The ISC Int'l Journal of Information Security

July 2018, Volume 10, Number 2 (pp. 107–115)

http://www.isecure-journal.org

Distributed Contingency Logic and Security

Rahim Ramezanian [1,*]

[1] *Department of Mathematical Sciences, Sharif University of Technology, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 11 January 2018
First Revised: 20 January 2018
Last Revised: 13 June 2018
Accepted: 26 July 2018
Published Online: 28 July 2018

Keywords:
Contingency Logic, Distributed Contingency, Secret Sharing, MITM Attack.

ABSTRACT

In information security, *ignorance is not bliss*. It is always stated that hiding the protocols (let the other be ignorant about it) does not increase the security of organizations. However, there are cases that ignorance creates protocols. In this paper we propose distributed contingency logic, a proper extension of contingency (ignorance) logic. Intuitively, a formula is distributed contingent in a group of agent if and only if it is not follow from the knowledge of all individual agents put together. We formalize secret sharing scheme (a security property that is built upon ignorance of all agents), and a man in the middle attack to a weak protocol in our logic. We also illustrate a condition where disclose a secret may hide another one for ever. Finally we prove the main theorems of every logics, soundness and completeness. We also prove that the distributed contingency logic is more expressive than the classical contingency logic and the epistemic logic.

1 Introduction

Security protocols are widely used in transportation and storage of data. They are some rules and instructions that perform security-related functions. Are they safe and correct? How we can detect unauthorized actions? A path to answering these questions is formal methods [1–3]. They are approaches to describing computational entities in a logical language and reasoning about their behavior.

In this paper we define a logical language to describe ignorance based properties in security protocols. We study three different problem. The first one is the formal description of secret sharing schema, the next one is formalization of a man in the middle attack. The third problem is too interesting, we provide an environment with two secrets, then by uncovering the first secret, we hide the second one forever.

Consider a secret sharing schema [4–6] with $m+1$ agents. Each agent, i, has a unique local secret, (x_i, y_i). Everyone knows that $y_i = f(x_i)$ where f is a polynomial of degree m. The polynomial is the main secret and no one knows it. If the agents share their knowledge about local secrets then by polynomial interpolation techniques they can find f.

Secret sharing schema has two properties, the first one is *capability to learn the main secret* whenever all agents cooperate and put their local secrets together. Besides that the second property is *any proper subgroup of agents can not learn the main secret*. In above example any group B of m agents can not find f through communication since they do not have enough points to run interpolation algorithm.

The part that agents can learn main secret through communication can be formalized in epistemic logic with *distributed knowledge* [7–10] operator. A formula is distributed knowledge among a group of agents if

* Corresponding author.
Email address: rahim.ramezanian1@student.sharif.ir (R. Ramezanian)
ISSN: 2008-2045

it is deducible from all their knowledge put together.

The second property of secret sharing states that for proper subgroups of agents the main secret is not distributed knowledge, it means agents of the subgroup can not learn the main secret if they do not share local secrets with other agents. The property stronger it also says the agents in the proper subgroup can not put aside the main secret. More formally if ϕ is the main secret then $\neg\phi$ is not distributed knowledge for them, too.

In logic of knowledge when an agents does not know a fact and also does not know its negation, we formalize that with contingency operator. Contingency [11–14] is an important notion in the logic of knowledge. If something is contingent then it is possibly true or possibly false. More precisely a "formula ϕ is contingent" means the agent is ignorant about ϕ, or in other words he does not know whether ϕ. Something is non-contingent if it is not contingent.

In some related articles [13, 15, 16] iglearnnorance and knowing whether operators are used to capture similar notion to non-contingency. In some models the non-contingency $\Delta\phi$, can be defined by the knowledge operator as $K\phi \vee K\neg\phi$. The interesting muddy children puzzle [17] can be formalizing better in contingency logic [18] instead of epistemic logic.

To formalizing the second property of secret sharing schema where the main secret and its negation are not distributed knowledge for the proper subgroup we extend the contingency logic to *distributed contingency logic* and we say the main secret is *distributed contingent* for the subgroup.

We denote distributed contingency operator with D. Intuitionistically, a formula $D_B\phi$ means agents in group B can not learn ϕ, and we say ϕ is distributed contingent for B.

A formula ϕ maybe contingent for every agent in the group (nobody knows whether ϕ) and be distributed knowledge between them. In this paper we study the situation where the agents can not reach to ϕ even if they put all their knowledge together. Thus they can not learn ϕ. We call this notion distributed contingency.

In [19], which is an extended abstract, author defined a similar notion *distributed knowledge whether*, with a bisimulation relation, on Kripke semantics. In this paper we focus to use our logic in formal modeling of security properties [1, 20, 21]. We also use neighborhood semantics that present possible worlds in a more geometric space, which can be seen in Section 3.1.

The paper is organized as follows. In section 2 we define the distributed contingency logic, its syntax, semantics, axiom sets, and the completeness theorem. Section 3 is assigned to application of our logic in security. We formalize three interesting security cases (secret sharing scheme, man in the middle attack, and Revealing A Secret To Hide Another One) in distributed contingency logic. In section 4 we show that our logic is more expressive than classical contingency logic, and epistemic logic. We put logical backgrounds and proofs of main theorems of logical part in the appendix.

2 Distributed Contingency Logic: Language and Semantics

In the following we define the syntax and semantics of distributed contingency logic. A finite group of agents A and a countable set of atomic formulas P are assumed to be given.

Definition 1. The language of Distributed Contingency logic, L_{DC}, over P and A is given by the following BNF:

$$\phi := p \mid \neg\phi \mid (\phi \wedge \phi) \mid \Delta_a\phi \mid D_B\phi$$

Formula $\Delta_a\phi$ is read as "it is non contingent for a that ϕ" and $D_B\phi$ is read as "in group B it is distributed non-contingent that ϕ".

Definition 2 (Neighborhood Model). A neighborhood model is a triple $M = (S, N, V)$ where S is a nonempty set of possible worlds, $N = \{N_a \mid a \in A\}$ is a set of functions such that $N_a : S \to P(P(S))$, and V is a valuation function.

Definition 3. Let $M = (S, N, V)$ be a neighborhood model. The satisfaction relation between a world (M, s) and a formula $\phi \in L_D$ is inductively defined as follows,

$$\begin{aligned}
M, s &\models \top && \text{iff true}\\
M, s &\models p && \text{iff } s \in V(p)\\
M, s &\models \neg\phi && \text{iff } M, s \not\models \phi\\
M, s &\models \phi \wedge \psi && \text{iff } M, s \models \phi \text{ and } M, s \models \psi\\
M, s &\models \Delta_a\phi && \text{iff } \phi^M \in N_a(s) \text{ or } (\neg\phi)^M \in N_a(s)\\
M, s &\models D_B\phi && \text{iff } \phi^M \in N_B(s) \text{ or } (\neg\phi)^M \in N_B(s)
\end{aligned}$$

where ϕ^M denotes the truth set of ϕ in M, (the set of all possible worlds that satisfy ϕ), also $N_B(s)$ is defined as follows,

$$N_B(s) = \{X \subseteq S \mid \textstyle\bigcap_{a\in B} c_a(s) \subseteq X\}$$

where $c_a(s) = \bigcap_{a \in A} N_a(s)$ is the core of $N_a(s)$.

Example 1. Let $M = (S, N, V)$ be a neighborhood model where $A = \{a, b\}$, $S = \{0, 1\}$, $V(p) = \{1\}$ and

- $N_a(0) = N_b(0) = \{\{0, 1\}\}$,
- $N_a(1) = N_b(1) = \{\{1\}, \{0, 1\}\}$.

then $p^M = \{1\} \notin N_a(0)$ so $M, 0 \models \neg\Delta_a p$.

Definition 4 (Neighborhood Properties). Let $M = (S, N, V)$ be a neighborhood model, $s \in S$, $a \in A$ and $X, Y \subseteq S$. Then,

(r) : $N_a(s)$ contains its core if $\bigcap N_a(s) \in N_a(s)$
(s) : $N_a(s)$ is closed under superset, if $X \in N_a(s)$ and $X \subseteq Y \subseteq S$ implies $Y \in N_a(s)$
(t) : $X \in N_a(s)$ implies $s \in X$

Definition 5. The proof system $D\Delta$ for distributed contingency logic is defined as follows:

TAUT all instances of tautologies

ΔEqu $\Delta_a\phi \leftrightarrow \Delta_a\neg\phi$

$Re\Delta$ $\dfrac{\phi \leftrightarrow \psi}{\Delta_a\phi \leftrightarrow \Delta_a\psi}$

$D1$ $D_a\phi \leftrightarrow \Delta_a\phi$

$D2$ $\Delta_a\phi \rightarrow D_B\phi$ if $a \in B$

$DEqu$ $D_B\phi \leftrightarrow D_B\neg\phi$

$ReD1$ $\dfrac{\phi \leftrightarrow \psi}{D_B\phi \leftrightarrow D_B\psi}$

$ReD2$ $D_C\phi \rightarrow D_B\phi$ if $C \subseteq B$

Theorem 1 (Soundness). *$D\Delta$ is sound with respect to the class of neighborhood models with properties (r) and (s).*

Proof. See B.1. □

Theorem 2 (Completeness). *$D\Delta$ is strongly complete with respect to the class of neighborhood models with properties (r), (s) and (t).*

Proof. See B.2. □

3 Security Properties

A bug is a fault in source code or design of computer program (protocol) that causes it to produce an incorrect or unexpected result. Usually the producer (designer) is *ignorant* about the bug. A hacker is the one who is *aware* of the bug and knows how to use it to perform an attack. Thus, contingency can play a useful role in formalizing security properties and protocols. In this section we demonstrate three interesting security problems.

3.1 Secret Sharing

We began our paper with introducing secret sharing among a group of agents. In Example 2 we formalize a problem in this category.

Example 2. Let $f = x^2 + x + 1$ be a polynomial and $\{a, b, c\}$ be a set of agents. Suppose each agent secretly knows a unique pair of integers. Assume agent a holds (knows) the pair $(1, 3)$, agent b has $(-1, 1)$ and agent c knows $(0, 1)$. All the agents know that there is a main secret $Ax^2 + Bx + C$, that is a polynomial of degree 2 and no one knows it. Let $M = (S, N, V)$ be a neighborhood model where,

- $S = \{(A, B, C) | A, B, C \in \mathbb{Z}\}$,
- $N_a(s) = \{X \subseteq S \mid s \in X \text{ and } \{(A, B, C) \mid A + B + C = 3\} \subseteq X\}$,
- $N_b(s) = \{X \subseteq S \mid s \in X \text{ and } \{(A, B, C) \mid A - B + C = 1\} \subseteq X\}$,
- $N_c(s) = \{X \subseteq S \mid s \in X \text{ and } \{(A, B, C) \mid C = 1\} \subseteq X\}$,
- $V((A, B, C)) = Ax^2 + Bx + C$.

Then for agents $\{a, b\}$ we have

$$N_{\{a,b\}}(s) = \{X \subseteq S \mid s \in X \text{ and } \{(A, B, C) \mid A + B + C = 3 \text{ and } A - B + C = 1\} \subseteq X\} = \{X \subseteq S \mid s \in X \text{ and } \{(A, B, C) \mid A + C = 2\} \subseteq X\}$$

Since for any $X \in N_{\{a,b\}}(1, 1, 1)$ we have $(2, 1, 0) \in X$ and $(1, 1, 1) \in X$ then $M, s \not\models D_{\{a,b\}}(x^2 + x + 1)$. In other words function f is distributed contingent between a and b. By similar reasoning for any proper subset of $\{a, b, c\}$ we can conclude distributed contingent of that group about f.

3.2 Man In The Middle Attack

In the following we are going to relate distributed contingency with "Man in the Middle attack", a popular security protocols [22–24]. Consider the messages passing between Alice to Bob in Table 1. Alice asked for the public key of Bob and he sent his key P_B to Alice. Then she encrypted a message and sent it to Bob, now he can decrypt the message with his private key.

A man in the middle attack can be applied successfully to the above protocol, where Mallory (attacker) intercepts the messages. (Table 2)

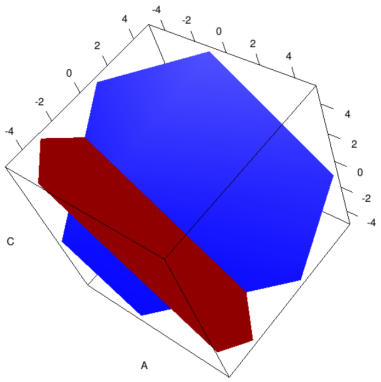

Figure 1. Two planes $A + B + C = 3$ and $A - B + C = 1$.

1 **Alice**	"Hi Bob, it's Alice. Give me your public key"	$->$ **Bob**
2 **Bob**	"P_B (Bob's public key)"	$->$ **Alice**
3 **Alice**	"(Meet me!")$_{P_B}$	$->$ **Bob**

Table 1. A non-secure protocol.

1	**Alice**	"Hi Bob, it's Alice. Give me your public key"	$->$ **Mallory**
1′	**Mallory**	"Hi Bob, it's Alice. Give me your public key"	$->$ **Bob**
2	**Bob**	"P_B (Bob's public key)"	$->$ **Mallory**
2′	**Mallory**	"P_M (Mallory's public key)"	$->$ **Alice**
3	**Alice**	"(Meet me!")$_{P_M}$	$->$ **Mallory**
3′	**Mallory**	"(Meet me!")$_{P_B}$	$->$ **Bob**

Table 2. A Man in the middle attack to a non-secure protocol.

In this attack Mallory plays the role of Bob (Alice) when she talks to Alice (Bob). In (2′) she replace Bob's public key with her own key and sent it to Alice. Therefore she can decrypt (3) and again encrypt it with Bob's public key in (3′).

Let p be "Mallory intercepted the messages". The neighborhood model for this attack is $M = (S, N, V)$ where,

- $S = \{0, 1\}$,
- $N_a(0) = N_b(0) = N_a(1) = N_b(1) = \{S\}$,
- $V(0) = \neg p$ and $V(1) = p$.

Then $M, 1 \models \neg D_{\{a,b\}}p$, and after the attack Alice and Bob has *distributed contingent* that Mallory intercepted their sequence of message. A man in the middle attack can be successful if after its execution the two parties have distributed contingent about the attack.

3.3 Revealing A Secret To Hide Another One

In epistemic logic [8, 25], the *principle of full communication* states, A set of formulas Φ entails a formula ϕ, $\Phi \vdash \phi$, if and only if every pointed model that satisfies all formula in Φ also satisfies ϕ. Let

$$\Delta S(M, s) = \{\psi \mid M, s \models (\psi \wedge \Delta_a \psi) \text{ for some } a \in A\}$$

be the non-contingency set (knowledge set) in (M, s). The principle of full communication is formalized as follows,

$$M, s \models (\phi \wedge D_B \phi) \Rightarrow \Delta S(M, s) \vdash \phi$$

Intuitively, the principle states "if a secret is distributed, then it follows from the knowledge of all individual agents put together. The principle is not always accurate [9, 26, 27]. There exists models where $M, s \models (\phi \wedge D_B \phi)$, but $\Delta S(M, s) \not\vdash \phi$.

Consider a neighborhood model, $M = (S, N, V)$ where, $S = \{w, x, y, z, v\}$, $V(w) = V(z) = \{p, q\}$, $V(x) = V(y) = \{q\}$ and the neighborhood set for agents a and b and all the states is,

- $N_a(w) = N_a(x) = \{X \subseteq S \mid \{x, w\} \subseteq X\}$,
- $N_b(w) = N_b(y) = \{X \subseteq S \mid \{y, w\} \subseteq X\}$,
- $N_a(y) = N_a(z) = \{X \subseteq S \mid \{z, y\} \subseteq X\}$,
- $N_b(x) = N_b(z) = N_b(v) = \{X \subseteq S \mid \{x, z, v\} \subseteq X\}$,
- $N_a(v) = \{X \subseteq S \mid \{v\} \subseteq X\}$,

Let w be the real world. In state (M, w) the secret p holds and is distributed non-contingent in group $\{a, b\}$. The principle of full communication is true in (M, w).

By semantics, $M, w \models D_{\{a,b\}}p$ since $c_a(w) \cap c_b(w) = \{w\}$ and $N_{\{a,b\}}(w) = \{X \mid w \in X\}$, which means $p^M = \{w, z\} \in N_{\{a,b\}}(w)$. It is also clear that $M, w \models p$. Thus $M, w \models (p \wedge D_{\{a,b\}}p)$. This means the left part of the principle holds.

For the right part,

1 $M, w \models (\Delta_b q \wedge q) \rightarrow p$ because $M, w \models p$.
2 $M, w \models \Delta_a((\Delta_b q \wedge q) \rightarrow p)$ because $((\Delta_b q \wedge q) \rightarrow p)^M = \{w, x, z\} \in N_a(w)$ [1].

From 1 and 2 we conclude,

$$M, w \models \Delta_a((\Delta_b q \wedge q) \rightarrow p) \wedge (\Delta_b q \wedge q) \rightarrow p \ (*)$$

Moreover,

3 $(\Delta_b q \wedge q)^M = \{w, y\} \in N_b(w)$ which means $M, w \models \Delta_b(\Delta_b q \wedge q) \wedge \Delta_b q \wedge q$.
4 Since $q \in V(w)$, $M, w \models q$

[1] In world w and z secret p holds. In world x the formula $\Delta_b q$ does not holds.

5 $M, w \models \Delta_b q$ because $q^M = \{w, x, y, z\} \in N_b(w)$.

From items 3,4 and 5 we conclude

$$M, w \models \Delta_b(\Delta_b q \wedge q) \wedge \Delta_b q \wedge q \ (**)$$

Now from $(*)$ and $(**)$ and definition of $\Delta S(M, w)$ we have $(\Delta_b q \wedge q) \in \Delta S(M, w)$ and $((\Delta_b q \wedge q) \to p) \in \Delta S(M, w)$. Thus, $\Delta S(M, w) \vdash p$. Therefore the principle of full communication holds in this models.

The attractive part happens when someone reveal the secret q to public. Suppose someone *publicly announce* q, then the updated model $M' = (S', N', V')$ is the previous structure, M, only limited to worlds $S' = \{w, x, y, z\}$ [2]. Thus, $V'(w) = V'(z) = \{p, q\}$, $V'(x) = V'(y) = \{q\}$ and,

- $N'_a(w) = N'_a(x) = \{X \subseteq S' \mid \{x, w\} \subseteq X\}$,
- $N'_b(w) = N'_b(y) = \{X \subseteq S' \mid \{y, w\} \subseteq X\}$,
- $N'_a(y) = N'_a(z) = \{X \subseteq S' \mid \{z, y\} \subseteq X\}$,
- $N'_b(x) = N'_b(z) = \{X \subseteq S' \mid \{x, z\} \subseteq X\}$,

We claim that if the agents a and b talk to each other and share their knowledge, they can not access to p.

More formally, $\Delta S(M, w) \nvdash p$.

i For every ϕ, $M, w \models \phi$ iff $M, z \models \phi$ and $M, x \models \phi$ iff $M, y \models \phi$. (The proof is straight forward by induction on the length of ϕ.)

ii Let $\phi \in \Delta S(M, w)$, then for some $c \in \{a, b\}$, $M, w \models \Delta_c \phi \wedge \phi$. If c is a then since $N_a(w) = N_a(x)$ we have $M, x \models \Delta_a \phi$, and similarly if c is b then $M, y \models \Delta_b \phi$. This means $\Delta S(M, w) \subseteq \Delta S(M, x) \cup \Delta S(M, y)$.

iii For every ϕ, $M, x \models \phi \wedge \Delta_a \phi$ iff $M, x \models \phi \wedge \Delta_b \phi$. (By part (i) and induction on the length of ϕ.)

By (i), we have $\Delta S(M, w) = \Delta S(M, z)$ and $\Delta S(M, x) = \Delta S(M, y)$, so by part (ii) we conclude that $\Delta S(M, w) = \Delta S(M, x)$. By part (iii) we have

$$\{\psi \mid M, x \models (\psi \wedge \Delta_a \psi)\} = \{\psi \mid M, x \models (\psi \wedge \Delta_b \psi)\}$$

Therefore,

$$\Delta S(M, w) = \Delta S(M, x) = \{\psi \mid M, x \models (\psi \wedge \Delta_a \psi)\}$$

Finally since $M, x \not\models p$, we conclude,

$$\Delta S(M, w) \nvdash p$$

Hence revealing secret q to public remove access to secret p forever.

4 Expressiveness

In this section we deal with expressivity of logic $D\Delta$. We will show that our logic is more expressive than contingency logic. In order to do that we first translate neighborhood models to Kripke models, then we present two bisimilar Kripke model, and show that they can be distinguished by distributed contingency logic but not by contingency logic. We will use some results from [14]. The following is the usual definition for expressivity of logical languages.

Definition 6 (Expressivity). Let L_1 and L_2 be two logical languages that are interpreted in the same class of models $\mathcal{M}$. Then,

- L_2 is at least as expressive as L_1, notation $L_1 \preceq L_2$ if for every formula $\phi_1 \in L_1$ there is an equivalent formula $\phi_2 \in L_2$ over $\mathcal{M}$,
- L_1 and L_2 are equally expressive, notation $L_1 \equiv L_2$, if $L_1 \preceq L_2$ and $L_2 \preceq L_1$,
- L_1 is less expressive than L_2, notation $L_1 \prec L_2$ if $L_1 \preceq L_2$ and $L_2 \not\preceq L_1$.

Let ML be the language of modal logic:

$$\text{If } \phi, \psi \in L_{ML} \text{ then } \neg\phi,\ \phi \wedge \psi,\ \Box_a \phi \in L_{DC}$$

where $\Box_a \phi$ is read as "it is necessary that ϕ". The proof system of modal logic, ML, consist of TAUT, K and M, where

$$K := \Box_a(\phi \to \psi) \to (\Box_a \phi \to \Box_a \psi)$$

$$M := \Box_a \phi \to \phi$$

Also let CL be the language of contingency logic:

$$\text{If } \phi, \psi \in L_{ML} \text{ then } \neg\phi,\ \phi \wedge \psi,\ \Delta_a \phi \in L_{DC}$$

where TAUT, ΔEqu and $Re\Delta$ form the proof system for contingency logic.

In [14] they study expressivity of CL and ML in neighborhood models with different kind of properties and they reach to the following result.

Proposition 1. *CL and ML are equally expressive on the class of neighborhood models satisfying (t)*

Proof. See [14] Prop 5. □

A neighborhood model is called augmented if it satisfies properties (r) and (s). The following theorem presents a 1-1 correspondence between neighborhood and Kripke models [3] for contingency logic CL.

Theorem 3.

- *For every Kripke model $M^K = (S, R, V)$ there exists an augmented neighborhood model $M^N =$*

[2] Secret q does not hold in world v so after announcement we should remove v.

[3] A Kripke model is a triple $M = (S, R, V)$ where S is a nonempty set of possible worlds, $R = \{R_a \mid a \in A\}$ is a set of accessibility relations such that $R_a \subseteq S \times S$, and V is a valuation function.

(S, N, V) *such that for all* $s \in S$ *and all formula* $\phi \in CL$, $M^K, s \models \phi$ *iff* $M^N, s \models \phi$

- *For every augmented neighborhood model* $M^N = (S, N, V)$ *there exists a Kripke model* $M^K = (S, R, V)$ *such that for all* $s \in S$ *and all formula* $\phi \in CL$, $M^K, s \models \phi$ *iff* $M^N, s \models \phi$

Proof. See [14] Prop 9. and Prop 10. □

At this state we are ready to prove Distributed contingency logic is more expressive than contingency logic.

Theorem 4. $CL \prec D\Delta$

Proof. See B.3. □

Acknowledgements

We thank the reviewers of the journal ISeCure for their comments. The authors would like to thank Professor Mohammad Ardeshir for his supports and comments on the paper. Rahim Ramezanian conducted this research as a Ph.D. student at Sharif University of Technology under the supervision of Mohammad Ardeshir.

References

[1] CJF Cremers, S Mauw, and EP De Vink. Formal methods for security protocols: Three examples of the black-box approach. *NVTI newsletter*, 7:21–32, 2003.

[2] Jim Woodcock, Peter Gorm Larsen, Juan Bicarregui, and John Fitzgerald. Formal methods: Practice and experience. *ACM computing surveys (CSUR)*, 41(4):19, 2009.

[3] Susan Older and Shiu-Kai Chin. Formal methods for assuring security of protocols. *The Computer Journal*, 45(1):46–54, 2002.

[4] Moni Naor and Adi Shamir. Visual cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 1–12. Springer, 1994.

[5] Douglas R Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2(4):357–390, 1992.

[6] Samaneh Mashhadi. Computationally secure multiple secret sharing: models, schemes, and formal security analysis. *The ISC International Journal of Information Security*, 7(2):91–99, 2015.

[7] J-J Ch Meyer and Wiebe Van Der Hoek. *Epistemic logic for AI and computer science*, volume 41. Cambridge University Press, 2004.

[8] Ronald Fagin, Joseph Y Halpern, Yoram Moses, and Moshe Vardi. *Reasoning about knowledge*. MIT press, 2004.

[9] Floris Roelofsen. Distributed knowledge. *Journal of Applied Non-Classical Logics*, 17(2):255–273, 2007.

[10] Jelle Gerbrandy. Distributed knowledge. In *Twendial*, volume 98, pages 111–124, 1998.

[11] IL Humberstone et al. The logic of non-contingency. *Notre Dame Journal of Formal Logic*, 36(2):214–229, 1995.

[12] Steven T Kuhn et al. Minimal non-contingency logic. *Notre Dame Journal of Formal Logic*, 36(2):230–234, 1995.

[13] Jie Fan, Yanjing Wang, and Hans van Ditmarsch. Contingency and knowing whether. *The Review of Symbolic Logic*, 8(01):75–107, 2015.

[14] Jie Fan and Hans Van Ditmarsch. Neighborhood contingency logic. In *Indian Conference on Logic and Its Applications*, pages 88–99. Springer, 2015.

[15] Christopher Steinsvold. A note on logics of ignorance and borders. *Notre Dame Journal of Formal Logic*, 49(4):385–392, 2008.

[16] Wiebe Van Der Hoek and Alessio Lomuscio. A logic for ignorance. In *Declarative Agent Languages and Technologies*, pages 97–108. Springer, 2004.

[17] Jelle Douwe Gerbrandy et al. *Bisimulations on planet Kripke*. ILLC Dissertation Series, 1999.

[18] Jie Fan. Removing your ignorance by announcing group ignorance: A group announcement logic for ignorance. *Stud. Log*, 9(4):4–33, 2016.

[19] Jie Fan. Distributed knowledge whether. *International Workshop on Logic, Rationality and Interaction*, 10455, 2017.

[20] Catherine Meadows. Formal methods for cryptographic protocol analysis: Emerging issues and trends. *IEEE journal on selected areas in communications*, 21(1):44–54, 2003.

[21] Seyit Ahmet Camtepe and Bülent Yener. A formal method for attack modeling and detection. *SA Camtepe, B. Yener*, 2006.

[22] Nadarajah Asokan, Valtteri Niemi, and Kaisa Nyberg. Man-in-the-middle in tunnelled authentication protocols. In *security protocols workshop*, volume 3364, pages 28–41. Springer, 2003.

[23] Zhe Chen, Shize Guo, Rong Duan, and Sheng Wang. Security analysis on mutual authentication against man-in-the-middle attack. In *Information Science and Engineering (ICISE), 2009 1st International Conference on*, pages 1855–1858. IEEE, 2009.

[24] Ratan K Guha, Zeeshan Furqan, and Shahabuddin Muhammad. Discovering man-in-the-middle attacks in authentication protocols. In *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1–7. Ieee, 2007.

[25] Hans Van Ditmarsch, Wiebe van Der Hoek, and Barteld Kooi. *Dynamic epistemic logic*, volume

337. Springer Science & Business Media, 2007.
[26] Wiebe Van Der Hoek, Bernd Van Linder, and John-Jules Meyer. Group knowledge is not always distributed (neither is it always implicit). *Mathematical social sciences*, 38(2):215–240, 1999.
[27] Rahim Ramezanian. *Classification of action models which preserve full communication, Master thesis*. Shahid Beheshti University, 2010. Persian.
[28] Patrick Blackburn, Maarten De Rijke, and Yde Venema. *Modal Logic: Graph. Darst*, volume 53. Cambridge University Press, 2002.
[29] Sandra M Hedetniemi, Stephen T Hedetniemi, and Arthur L Liestman. A survey of gossiping and broadcasting in communication networks. *Networks*, 18(4):319–349, 1988.
[30] Hans van Ditmarsch, Jan van Eijck, Pere Pardo, Rahim Ramezanian, and François Schwarzentruber. Epistemic protocols for dynamic gossip. *Journal of Applied Logic*, 20:1–31, 2017.
[31] Hans van Ditmarsch, Jan van Eijck, Pere Pardo, Rahim Ramezanian, and François Schwarzentruber. Dynamic gossip. *arXiv preprint arXiv:1511.00867*, 2015.
[32] Maduka Attamah, Hans Van Ditmarsch, Davide Grossi, and Wiebe van der Hoek. Knowledge and gossip. In *ECAI*, pages 21–26, 2014.
[33] Walter Knödel. New gossips and telephones. *Discrete Mathematics*, 13(1):95, 1975.

Rahim Ramezanian was born in Mashhad, Iran in 1985. He received his B.S. in 2007 from Ferdowsi University of Mashhad and M.S. degree in mathematics in 2010 from Shahdi Beheshti University of Tehran. Since 2011 he is a Ph.D. student at the department of Mathematical Sciences at Sharif University of Technology. His research interests are application of logics (epistemic logic, temporal logic, process algebra) in security and social networks.

Appendix A Backgrounds

A.1 Contingency Logic

Contingency [11–14] is an important notion in philosophical and epistemic logic. In the literature it also has appeared with other names, *ignorance*[15, 16] and *knowing whether* [13]. A formula ϕ is contingent if it is possibly true and possibly false, in other words the agent is ignorant about ϕ.

A formula ϕ is non-contingent if it is necessarily true or necessarily false, it means the agent knows whether ϕ. If $\Box\phi$ is necessarily ϕ then non-contingency of ϕ, denoted by $\Delta\phi$, is defined by $\Delta\phi := \Box\phi \vee \Box\neg\phi$.

If we omit the distributed contingency operator from definitions 1 and 3 we will have language and semantics definitions of contingency logic. Two interesting axioms of contingency logic are ΔEqu and $Re\Delta$ (see Def. 5) where respectively state that,

- If we know whether ϕ then we also know whether $\neg\phi$
- If ϕ is equivalent to ψ then we are non contingent about ϕ if and only if we are non contingent about ψ.

A.2 Kripke Semantics

A Kripke model [28] is a triple (S, R, V), where,

- S is a nonempty sets of worlds,
- R is a function, assigning to each agent $a \in A$ an accessibility relation $R_a \subseteq S \times S$,
- V is a valuation function,

A relation sR_at for $a \in A$ and $s, t \in S$ intuitively means agent a can not distinguish two possible worlds s and t. The satisfaction relation between a formula ϕ in L_{DC} and a pointed model (M, s), is inductively defined as follows,

$$
\begin{aligned}
M, s &\models \top && \text{iff true}\\
M, s &\models p && \text{iff } s \in V(p)\\
M, s &\models \neg\phi && \text{iff } M, s \not\models \phi\\
M, s &\models \phi \wedge \psi && \text{iff } M, s \models \phi \text{ and } M, s \models \psi\\
M, s &\models \Delta_a\phi && \text{iff } \forall t \in S\ sR_at \Rightarrow M, t \models \phi \text{ or}\\
& && \quad \forall t \in S\ sR_at \Rightarrow M, t \models \neg\phi\\
M, s &\models D_B\phi && \text{iff } \forall t \in \textstyle\bigcap_{a\in A} R_a(s)\ M, t \models \phi \text{ or}\\
& && \quad \forall t \in \textstyle\bigcap_{a\in A} R_a(s)\ M, t \models \neg\phi
\end{aligned}
$$

A.3 Gossip Protocols

A gossip protocol [29–33] is a procedure for spreading secrets among a group of agents using a connection graph. In each call between a pair of connected agents, they share all the secrets they have learned. In gossip problem main secret, the collection of all individual secrets is *distributed knowledge* between agents.

Initially, it seems the main secret can be learned by all agents after execution of the protocol, however, the problem depends on other variables such as connectivity of graph and expressiveness of protocol.

The main secret cannot be learn [4] by agents if the graph is disconnected. In a problem where the graph is a tree with more than 2 nodes and the protocol is LNS [5] the main secret is non-learnable too.

Appendix B Proofs

B.1 Proof of Theorem 1: (Soundness)

Proof.

- (ΔEqu) $M, s \models \Delta_a\phi$ iff, $\phi^M \in N_a(s)$ or $(\neg\phi)^M \in N_a(s)$, iff $M, s \models \Delta_a\neg\phi$.
- $(Re\Delta)$ Suppose $\models \phi \leftrightarrow \psi$, then $M, s \models \Delta_a\phi$ iff $\phi^M \in N_a(s)$ or $(\neg\phi)^M \in N_a(s)$ iff $\psi^M \in N_a(s)$ or $(\neg\psi)^M \in N_a(s)$ iff $M, s \models \Delta_a\psi$.
- $(D1)$ By properties (r) and (s) it is easy to show $N_{\{a\}}(s) = N_a(s)$. Hence the claim holds.
- $(D2)$ Suppose $M, s \models \Delta_a\phi$, so $\phi^M \in N_a(s)$ or $(\neg\phi)^M \in N_a(s)$. By property (r), $c_a(s) \subseteq \phi^M$ or $c_a(s) \subseteq (\neg\phi)^M$. Therefore $\phi^M \in N_B(s)$ or $(\neg\phi)^M \in N_B(s)$.
- $(DEqu)$ $M, s \models D_B\phi$ iff, $\phi^M \in N_B(s)$ or $(\neg\phi)^M \in N_B(s)$, iff $M, s \models D_B\neg\phi$.
- $(ReD1)$ Suppose $\models \phi \leftrightarrow \psi$, then $M, s \models D_B\phi$ iff $\phi^M \in N_B(s)$ or $(\neg\phi)^M \in N_B(s)$ iff $\psi^M \in N_B(s)$ or $(\neg\psi)^M \in N_B(s)$ iff $M, s \models D_B\psi$.
- $(ReD2)$ Since $C \subseteq B$, by Def. 3 we have $N_C(s) \subseteq N_B(s)$ $(*)$. If $M, s \models D_C\phi$ then $\phi^M \in N_C(s)$ or $(\neg\phi)^M \in N_C(s)$. By $(*)$ $\phi^M \in N_B(s)$ or $(\neg\phi)^M \in N_B(s)$. Thus, $M, s \models D_B\phi$.

□

B.2 Stages for Proof of Theorem 2: (Completeness)

The canonical neighborhood model of $D\Delta$ is the triple $M^c = (S^c, N^c, V^c)$ where

- S^c is the set of all maximal consistent sets,
- $N^c_a(s) = \{|\phi|| \ \Delta_a\phi \in s\}$,
- $V^c(p) = \{s \mid s \in |p|\}$,

and $|\phi| = \{s \in S^c \mid \phi \in s\}$.

Lemma 1 (Truth)**.** *For any $s \in S^c$ and formula ϕ $M^c, s \models \phi$ if and only if $\phi \in s$.*

Proof. By induction on ϕ. The base case and boolean cases are trivial.

- Case $\Delta_a\phi$.

$M^c, s \models \Delta_a\phi \Leftrightarrow_{\text{semantics}}$
$\phi^{M^c} \in N^c_a(s)$ or $(\neg\phi)^{M^c} \in N^c_a(s) \Leftrightarrow_{\text{IH}}$
$|\phi| \in N^c_a(s)$ or $|\neg\phi| \in N^c_a(s) \Leftrightarrow_{\text{Def. } N^c}$
$\Delta_a\phi \in s$ or $\Delta_a\neg\phi \in s \Leftrightarrow_{\Delta Equ}$
$\Delta_a\phi \in s$

- Case $D_B\phi$.

$M^c, s \models D_B\phi \Leftrightarrow_{\text{semantics}}$
$\phi^{M^c} \in N^c_B(s)$ or $(\neg\phi)^{M^c} \in N^c_B(s) \Leftrightarrow_{\text{Def. } N_B}$
for all $a \in B$ $\phi^{M^c} \in N^c_a(s)$ or
for all $a \in B$ $(\neg\phi)^{M^c} \in N^c_a(s) \Longleftrightarrow_{\text{IH}}$
for all $a \in B$ $|\phi| \in N^c_a(s)$ or
for all $a \in B$ $|\neg\phi| \in N^c_a(s) \Longleftrightarrow_{\text{Def. } N^c}$
for all $a \in B$ $\Delta_a\phi \in s$ or
for all $a \in B$ $\Delta_a\neg\phi \in s \Longleftrightarrow_{\Delta Equ}$
for all $a \in B$ $\Delta_a\phi \in s \Longleftrightarrow_{D2}$
$D_B\phi \in s$

□

The following lemma prove that N^c is well defined. (See [14] Lemma 2).

Lemma 2. *If $|\phi| \in N^c_a(s)$ and $|\phi| = |\psi|$ then $\Delta_a\psi \in s$.*

Theorem 5 (Completeness)**.** *$D\Delta$ is strongly complete with respect to the class of neighborhood models with properties (r), (s) and (t).*

Proof. Suppose $\Gamma \nvdash \phi$, then $\Gamma \cup \{\neg\phi\}$ is consistent. By Lindenbaum's Lemma, there exists $s \in S^c$ such that $\Gamma \cup \{\neg\phi\} \subseteq s$. By Truth Lemma $\Gamma \not\models \phi$. □

B.3 Proof of Theorem 4

Proof. Let M (up) and M' (down) be the Kripke models in Fig.2.

It is easy to see that M and M' are bisimilar with relation $Z = \{(s, s'), (t, t'), (t, v'), (u, u')\}$ From theorem 2.20 in [28] we induce that ML can not distinguish M from M'. By Thm.3:

- $M_n = (S, N, V)$ is neighborhood model corresponds to M where $S = \{s, t, u\}$, $V(p) = \{s, u\}$ and
  - $N_a(s) = N_b(s) = \{\{s, t, u\}\}$.
  - $N_a(t) = N_b(t) = \{X \mid \{t\} \subseteq X \subseteq S\}$.
  - $N_a(u) = N_b(u) = \{X \mid \{u\} \subseteq X \subseteq S\}$.
- $M'_n = (S', N', V')$ is neighborhood model corresponds to M' where $S' = \{s', t', u', v'\}$, $V'(p) = \{s', u'\}$ and
  - $N'_a(s') = \{\{s', t', u'\}, \{s', t', u', v'\}\}$.
  - $N'_b(s') = \{\{s', v', u'\}, \{s', t', u', v'\}\}$.
  - $N'_a(t') = N'_b(t') = \{X \mid \{t'\} \subseteq X \subseteq S'\}$.
  - $N'_a(u') = N'_b(u') = \{X \mid \{u'\} \subseteq X \subseteq S'\}$.
  - $N'_a(v') = N'_b(v') = \{X \mid \{v'\} \subseteq X \subseteq S'\}$.

[4] Note that the idea of defining distributed contingency is formalizing non-learnable facts.
[5] Learn New Secret: x will call y if x does not know the secret of y

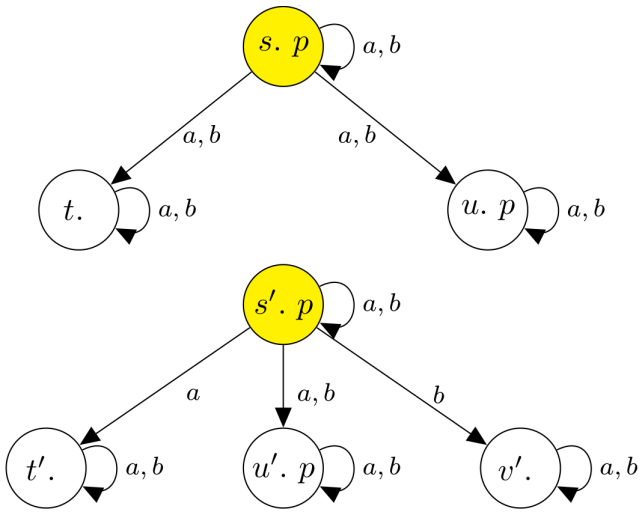

Figure 2. Two bisimilar Kripke models M (up) and M' (down).

By Prop.1 M_n and M'_n indistinguishable for contingency logic CL. We claim that $M_n, s \models \neg D_{\{a,b\}}p$ but $M'_n, s' \not\models \neg D_{\{a,b\}}p$

- Since $N_a(s) = N_b(s)$ we have $N_{\{a,b\}}(s) = N_a(s) = \{S\}$. Hence $p^{M_n} \notin N_{\{a,b\}}(s)$ and $(\neg p)^{M_n} \notin N_{\{a,b\}}(s)$. Thus, $M_n, s \models \neg D_{\{a,b\}}p$.
- $N'_{\{a,b\}}(s') = \{X \mid \{s', u'\} \subseteq X \subseteq S'\}$. Hence $p^{M'_n} \in N'_{\{a,b\}}(s)$ and , $M'_n, s' \not\models \neg D_{\{a,b\}}p$.

□