Annals of Pure and Applied Logic 165 (2014) 253–265

Contents lists available at SciVerse ScienceDirect

Annals of Pure and Applied Logic

www.elsevier.com/locate/apal

Symmetry in information flow

Jeffrey Kane, Pavel Naumov *

Department of Mathematics and Computer Science, McDaniel College, Westminster, MD, USA

ARTICLE INFO

Article history:
Available online 19 August 2013

MSC:
03B42
03B70
20A15
03B60

Keywords:
Information flow
Symmetry
Axiomatization
Completeness

ABSTRACT

The article investigates information flow properties of symmetric multi-party protocols. It gives a sound and complete axiomatic system for properties of the functional dependence predicate that are common to all protocols with the same group of symmetries.

1. Introduction

1.1. Symmetric protocols

In this article we study properties of information flow under symmetric protocols. An example of such a protocol is the parity encryption protocol illustrated in Fig. 1. Under this protocol, party p sends a binary message a to a party q. Then q encodes it into b using random encryption key c in such a way that $a \equiv b+c \pmod 2$. It sends both the encrypted message b and the key c to party r. Party r decrypts message using formula $d \equiv b + c \pmod 2$ and sends the result to party s. This protocol is symmetric in the sense that if $a = x$, $b = y$, $c = z$, $d = t$ is a valid set of values under this protocol, then so is $a = x$, $b = z$, $c = y$, $d = t$. We will formally express it by saying that permutation

$$\sigma = \begin{pmatrix} a & b & c & d \\ a & c & b & d \end{pmatrix}$$

is a symmetry of the protocol. We will also use a graphical way to describe symmetry σ as shown in Fig. 2.

* Corresponding author.
E-mail addresses: jmk001@mcdaniel.edu (J. Kane), pnaumov@mcdaniel.edu (P. Naumov).

0168-0072/$ – see front matter
http://dx.doi.org/10.1016/j.apal.2013.07.013

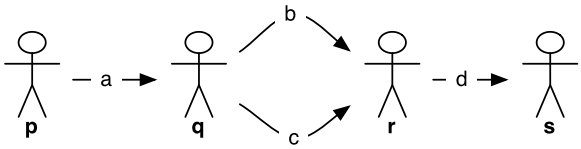

Fig. 1. Parity Protocol.

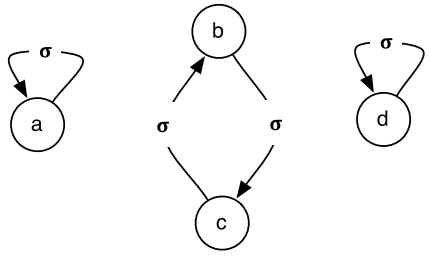

Fig. 2. Symmetry σ of the Parity Protocol.

Another example of a symmetric protocol is an anonymous vote protocol. If a, b, and c represent votes of three different parties and m the majority vote, then if $a = x$, $b = y$, $c = z$, $m = t$ is a valid set of values, then so is $a = y$, $b = z$, $c = y$, $m = t$ or any other permutation of these values that preserves m. Using the language of abstract algebra, symmetries of this protocol are all permutations in the *stabilizer subgroup* of the element m.

In general, we specify symmetries of an information flow protocol by giving a group of permutations under which the protocol is invariant in the described above sense. The formal definition will be given in Section 3 below. Properties of symmetry in information [13] and especially in applications to model checking [7] have been studied before.

1.2. Functional dependence

The properties of information flow protocols between different pieces of information, from now on referred to as secrets, can be studied in different languages. The language is specified by the choice of the predicate(s) it is using. A natural example of such predicate that we will be using in this article is *functional dependence*, which we denote by $a \rhd b$. It means that the value of secret a reveals the value of secret b. A more general form of functional dependence is functional dependence between sets of secrets. If A and B are two sets of secrets, then $A \rhd B$ means that, together, the values of all secrets in A reveal the values of all secrets in B. Armstrong [1] presented the following sound and complete axiomatization of this relation:

1. *Reflexivity*: $A \rhd B$, if $A \supseteq B$,
2. *Augmentation*: $A \rhd B \to A \cup C \rhd B \cup C$,
3. *Transitivity*: $A \rhd B \to (B \rhd C \to A \rhd C)$.

The above axioms are known in database literature as Armstrong's axioms [4, p. 81]. Beeri, Fagin, and Howard [2] suggested a variation of Armstrong's axioms that describe properties of multi-valued dependence. Naumov and Nicholls axiomatized a related relation of rationally functional dependence in strategic games [14].

Another natural relation between secrets is the "nondeducibility" predicate introduced by Sutherland [15]. Halpern and O'Neill [5] proposed a closely-related notion called f-secrecy. More and Naumov [10] studied this relation between sets of secrets. A logical system that combines independence and functional dependence predicates was described by Kelvey, More, Naumov, and Sapp [6]. The relation on secrets, "secret a knows at