, April 11-13, Springer-Verlag, London, pp: 187-204.

Mateus, P., J. Mitchell and A. Scedrov, 2003. Composition of cryptographic protocols in a probabilistic polynomial-time process calculus. Lecture Notes Comput. Sci., 2761: 327-349.

Meadows, C. and P.F. Syverson, 1998. A formal specification of requirements for payment transactions in the SET protocol. Proceedings of the Second International Conference on Financial Cryptography, Feb. 23-25, Springer-Verlag, London, pp: 122-140.

Meadows, C., 2003. Formal methods for cryptographic protocol analysis: Emerging issues and trends. IEEE J. Selected Areas Commun., 21: 44-54.

Meng, B. and Q. Xiong, 2004. SOCPT: A secure online card payment protocol. Proc. 8th Int. Conf., 2: 679-684.

Meng, B. and H.G. Zhang, 2005. Research on accountability in electronic transaction. Proceedings of the 9th International Conference on Computer Supported Cooperative Study in Design, May 24-26, Wuhan University China, pp: 745-749.

Meng, B., H. Zhang and Q. Xiong, 2005. The practical detailed requirements of accountability and its application in the electronic payment protocols. Proceedings of the 2005 IEEE international Conference on E-Technology, E-Commerce and E-Service, Mar. 29-Apr. 1, Acadmic Press, pp: 556-561.

Meng, B., 2007a. Analysis of internet voting protocols with jonker-vink receipt freeness formal model. Proceedings of the International Conference on Convergence Information Technology, Nov. 21-23, ICCIT., IEEE Computer Society, Washington, DC., pp: 663-669.

Meng, B., 2007b. An internet voting protocol with receipt-free and coercion-resistant. Proceedings of 7th IEEE International Conference on Computer and Information Technology, Oct. 16-19, IEEE Computer Society, Washington DC, USA., pp: 721-726.

Meng, B., 2008. Formal analysis of key properties in the internet voting protocol using applied pi calculus. Inform. Technol. J., 7: 1133-1140.

Meng, B., 2009a. A formal logic framestudy for receipt-freeness in internet voting protocol. J. Comput., 4: 184-192.

Meng, B., 2009b. A secure internet voting protocol based on non-interactive deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext J. Netstudys, 4: 370-377.

Meng, B., 2009c. Formalizing deniability. Inform. Technol. J., 8: 625-642.

Meng, B., 2009e. A secure non-interactive deniable authentication protocol with strong deniability based on discrete logarithm problem and its application on Internet voting protocol. Inform. Technol. J., 8: 302-309.

Meng, B., 2009d. A critical review of receipt-freeness and coercion-resistance. Inform. Technol. J., 8: 934-964.

Meng, B. and F. Shao, 2010. Computationally sound mechanized proofs for deniable authentication protocols with a probabilistic polynomial calculus in computational model. Inform. Technol. J., 10: 611-625.

Meng, B., W. Huang and J. Qin, 2010a. Automatic verification of security properties of remote internet voting protocol in symbolic model. Inform. Technol. J., 9: 1521-1556.

Meng, B., Z. Li and J. Qin, 2010b. A receipt-free coercion-resistant remote internet voting protocol without physical assumptions through deniable encryption and trapdoor commitment scheme. J. Software, 5: 942-949.

Meng, B., W. Huang, Z. Li and D. Wang, 2010c. Automatic verification of security properties in remote internet voting protocol with applied pi calculus. Int. J. Digital Content Technol. Appl., 4: 88-107.

Meng, B., 2011a. Automatic verification of deniable authentication protocol in a probabilistic polynomial calculus with cryptoverif. Inform. Technol. J., 10: 717-735.

Meng, B., 2011b. Computer aided verification of accountability in electronic payment protocol with cryptoverif. Int. J. Advancements Comput. Technol.,

Meng, B., 2011c. Refinement of mechanized proof of security properties of remote internet voting protocol in applied PI calculus with proverif. Inform. Technol. J., 10: 293-334.

Meng, B., F. Shao and W. Huang, 2011a. A computer-assisted framestudy for accountability of electronic payment protocol in computational model. Int. J. Advancements Comput. Technol.,

Meng, B., L. Li and F. Shao, 2011b. Computationally sound mechanized proofs for electronic payment protocol in a probabilistic polynomial calculus with cryptoverif. Int. J. Digital Content Technol. Appl.,

Meng, B., F. Shao, L. Li, W. Huang and D. Wang, 2011c. Automatic proofs of deniable authentication protocols with a probabilistic polynomial calculus in computational model. Int. J. Digital Content Technol. Appl., 5: 335-355.

Micciancio, D. and B. Warinschi, 2002. Completeness theorems for the abadi-rogaway logic of encrypted expressions. Proceedings of the 2nd IFIP WG1.7 Studyshop on Issues in the Theory of Security (WITS'02), 2002.

Micciancio, D. and B. Warinschi, 2004a. Soundness of formal encryption in the presence of active adversaries. Theory Cryptography (LNCS), 2951: 133-151.

Micciancio, D. and B. Warinschi, 2004b. Completeness theorems for the Abadi-Rogaway language of encrypted expressions. J. Comput. Sec., 12: 99-129.

Micciancio, D. and S. Panjwani, 2005. Adaptive security of symbolic encryption. Lecture Notes Comput. Sci., 3378: 169-187.

Mitchell, J.C., A. Ramanathan, A. Scedrov and V. Teague, 2005. A probabilistic polynomial-time calculus for the analysis of cryptographic protocols. Theor. Comput. Sci., 353: 118-164.

Mitchell, J.C., M. Mitchell and U. Stern, 1997. Automated analysis of cryptographic protocols using Mur. Proceedings of the 1997 IEEE Symposium on Security and Privacy, May 04-07, Digital Library, pp: 141-141.

Panti, M., L. Spalazzi, S. Tacconi and S. Valenti, 2003. Automatic verification of security in payment protocols for electronic commerce. Enterprise Inform. Syst., 4: 276-282.

Ramanathan, A., J. Mitchell, A. Scedrov and V. Teague, 2004. Probabilistic bisimulation and equivalence for security analysis of netstudy protocols. Lecture Notes Comput. Sci., 2987: 468-483.

Shaikh, A.R.R. and S. Devane, 2010. Formal verification of payment protocol using AVISPA. Int. J. Infonomics, Vol. 3. http://www.infonomics-society.org/IJI/Formal%20Verification%20of%20Payment%20protocol%20using%20AVISPA.pdf

Sprenger, C., M. Backes, D. Basin, B. Pfitzmann and M. Waidner, 2006. Cryptographically sound theorem proving. Proceedings of the 19th IEEE Studyshop on Computer Security Foundations, July 05-07, Venice, pp: 153-166.

Talbi, M., B. Morin, V. V.T. Tong, A. Bouhoula and M. Mejri, 2008. Specification of electronic voting protocol properties using ADM logic: FOO case study. Proceedings of the 10th international Conference on information and Communications Security, Oct. 20-22, Birmingham, UK., pp: 403-418.

Van Eijck, J. and S. Orzan, 2007. Epistemic verification of anonymity. Elect. Notes Theor. Comput. Sci., 168: 159-174.

Van Herreweghen, E., 2001. Non-Repudiation in set: Open issues. Financial Cryptography, 1962/2001: 140-156.