Discrete Applied Mathematics 198 (2016) 118–135

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Secure aggregation of distributed information: How a team of agents can safely share secrets in front of a spy

David Fernández-Duque [a,*], Valentin Goranko [b,c]

[a] Department of Mathematics, Instituto Tecnológico Autónomo de México, Río Hondo 1, 01080 Mexico City, Mexico

[b] Department of Philosophy, Stockholm University, SE - 10691 Stockholm, Sweden

[c] Department of Mathematics, University of Johannesburg, South Africa[1]

ARTICLE INFO

Article history:
Received 29 July 2014
Received in revised form 5 June 2015
Accepted 21 June 2015
Available online 13 July 2015

Keywords:
Multi-agent systems
Secure information exchange
Safe and informative protocols
Generalized Russian cards problems

ABSTRACT

We consider the generic problem of Secure Aggregation of Distributed Information (SADI), where several agents acting as a team have information distributed amongst them, modelled by means of a publicly known deck of cards distributed amongst the agents, so that each of them knows only her cards. The agents have to exchange and aggregate the information about how the cards are distributed amongst them by means of public announcements over insecure communication channels, intercepted by an adversary "eavesdropper", in such a way that the adversary does not learn who holds any of the cards. We present a combinatorial construction of protocols that provides a direct solution of a class of SADI problems and develop a technique of iterated reduction of SADI problems to smaller ones which are eventually solvable directly. We show that our methods provide a solution to a large class of SADI problems, including all SADI problems with sufficiently large size and sufficiently balanced card distributions.

1. Introduction

We consider a generic scenario where a set of agents Agt have information distributed amongst them, i.e., included in their collective knowledge, while each agent has only partial knowledge of it. The agents act as a team that has to exchange and aggregate that information, either as common knowledge within their group or in the individual knowledge of at least one of them. The exchange is performed over insecure communication channels and is presumed intercepted by an adversary. The task of the team is to achieve the aggregation of the distributed information, following a prearranged protocol, in such a way that the adversary does not learn important information.

More specifically, we model the problem by assuming that the information that each agent has is encoded by a set of "cards" that she[2] holds in her hands, where the cards are drawn from a publicly known deck[3] and every card is in the hands of exactly one agent of the team. The deck of cards should be seen merely as a metaphor for the information held by each agent, an idea that has proven useful for modelling secure computations in several settings unrelated to our own [7–9]. The

* Corresponding author.
E-mail addresses: david.fernandez@itam.mx (D. Fernández-Duque), valentin.goranko@philosophy.su.se (V. Goranko).

1 Visiting professor.

2 For convenience of exposition, we will assume that the agents are female while the eavesdropper is male.

3 The drawing and distribution of these cards is considered secret and secure and we will not discuss the side issue of how exactly that is done. In reality, we assume that each of the agents has obtained her initial information in some private way.

http://dx.doi.org/10.1016/j.dam.2015.06.022
0166-218X/

goal of the team is to exchange and disseminate across the whole team the information about how the cards are distributed among the agents. It is assumed that the agents can only communicate by making public announcements over insecure channels and that there is an "eavesdropper" Eaves ($\mathcal{E}$) whose goal is to learn as much as possible about the distribution of the cards by intercepting and analysing the announcements exchanged by the agents in Agt. In particular, Eaves wants to learn who owns at least one of the cards. We further assume that in their exchange of announcements the agents follow a publicly known (hence, known by the eavesdropper, too) protocol.

The scenario described above is a variation of the well-known "Russian cards problem", which is more than one-and-a-half centuries old [5] but has recently had renewed attention [12], leading to many new solutions (e.g. [1,2,10,11]). Here we will generalize the problem substantially by allowing an arbitrary number of agents, but on the other hand we restrict it essentially by assuming that the eavesdropper has no cards in his hands.[4] According to our knowledge, such a multi-agent setup had only previously been considered in [4], although our approach is very different. Interest in this problem arises from the fact that it is based on *information-theoretic cryptography* [6], where security is not contingent on the computational complexity of breaking the code but rather on communications that do not contain sufficient information for an eavesdropper to learn the original message.

Main results and contributions

In this paper, we introduce the generic *Secure Aggregation of Distributed Information (SADI)* problem and model it in the style of the Russian cards problem. We introduce a formal framework for specifying SADI problems involving any number of communicating agents and leading to several notions of security and informativity. We then focus on a version of SADI problems with natural safety and informativity conditions, for which we present a combinatorial construction of protocols that provides a direct solution of a class of SADI problems and then develop a general technique for solving the problem by reducing it recursively to smaller instances. Finally, we show how this method can be used to solve a wide class of SADI problems, including all SADI problems with sufficiently large size and sufficiently balanced card distribution.

Our results and methods may eventually be used for developing practical protocols for secure communication, which we briefly suggest in the concluding section.

Organization of the paper

We motivate the current work in Section 2 by presenting a detailed example which showcases some of the notions that will arise throughout the text. Section 3 then provides the general setup of the Secure Aggregation of Distributed Information (SADI) problem. In Section 4 we focus on solving the SADIproblem in the 3-agent case, and in Section 5 we set the stage for working with more agents. Section 6 describes a general technique by reduction to smaller cases, which is then employed in Section 7 to prove that a large class of instances of the SADI problem are solvable. In a brief concluding section we suggest further extensions of our techniques and some applications. Then, we include in an appendix some more technical proofs consisting of algebraic manipulations.

2. An illustrative example

Before we present the generic setup and embark on a general analysis of the multi-agent setting, we begin with a non-trivial illustrative example of the type of problems we consider in the paper. It involves a team of three agents,[5] Alice ($\mathcal{A}$), Bob ($\mathcal{B}$) and Cath ($\mathcal{C}$) who hold respectively 2, 3 and 4 cards, identified with the numbers $1, \ldots, 9$.

We are interested in designing a protocol that would eventually inform each of the agents about the deal, while the eavesdropper Eaves ($\mathcal{E}$) may not learn the ownership of any of the cards.

We will describe informally a protocol solving this problem, by describing it on a (randomly chosen) particular deal in which we assume, without loss of generality, that Alice gets $\{1, 2\}$, Bob gets $\{3, 4, 5\}$, and Cath gets the remaining cards $\{6, 7, 8, 9\}$. We will use the notation $H_{\mathcal{A}} \mid H_{\mathcal{B}} \mid H_{\mathcal{C}}$ to represent the deal and may omit set-brackets, so that the deal may also be written as $1, 2 \mid 3, 4, 5 \mid 6, 7, 8, 9$.

Step 1. Alice chooses at random a card not in her hand, say 9. Then she makes an announcement, saying (essentially):

> *"My cards are among* $\{1, 2, 9\}$".

After such announcement, the agent who holds the extra card (9) – in this case Cath – knows the card distribution.

Step 2. That agent (Cath) makes the next announcement, which has to inform the others of the distribution, as follows. There are three possible ways that the cards 1, 2, 9 may be distributed among Alice and Cath: $1, 2 \mid 9$, $2, 9 \mid 1$ or $1, 9 \mid 2$.

[4] The effect of allocating cards to the eavesdropper is deeper than just the fact that not all cards are in the hands of the team. It also creates the danger that the announcements of the agents in the team about cards they do not hold may reveal unwanted information to the eavesdropper. So, the solution protocols developed here would generally not work in the case where the eavesdropper holds cards, and we leave that case for future work.

[5] Note that the case of two agents that hold all the cards is trivial as they know the distribution from the beginning.