Information Sciences 354 (2016) 153–164

Contents lists available at ScienceDirect

Information Sciences

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

Perfectly secure data aggregation via shifted projections

David Fernández-Duque [a,b,*]

[a] Centre for Mathematics and Computer Science, University of Toulouse, 118 Route de Narbonne, F-31062 Toulouse Cedex 9, Toulouse, France

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

ARTICLE INFO

Article history:
Received 2 July 2015
Revised 5 January 2016
Accepted 16 March 2016
Available online 22 March 2016

Keywords:
Private key safeguarding
Data aggregation
Information-theoretic cryptography
Secret sharing

ABSTRACT

We study a general scenario where confidential information is distributed among a group of agents who wish to share it in such a way that the data becomes common knowledge among them but an eavesdropper intercepting their communications would be unable to obtain any of said data. The information is modeled as a deck of cards dealt among the agents, so that after the information is exchanged, all of the communicating agents must know the entire deal, but the eavesdropper must remain ignorant about who holds each card.

This scenario was previously set up in Fernández-Duque and Goranko (2014) as the *secure aggregation of distributed information* problem and provided with *weakly safe* protocols, where given any card c, the eavesdropper does not know with certainty which agent holds c. Here we present a *perfectly safe* protocol, which does not alter the eavesdropper's perceived probability that any given agent holds c. In our protocol, one of the communicating agents holds a larger portion of the cards than the rest, but we show how for infinitely many values of a, the number of cards may be chosen so that each of the m agents holds more than a cards and less than $4m^2a$.

1. Introduction

Consider a scenario where we wish to safeguard multiple bits of information (such as a list of passwords or private keys) by distributing it among several secure locations or trusted agents. For security reasons, we do not wish for any one of the individuals to possess the full list. However, in case the original copy is destroyed, they should be able to pool their shares of the information together in order to reconstruct the original data. Moreover, the agents' communications may be intercepted, and we do not wish for an eavesdropper to be able to retrieve *any* or the protected bits of information. We assume that the eavesdropper has unlimited computational resources, so that the agents must use an unconditionally secure protocol, where the exchange would not contain enough information for an eavesdropper to learn a secret [13].

We will represent the data using a deck of cards Ω dealt among m agents; the secret bits of information will be of the form *The agent $\mathcal{X}$ holds the card c.* The cards are distributed in a previous dealing phase which is treated as a black box and assumed to be secure. Each of the agents may see her hand, but not the others'. They then want to inform each other of which cards they hold. Meanwhile, the eavesdropper, Eve, may intercept all communications, and the agents do not want

* Correspondence address: Department of Mathematics, Instituto Tecnológico Autónomo de México, Río Hondo 1, 01080 Mexico City, Mexico. Tel.: + (33) 5 61 55 67 65.
E-mail address: david.fernandez@irit.fr

http://dx.doi.org/10.1016/j.ins.2016.03.031
0020-0255/

her to obtain information about who holds any card. In this setting, we will show that for many possible distributions of cards among the agents, it is indeed possible for them to share the data securely.

1.1. Comparison to known results

Schemes for safeguarding private keys by multiple parties may be traced back to [2,14]. The protocol we propose, however, uses very different constructions and has the unique feature that multiple bits of information are shared in such a way that each one is individually kept secure from an eavesdropper. This is also related to *verifiable secret sharing (VSS) schemes,* where multiple agents communicate in order to agree on a shared private key [9]. The main difference is that in safeguarding protocols, the information to be shared is fixed beforehand and meant to be reconstructed by the agents, rather than being generated by the exchange. For this reason, our protocol requires a trusted third party (the 'dealer'), whereas VSS schemes do not.

The setup we consider, where information is modeled using a deck of cards, is a multi-agent variant of the well-known *Russian cards problem.* The latter may be traced back to the study in [10] but has recently received renewed attention [6], leading to many new solutions (e.g. [1,4,16]). In the original Russian cards problem, there are only two communicating agents. In [8], this was generalized by allowing an arbitrary number of agents, but also simplified by assuming that the eavesdropper has no cards in her hand. With only two agents, two announcements are needed for the information exchange, one per agent; similarly, with multiple agents, one might expect for each one to make at least one announcement. Indeed, in our protocol, each agent makes exactly one announcement. However, we remark that longer protocols are already needed to solve some instances with two agents [3,7].

There is more than one notion of *safety* that one may consider in this context. For any card c not held by Eve, she should not know with certainty which agent holds c; this is known as *weak safety.* But it may be the case that Eve has a very high probability of guessing correctly who holds c. To this end, Swanson and Stinson [16] introduced the stronger notion of *perfect safety,* where Eve's perceived probability that an agent holds c does not change after executing the protocol. Perfectly safe solutions for a wider number of cases were later reported in [15], and [11] proposed an approximate notion which led to 'almost-perfectly' safe solutions.

In [8] we formalized the secure aggregation of distributed information problem and constructed weakly safe solutions for any number of agents. Our goal now is to construct, instead, perfectly safe solutions. These are based on finite linear algebra, and typically one agent (Alice) holds a large portion of the cards. For practical purposes it is convenient to think of Alice as holding a 'master list' of the cards held by other agents (without her knowing which agent holds any specific card). Nevertheless, for infinitely many values of a, the size of the deck may be chosen so that each of the m agents holds more than a and less than $4m^2a$ of the cards.

1.2. Geometric preliminaries

Our perfectly safe solution is based on finite linear algebra. We assume some basic familiarity with finite fields and finite geometry; these are covered in texts such as [12] and [5], respectively.

Throughout the paper, q will denote a prime or a power of a prime, and $\mathbb{F}_q$ the field with q elements. If d is any natural number, $\mathbb{F}_q^d$ denotes the vector space of dimension d over $\mathbb{F}_q$. Given $U \subset \mathbb{F}_q^d$ and $v \in \mathbb{F}_q^d$, we write $U + v$ for the set $\{u + v : u \in U\}$. A *hyperspace* is a subspace of dimension $d - 1$, and by a *hyperplane* we mean any set of the form $V + x$, where $V \subset \mathbb{F}_q^d$ is a hyperspace and $x \in \mathbb{F}_q^d$. Two hyperplanes X, Y are *parallel* if $X \neq Y$ but there is a vector x such that $X = Y + x$.

Recall that $|\mathbb{F}_q^d| = q^d$, where in general $|X|$ denotes the cardinality of X. Moreover, if $U \neq V$ are hyperplanes, then U has exactly q^{d-1} elements, while $|U \cap V| \leq q^{d-2}$ and equality holds unless U, V are parallel, in which case their intersection is empty.

1.3. Layout of the article

In Section 2 we formalize the *secure aggregation of distributed information* problem and in Section 3 we introduce the notion of perfect safety. Then, in Section 4 we present a motivating example illustrating our protocol in an informal setting. This protocol uses constructions over affine spaces, which we present in Section 5. In Section 6 we define the protocol and show that it is informative, while in Section 7 we prove that it is perfectly safe. Finally, in Section 8 we show how one can find relatively balanced card distributions to which the protocol may be applied.

2. Formalizing the problem

Here we will give the basic definitions needed to set up the secure aggregation of distributed information problem, including the notions of informativity and safety that concern us. This section is essentially a review of notions from [8], although we remark that some definitions are new and some of the terminology has changed.