Hindawi Publishing Corporation
Discrete Dynamics in Nature and Society
Volume 2014, Article ID 904717, 7 pages
http://dx.doi.org/10.1155/2014/904717

Research Article

Fairness Analysis for Multiparty Nonrepudiation Protocols Based on Improved Strand Space

Lei Li,[1] Licheng Wang,[2] Jing Chen,[1] Ruiming Wang,[1] and Zhihong Zhang[1]

[1] *School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China*
[2] *Shanghai Key Lab of Modern Optical System, Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China*

Correspondence should be addressed to Lei Li; ielilei@zzu.edu.cn

Received 5 November 2013; Revised 21 November 2013; Accepted 21 November 2013; Published 2 January 2014

Academic Editor: Guoliang Wei

Aimed at the problem of the fairness analysis for multiparty nonrepudiation protocols, a new formal analysis method based on improved strand space is presented. Based on the strand space theory, signature operation is added; the set of terms, the subterm relation and the set of penetrator traces are redefined and the assumption of free encryption is extended in the new method. The formal definition of fairness in multi-party non-repudiation protocols is given and the guideline to verify it based on improved strand space is presented. Finally, the fairness of multi-party non-repudiation protocols is verified with an example of Kremer-Markowitch protocol, which indicates that the new method is suitable for analyzing the fairness of multiparty nonrepudiation protocols.

1. Introduction

As a crucial foundation of the realization of electronic commerce, nonrepudiation protocols provide the nonrepudiation services for the interbehavior between the network entities. Generally speaking, some security properties of the nonrepudiation protocols should be equipped with such as nonrepudiation, fairness, and timeliness, among which the fairness acts as the most important one. The nonrepudiation protocols are usually the ones being of one sender and multireceptors.

Formal methods, theory, and supporting tools paly an important role in the design, analysis, and verification of the security-related and cryptographic protocols [1]. There are numbers of approaches for analyzing the security protocol; however, it turns out to be that each one is subjected to its own limitations since it can only analyze a certain class of protocols or security properties. During the period of designing the security protocols, it is required to guarantee the security properties of security protocol as much as possible by applying multikinds of formal analysis methods. Currently, the formal analysis methods based on nonrepudiation protocols can be divided into two classes.

(1) Belief logic method: in [2], Kailar firstly extended the BAN logic and applied it to the analysis of fairness of the nonrepudiation protocols; the authors in [3, 4] analyzed the fairness and timeliness of the nonrepudiation protocols by using belief logic, respectively. In [5, 6], the authors introduced the alternating-time temporal logic analyzing the fairness of the nonrepudiation protocols. However, the formal analysis based on the belief logic method only works under a lot of assumptions.

(2) State space method: the automatic analysis method with a protocol checker adopted in [7] and Petri net method proposed in [8] both need to search the state space; while analyzing the complex space, human intervention is indispensable to both the two methods in case of the blast of state space.

In the recent years, some formal methods have been developed which are suitable for the analysis of nonrepudiation protocols; see, for example, [9–11]. However, fairness analysis for multi-party nonrepudiation protocols seems to be more complex, and only nonformal analysis for fairness,

and so on, has been done by utilizing various typical kinds of nonrepudiation protocols in [12–14].

The theory of strand space is a proof technique which is based on induction and free encryption assumption; furthermore, this theorem can analyze any protocol for any size neither constrained from the amounts of participative entities nor dependent on the state space searching. Nevertheless, in the strand space theory, some cryptographic primitives are lack of definition, such as signature; therefore, it is not suitable for the analysis of the fairness for multi-party nonrepudiation protocols.

In this paper, the operation for signature in the strand space theorem is added and the set of terms, subterm relation, and the set of penetrator traces are redefined. The assumption of free encryption is extended in the new method. The formal definition of fairness in multi-party nonrepudiation protocols is given and the guideline to verify it based on improved strand space is presented. Finally, the fairness of multi-party nonrepudiation protocols is verified with an example of Kremer-Markowitch protocol, which indicates that the new method is suitable for analyzing the fairness of multi-party nonrepudiation protocols.

2. The Basic Notions of Strand Space [15]

A strand is a sequence of events that a single principal may engage in. Each individual strand is a sequence of message transmissions and receptions, with specific values of all data such as keys and nonces. One may think of a strand space as containing all the legitimate executions of the protocol expected within its useful lifetime, together with all the actions that a penetrator might apply to the messages contained in those executions, together with penetrator part strands. The basic notions of a strand space, as follows.

Consider a set A, the elements of which are the possible messages that can be exchanged between principals in a protocol, and we will refer to the elements of A as terms.

A strand space is a pair (Σ, tr) with a trace mapping $\mathrm{tr}: \Sigma \to A$, in which Σ is the set of a strand; here, the strand can represent any sequences and be denoted by ζ.

Subterm: $t_1 \subseteqq t_1$ means that t_1 is a subterm of t_2.

Definition 1. A signed term is a pair $\langle \sigma, a \rangle$ with $a \in A$ and σ one of the symbols $+, -$. One will write a signed term as $+t$ or $-t$; $(\pm A)$ is the set of finite sequences of signed terms.

Definition 2. A strand space is a set Σ with a trace mapping $\mathrm{tr}: \Sigma \to (\pm A)$.

Definition 3. Fix a strand space with the following steps.

(1) A node is a pair $\langle \zeta, i \rangle$, with $s \in \Sigma$ and i an integer satisfying $1 \leq i \leq \mathrm{length}(\mathrm{tr}(s))$. The set of nodes is denoted by N. One will say that the node $\langle \zeta, i \rangle$ belongs to the strand s. Clearly, every node belongs to a unique strand.

(2) If $n_1, n_2 \in N$, $n_1 \to n_2$ means that term $(n_1) = +a$ and term $(n_2) = -a$. It means that node n_1 sends the message a, which is received by n_2, creating a causal link between their strands.

(3) If $n_1, n_2 \in N$, then $n_1 \Rightarrow n_2$ means that n_1, n_2 occur on the same strand. It expresses that n_1 is an immediate causal predecessor of n_2 in the strand.

(4) An unsigned term t occurs in $n \in N$ if and only if $t \subseteqq \mathrm{term}(n)$.

(5) I is an unsigned term set, node $n \in N$ is an entry point of I, if and only if $(n) = +t$, and whenever n' precedes n on the same strand, $t \subseteqq \mathrm{term}(n)$.

(6) An unsigned term t originates on $n \in N$ if and only if $I = \{t', t \subseteqq t'\}$.

(7) An unsigned term t is uniquely originating if and only if t originates on a unique $n \in N$.

A bundle is a portion of a strand space. It consists of a number of strands legitimate or otherwise hooked together where one strand sends a message and another strand receives that same message. Typically, for a protocol to be correct, each such bundle must contain one strand for each of the legitimate principals apparently participating in this session, all agreeing on the principals, nonces, and session keys. Penetrator strands or stray legitimate strands may also be entangled in a bundle, even in a correct protocol, but they should not prevent the legitimate parties from agreeing on the data values or from maintaining the secrecy of the values chosen.

Definition 4. If $\to_\Omega \subset \to$; $\Rightarrow_\Omega \subset \Rightarrow$; and $\Omega = \langle N_\Omega, (\to_\Omega \cup \Rightarrow_\Omega) \rangle$ is the subgraph of $\Omega = \langle N, (\to \cup \Rightarrow) \rangle$, then Ω is a bundle if and only if

(1) Ω is a finite acyclic graph;

(2) $n_2 \in N_\Omega$ and term N_2 is negative; thus, there exists a unique node n_1, so that $n_1 \to_\Omega n_2$;

(3) $n_2 \in N_\Omega$ and $n_1 \Rightarrow n_1$, then $n_1 \Rightarrow_\Omega n_2$.

3. The Improved Strand Space

In the basic theorem of strand space, only encryption and connection operation are defined for term set; however, neither the symmetric and asymmetric keys are distinguished nor the signature operation is defined. Nonrepudiation protocols are dependent on the cryptographic primitives of encryption and signature. Therefore, the basic strand space theorem is not suitable for analyzing the fairness of multi-party nonrepudiation protocols. In this paper, we redefine the term set A as follows.

Definition 5. The term set A satisfies the following conditions.

(1) $W \subseteq A$ is a set of atomic messages.

(2) $W_{\mathrm{name}} \subseteq A$ is the set of identifiers, ORT are used to denote origination party, receiving party and the trusted third party in our following discussions.

(3) $K \subseteq A$ is the set of keys; K and W are nonintersect and $\mathrm{inv}: K \to K$ is a monadic operator mapping one

key of the key pair in the asymmetric cryptosystem to another and mapping the symmetric key to itself.

(4) $P \subseteq K$, $P^{-1} \subseteq K$ is the set of asymmetric keys; one denotes the private key set as K and public key as P^{-1}.

(5) $K_s \subset K$ is the set of symmetric keys; K_s and P are nonintersect and also nonintersect with P^{-1}.

(6) Three binary operators Encr: $K_s \times A \rightarrow A$; Conn $A \times A \rightarrow A$; and sign $P \times A \rightarrow A$.

In this paper, we use the notation $E_k(m)$, gh, and $S_p(m)$ to denote the encryption of message m by key k, connection between g and h, and the signature of message m by private key P, respectively.

Due to the addition of the operation signature, relations of subterms are redefined as follows.

Definition 6. The recursion of subterm relations is defined as the minimum relation which satisfies the following relations:

(1) $a \sqsubseteq a$;

(2) $a \sqsubseteq E_k(g)$ if $a \sqsubseteq g$;

(3) $a \sqsubseteq S_p(g)$ if $a \sqsubseteq g$;

(4) $a \sqsubseteq gh$ if $a \sqsubseteq g \vee a \sqsubseteq h$.

The stand space theorem builds the model of actions by a penetrator and gives some formal descriptions about the basic penetrations of a penetrator; the penetrator's powers are mainly depicted by two ingredients, namely, a set of keys known initially to the penetrator and the capabilities to generate new messages from messages he receives.

The basic actions of the penetrator are characterized by a set of penetrator traces which are composed of the available atomic actions. Owing to the additions of operations such as signature, the penetrator traces are required to consist of some atomic operations including signature and verification. The penetrator traces are redefined with the following forms.

Definition 7. The penetrator traces include

(1) text message: $\langle +w \rangle$, $w \in W$;

(2) *key*: $\langle +k \rangle$, $k \in K$;

(3) concatenation: $\langle -g, -h, +gh \rangle$;

(4) separation into components: $\langle -gh, +g, +gh \rangle$;

(5) encryption: $\langle -k, -h, +E_k(h) \rangle$;

(6) decryption: $\langle -k^{-1}, -E_k(h), +h \rangle$;

(7) signature: $\langle -p, -h, -S_p(h) \rangle$, $p \in P$;

(8) verification: $\langle -p^{-1}, -S_p(h), +h \rangle$.

In the assumption of free encryption, it stipulates that a ciphertext can be regarded as a ciphertext in just one way. After *Dolev* and *Yao*, the assumption of free encryption has been fully applied to different kinds of formal analysis methods.

In the basic strand space theorem, A is the algebra freely generated from K and W by the two operators' encryption and join. The following are some extensions of the assumption of free encryption due to the addition of signature operation.

Axiom. For $m', m' \in A$, $k, k' \in K_s$, $P_a, P_b, P_c \in P$, $a, b, c \in W_{\text{name}}$,

(1) $S_{P_a}(m) = S_{P_b}(m') \Leftrightarrow m = m' \wedge P_a = P_b \wedge a = b$;

(2) $mm' \neq E_{k'}(m) \neq S_{P_c}(m')$;

(3) $S_{P_c}(m) \neq W \cup K$.

The improved strand space method is a formal analysis method consisting of some key concepts, for example, the redefined term set, relations between subterms, penetrator traces, extended assumption of free encryption, and the bundles in the basic strand space, and also combining with protocol traces and theorem proof.

4. Definition of Fairness and Proof Line

Among numbers' properties of the nonrepudiation protocols possess, fairness is the most important one which includes two aspects; first, when the protocols are completed, the origination party received the evidence of nonrepudiation protocols from receiving party and denoted by Z_{nrr} was well as receiving party received the evidence of nonrepudiation protocols from origination party and is denoted by Z_{nro}; second, when the protocols are terminated abruptly, it should have the capability to keep both sides of communication equal and neither sides in a dominant position. Hence, we make a formal definition as the following form about fairness.

Definition 8. If the origination party receives Z_{nrr} if and only if the receiving party receives Z_{nor}, then we say that the nonrepudiation protocols satisfy the fairness.

In the multi-party nonrepudiation protocols, there exists one origination party and multireceiving parties, and in the process of protocol running, it is allowable that some receiving parties complete the protocols and the others terminate the protocols. If we denote the ith receiver as R_i, the ith nonrepudiation evidence of receiving party as $Z_{\text{nrr}i}$, and the ith nonrepudiation evidence of origination party as $Z_{\text{nro}i}$, then the fairness is defined as follows.

Definition 9. If the origination party receives $Z_{\text{nrr}i}$ if and only if the receiving party receives $Z_{\text{nro}i}$, then one says that the nonrepudiation protocols satisfy the fairness.

We can consider the proof of fairness from two aspects: firstly, when origination party receives $Z_{\text{nrr}i}$, it is sure that the receiving party receives $Z_{\text{nro}i}$; secondly, when origination party O receives $Z_{\text{nro}i}$, then the receiving party R certainly receives $Z_{\text{nrr}i}$. Hence, the conditions in Definition 9 are satisfied and the protocols are guaranteed to meet the fairness.

The proof steps of the fairness of multi-party nonrepudiation protocols by using the improved strand model are listed as follows.

(1) Build the strand model for multi-party nonrepudiation protocols.

(2) Prove that if there exists originator strand in bundle Ω and the nodes in the stand contain term Z_{nrri}, then there must exist receiver strand as well as the nodes in this strand contain term Z_{nroi}.

(3) Prove that if there exists receiver strand in bundle Ω and the nodes in the strand contain term Z_{nroi}, then there must exist originator strand as well as the nodes in this stand contain term Z_{nrri}.

5. Prove the Fairness of KM Protocol Based on Extended strand Method

5.1. KM Protocol. KM protocol is a typical multi-party nonrepudiation protocol, and we denote the notation in the protocol as follows:

(1) O, T denotes origination party and the trusted third party TTP of protocols;

(2) $R = P_{R_1'}(R_1'), P_{R_2'}(R_1'), \ldots : R'$ is the subset of R and represents the receiver set which returns the valid evidence to O, $R_i' \in R'$;

(3) l represents the unique identifier of the current running protocol;

(4) m: message from O to R;

(5) k: a symmetric secret key used when O encrypts M;

(6) $C = E_k(m)$: cryptograph of message M from O to R;

(7) $A \rightarrow B$: customer A sends a message to customer B;

(8) $A \Rightarrow B$: customer A broadcasts a message to customer B;

(9) $A \leftrightarrow B$: the obtained operations of A to B, namely, A can always get messages from B;

(10) $E_R(m)$ encrypts secret key k by utilizing the group encryption mechanism, and only $R_i' \in R'$ can decrypt and obtain k;

(11) $Z_o = S_{po}(R, L, C)$: the evidence of signatured cryptograph C from originator to R;

(12) $Z_{r_i} = S_{r_i}(O, L, C)$: signatured cryptograph C from originator to R_i receives evidence;

(13) $Z_{s_k} = S_{P_o}(R', L, E_{R'}(k))$: a secret key k is sent to R' from the signatured O by TTP and the evidence received by R' from secret key k.

The KM protocol can be described as follows:

(1) $O \Rightarrow R : R, L, C, Z_0$;

(2) $R_i \Rightarrow O : O, L, Z_{R_i}$;

(3) $O \Rightarrow T : R', L, E_R(k), Z_{sk}$;

(4) $R \leftrightarrow T : O, R', L, E_{R'}(k), Z_{ck}$;

(5) $O \leftrightarrow T : O, R', L, E_{R'}(k), Z_{ck}$.

Firstly, originator O broadcasts C and evidence Z_0 to the receiver set R, and $R \in R'$ responses by evidence Z_{R_i} when it receives the messages, and then O submits k to the trusted third party with group encryption form $E_{R'}(k)$; finally, O and R can obtain $E_{R'}(k)$ and evidence Z_{ck} from T by obtaining operations.

Nonrepudiation evidence $Z_{\text{nrri}} = (Z_{ri}, Z_{ck})$; $Z_{\text{nroi}} = (Z_o, Z_{ck})$ for all $R_i \in R'$. If there exists any argument, O can submit Z_{nroi} to arbitration agency for arbitration.

5.2. KM Strand Space. The obtained operations in KM protocol can be regarded as the message m can be always received by O and R from T. Denote $f(n)$ as the sign term of node n and $f'(n)$ as the unsigned parts of $f(n)$. The obtained operation can be defined as follows in the improved strand space.

Definition 10. If entity a obtains message m from T by obtained operation, then strand ζ_T satisfies $\exists i \cdot f(\langle \zeta_T, i \rangle)$. Denoting bundle Ω as an arbitrary bundle satisfying $\zeta_T \in \Omega$, there always exists $\zeta_a \in \Omega$ satisfying $\exists j \cdot f(\langle \zeta_a, j \rangle) = -m$ and $\langle \zeta_T, i \rangle \prec \langle \zeta_a, j \rangle$.

KM strand space can be depicted with the following form.

Definition 11. Assuming that (Σ, ρ) is a penetrator strand space, if Σ is comprised of the following four kinds of strands, then one says that Σ is a KM strand space.

(1) The penetrator strand: $s \in \rho$.

(2) The originator strand $s \in \zeta_O[O, R, R', T, L, m, k]$, whose traces are $\langle +RLE_k(m)Z_o, -OLZ_{R_i}, +R'LE_{R'}(K)Z_{sk}, -OR'LE_{R'}(k)Z_{ck} \rangle$, $O, R, R', T \in W_{\text{name}}$; $L, m \in W$, and $L, m \notin W_{\text{name}}$; $k \in K_s$. Here, $\zeta_O[O, R, R', Lm, k]$ is a trace set whose elements are the traces discussed above and the corresponding entity is originator O.

(3) The receiver strand $s \in \zeta_R[O, R, R', T, L, m, k]$, whose traces are $\langle -RLE_k(m)Z_o, +OLZ_{R_i}, -OR'LE_{R'}(k)Z_{ck} \rangle$, $O, R, R', T \in W_{\text{name}}$; $L, m \in W$ and $L, m \notin W_{\text{name}}$; $k \in K_s$. Here, $\zeta_O[O, R, R', Lm, k]$ is a trace set whose elements are the traces discussed above and the corresponding entity is receiver R_i.

(4) The trusted third strand $s \in \zeta_T[O, R, R', T, L, k]$, whose traces are $\langle -R'LE_{R'}(k)Z_{sk}, +ORLE_{R'}Z_{ck}, +ORLE_{R'}Z_{ck} \rangle$. Here, $\zeta_T[O, R, T, L, k]$ is a trace set whose elements are the traces discussed above and the corresponding entity is the trusted third part T.

We say that the originator strand, receiver strand, and trusted third strand are all regular strands whose nodes are called regular nodes. Given a strand in the Σ, we can confirm that whether it belongs to penetrator strand, originator strand, receiver strand, or the trusted third part strand uniquely form its formal. Therefore, there is no confusion for omitting ρ of the KM strand space (Σ, ρ).

5.3. Analysis of Fairness of the KM Protocol. In order to prove KM protocol that satisfies the fairness, we need to prove the following two propositions.

Proposition 12. *Assume the following conditions are true:*

(1) Σ *is a KM strand space,* Ω *is a bundle in the* Σ*, and* s *is an originator strand in* $\zeta_0[O, R, R', T, L, m, k]$ *which includes the compositions* Z_{R_i} *and* Z_{ck} *of* Z_{nrri}*;*

(2) $P_O \notin K_\rho$*;* $P_{R_i} \notin K_\rho$*;* $P_T \notin K_\rho$ *(*P_O*,* P_{R_i}*,* P_T *represent the private key of originator party, receiver party, and TTP, respectively, and* K_ρ *represents a private space known well by penetrator);*

(3) $L \neq m$*;* L*,* m*,* k *are the only original terms in* Σ*;*

then the bundle Ω *consists of a receiver strand* $r \in \zeta_R[O, R, R', T, L, m, k]$ *as well as* r *consists of the compositions* Z_o *and* Z_{ck} *of* Z_{nroi}*.*

Proposition 13. *Assume the following conditions are true:*

(1) Σ *is a KM strand space,* Ω *is a bundle in the* Σ*, and* r *is a receiver strand in* $\zeta_R[O, R, R', T, L, m, k]$ *which includes the compositions* Z_O *and* Z_{ck} *of* Z_{nroi}*;*

(2) $P_O \notin K_\rho$*;* $P_R \notin K_\rho$*;* $P_T \notin K_\rho$ *(*P_O*,* P_{R_i}*,* P_T *represents the private key of originator party, receiver party, and TTP, respectively, and* K_ρ *represents a private space known well by penetrator);*

(3) $L \neq mL$*,* m*,* k *are the only original terms in* Σ*;*

then the bundle Ω *consists of an originator strand* $r \in \zeta_O[O, R, R', T, L, m, k]$ *as well as* s *consists of the compositions* Z_{Ri} *and* Z_{ck} *of* Z_{nrri}*.*

In the following section, we focus our attention on the proof of Proposition 12 in terms of a series of lemmas. Choose Σ, Ω, s, O, R, T, L, m, k arbitrarily which satisfy the assumptions in Proposition 12. It is obvious that terms Z_{Ri} and Z_{ck} are included in s. The output value $RLE_k(m)Z_O$ of node $\langle s, 1\rangle$ is denoted by n_0 whose term is denoted by v_0.

Lemma 14. *Term* Z_{ck} *originates from regular node* n_3*.*

Proof. As $Z_{ck} = S_{P_T}(O, R', L, E_{R'}(k))$, we assume that term Z_{ck} originates from regular node n_3, and then we investigate the probability of positive node in the penetrator traces, respectively:

(1) $\langle +w\rangle$, $w \in W$; it follows from the assumption of free encryption that $Z_{ck} \nsubseteqq w$ thus, n_3 is not its positive node;

(2) $\langle +k\rangle$, $k \in K$; it follows from the assumption of free encryption that $Z_{ck} \nsubseteqq k$; thus, n_3 is not its positive node;

(3) $\langle -g, -h, +gh\rangle$; if n_3 is its positive node, then $Z_{ck} \subseteqq gh$ and we can confirm that $Z_{ck} \subseteqq g \vee Z_{ck} \subseteqq h$. Therefore, there obviously exists positive node n' to make sure that $Z_{ck} \subseteqq f(n') \wedge n' \prec n_3$, which is in contradiction with that n is the original node;

(4) $\langle -gh, +g, +h\rangle$; if n_3 is its positive node, then $Z_{ck} \subseteqq g \vee Z_{ck} \subseteqq h$ and we can confirm that $Z_{ck} \subseteqq gh$. Therefore, there obviously exists positive node n' to make sure that $Z_{ck} \subseteqq f(n') \wedge n' \prec n_3$, which is in contradiction with that n is the original node;

(5) $\langle -k, -h, +E_k(h)\rangle$; if n_3 is its positive node, we can confirm that $Z_{ck} \subseteqq h$ since $E_k(h) \neq Z_{ck}$. Therefore, there obviously exsits positive node n' to make sure that $Z_{ck} \subseteqq f(n') \wedge n' \prec n_3$, which is in contradiction with that n is the original node;

(6) $\langle -k^{-1}, -E_k(h), +h\rangle$; if n_3 is its positive node, then $Z_{ck} \subseteqq h$ and we can confirm that $Z_{ck} \subseteqq E_k(h)$. Therefore, there obviously exists positive node n' to make sure that $Z_{ck} \subseteqq f(n') \wedge n' \prec n_3$, which is in contradiction with that n is the original node;

(7) $\langle -p, -h, +S_p(h)\rangle$; $S_p(h) \neq Z_{ck}$ since $p \in K_p$, $P_T \notin K_p$. Hence, if n_3 is its positive node, then $Z_{ck} \subseteqq S_p(h)$ and we can confirm that $Z_{ck} \subseteqq h$. Therefore, there obviously exists positive node n' to make sure that $Z_{ck} \subseteqq f(n') \wedge n' \prec n_3$, which is in contradiction with that n is the original node;

(8) $\langle -p^{-1}, -S_p(h), +h\rangle$; if n_3 is its positive node, then $Z_{ck} \subseteqq h$ and we can confirm that $Z_{ck} \subseteqq S_p(h)$. Therefore, there obviously exists positive node n' to make sure that $Z_{ck} \subseteqq f(n') \wedge n' \prec n_3$, which is in contradiction with that n is the original node.

Summing up the above discussions, it is impossible that n_3 is in only one penetrator strand. Therefore, n_3 is a regular node. □

Lemma 15. *Assume that* n_3 *is on the regular strand* t*; then* t *is a trusted third party of* Ω*.*

Proof. Node n_3 is a positive regular node containing terms with the form of $S_p(a, b, c, d)$. Among the whole regular nodes, only the second and third nodes of the trusted third strand consist of such terms; furthermore, n_3 is the original node of Z_{ck}; hence, n_3 is the second node of the trusted third party strand. It follows from the creditability of the trusted third party that there must exist the third strand of this strand; therefore, t is the trusted third party strand of bundle Ω. □

Lemma 16. *Term* Z_{Ri} *originates from regular node* n_2*.*

Proof. As $Z_{Ri} = S_{P_{Ri}}(O, L, E_K(m))$. Assuming that term Z_{Ri} originates from n_2, we investigate the penetrator traces successively. With the similar proof of Lemma 14, we can conclude that n_2 is the regular node. □

Lemma 17. *m originates from regular node* n_0*.*

Proof. As $Z_{Ri} = S_{P_{Ri}}(O, L, E_K(m))$. It follows from the assumption that $m \subseteqq n_0$ and n_0 is positive. Since there is no predecessor in the strand which n_0 locates, we can derive that m originates from n_0. □

Lemma 18. *It is assumed that* n_2 *is on the regular strand* r*; then there exists predecessor* n_1 *of* n_2 *in the* r *and* $m \subseteqq f(n_1)$*.*

Proof. Because $Z_{Ri} \subseteqq n_2$, $Z_{Ri} \nsubseteqq n_0$, we have $n_2 \neq n_0$. It can be seen that m originates from n_0; together with condition (3) of Proposition 12, we have only m original in the Σ; hence, m

does not originate from n_2. Furthermore, $m \sqsubseteq Z_{Ri} \sqsubseteq f(n_2)$, then there must exist predecessor n_1 of n_2 in the strand r to guarantee $m \sqsubseteq f(n_1)$. □

Lemma 19. *Regular strand r consisting of n_1 and n_2 is a receiver strand in the bundle of Ω.*

Proof. Nodes n_1 and n_2 in the regular strand r satisfy the following properties: (1) n_2 is a positive regular node; (2) n_2 consists of a subterm with form of $S_p(a, b, E_k(c))$; (3) n_1 and n_2 are predecessors in the strand r; and (4) $m \sqsubseteq f(n_1)$. Investigating the whole regular strands in the bundle of Ω, we found that only the first and the second nodes of the receiver strand satisfy the conditions listed above. Regular strand r consisting of n_1 and n_2 is a receiver strand in the bundle of Ω. In addition, from Lemma 15 we can see that there exists a trusted third party t to guarantee $f(\langle t, 3\rangle) = +OR'LE_{R'}(k)Z_{ck}$. According to Definition 10, there must exist a node n' in the receiver strand r to make sure that $f(n') = -OR'LE_{R'}(k)Z_{ck}$, which is the third node in the receiver strand while investigating the receiver in bundle Ω. □

Lemma 20. *Receiver strand r consists of terms Z_o and Z_{ck}.*

Proof. According to the definition of receiver strand in the KM strand space, r obviously contains Z_o and Z_{ck}. □

Summing up the lemmas discussed above, we can derive that Proposition 12 is true.

In order to prove that Proposition 13 along the similar proof line, we can firstly prove there exists a trusted third party in the bundle Ω in terms of the original of Z_{ck}, and then prove that there exists originator strand in bundle Ω by using the original of m, k, Z_o.

6. Conclusions

It can be seen that some operations have not been defined in the basic strand space theorem such as signature. In this paper, we add the signature operation and redefine the term set, relations between subterms, and penetrator traces as well as extend the assumption of free encryption. Furthermore, the formal definition of fairness of multiparty nonrepudiation protocols is put forward. Idea and method of fairness analysis for multi-party nonrepudiation protocols based on improved strand space have been discussed in detail. Analyzing the fairness of KM protocol by using the analysis method based on improved strand space, we can conclude that KM protocol satisfies the fairness property, which shows that our improved strand space method is suitable for fairness analysis for multi-party nonrepudiation protocols. Kim's work [16] has revealed that ZG protocol in [17] cannot meet the timeliness. Our further research topic would be to investigate the corresponding other properties for multi-party nonrepudiation protocols, such as nonrepudiation and/or timeliness. Consequently, it is an extension of our results and seems to be much more interesting and challenging.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the 863 Program of China under Grant 2011AA01A201, Technological Brainstorm Project of Henan Province of China under Grant 12B520054, the National Natural Science Foundation of China under Grant 61074016, the Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning, the Program for New Century Excellent Talents in University under Grant NCET-11-1051, the Leverhulme Trust of the UK, and the Alexander von Humboldt Foundation of Germany.

References

[1] S. Gritzalis, D. Spinellis, and P. Georgiadis, "Security protocols over open networks and distributed systems: formal methods for their analysis, design, and verification," *Computer Communications*, vol. 22, no. 8, pp. 697–709, 1999.

[2] R. Kailar, "Accountability in electronic commerce protocols," *IEEE Transactions on Software Engineering*, vol. 22, no. 5, pp. 313–328, 1996.

[3] L. Botao and L. Junzhou, "On timeliness of a fair non-repudiation protocol," in *Proceedings of the 3rd International Conference on Information Security (InfoSecu '04)*, pp. 99–106, Shanghai, China, November 2004.

[4] Y. Xu and X. Xie, "Analysis of electronic commerce protocols based on extended rubin logic," in *Proceedings of the 9th International Conference for Young Computer Scientists (ICYCS '08)*, pp. 2079–2084, Hunan, China, November 2008.

[5] W. Jamroga, S. Mauw, and M. Melissen, "Fairness in non-repudiation protocols," in *Proceedings of the 7th International workshop on security and trust management*, pp. 122–139, Copenhagen, Denmark, June 2011.

[6] S. Kremer and J. F. Raskin, "A game-based verification of non-repudiation and fair exchange protocols," in *CONCUR, 2001—Concurrency Theory*, pp. 551–565, Springer, Berlin, Heidelberg, 2001.

[7] R. Lanotte, A. Maggiolo-Schettini, and A. Troina, "Automatic analysis of a non-repudiation protocol," *Electronic Notes in Theoretical Computer Science*, vol. 112, pp. 113–129, 2005.

[8] Y. Guo, C. Lin, and H. Yin, "Formal proof of the IDOP-SP protocol based on the Petri Net," in *Proceedings of the IEEE International Conference on Networking, Architecture, and Storage (IEEE NAS '08)*, pp. 161–162, Chongqing, June 2008.

[9] L. Chen and X. Li, "Cryptographic protocol logic for analyzing a variety of security properties and its formal semantics," *International Journal of Advancements in Computing Technology*, vol. 4, no. 9, pp. 283–293, 2012.

[10] J. Dreier, P. Lafourcade, and Y. Lakhnech, "Formal verification of e-Auction protocols," in *Proceedings of the 2nd International Conference on Principles of Security and Trust*, pp. 247–266, Rome, Italy, 2013.

[11] H. Zhang, "Analysis on authentication secrecy of non-repudiation protocols," in *Proceedings of the International Conference*

on Electrical and Electronics Engineering, pp. 705–711, Wuhan, China, 2011.

[12] G. Draper-Gil, J. Zhou, J. L. Ferrer-Gomila, and M. F. Hinarejos, "An optimistic fair exchange protocol with active intermediaries," *International Journal of Information Security*, vol. 12, no. 4, pp. 299–318, 2013.

[13] S. Kremer and O. A. Markowitch, "Multi-party non-repudiation protocol," in *Proceedings of the 15th International Conference on Information Security*, pp. 271–280, Beijing, China, 2000.

[14] J. Zhou, J. Onieva, and J. Lopez, "Optimized multi-party certified email protocols," *Information Management and Computer Security*, vol. 13, no. 5, pp. 350–366, 2005.

[15] F. J. T. Fabrega, J. C. Herzog, and J. D. Guttman, "Strand spaces: Why is a security protocol correct," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 160–171, Oakland, Calif, USA, 1998.

[16] K. Kim, S. Park, and J. Baek, "Improving fairness and privacy of Zhou-Gollmanns fair non-repudiation protocol," in *Proceedings of the International Workshops on Parallel Processing*, pp. 140–145, IEEE Computer Society Press, 1999.

[17] J. Zhou and D. Gollmann, "Fair non-repudiation protocol," in *Proceedings of the 17th IEEE Symposium on Security and Privacy*, pp. 55–61, May 1996.