بسم الله الرحمن الرحيم

شبكة المعلومـــــات الجامعية

التوثيق الالكتروني والميكروفيلم

شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الالكتروني والميكروفيلم

﴿ قـــســـم ﴾

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأفلام قد اعدت دون آية تغيرات

يجب أن

تحفظ هذه الأفلام بعيداً عن الغبار

في درجة حرارة من 15 – 20 مئوية ورطوبة نسبية من 20-40 %

To be kept away from dust in dry cool place of
15 – 25c and relative humidity 20-40 %

بعض الوثائق الأصلية تالفة

بالرسالة صفحات

لم ترد بالأصـــل

MULTIRECEIVER AUTHENTICATION CODES: MODELS, BOUNDS, AND CONSTRUCTIONS

By

Tamer Hashem Farag

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
AT
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
CAIRO UNIVERSITY
GIZA, EGYPT

Supervisors

Prof. Dr. Laila F. Abdelall

Dr. Hassan Aly

Approval Sheet

Tile of the Master thesis:

Multireceiver Authentication Codes: Models, Bounds, and Constructions

Name of the candidate:

Tamer Hashem Farag

Submitted to:

Department of Mathematics – Faculty of Science – Cairo University

Super vision Committee:

Prof. Dr. Laila F. Abdelal L. F. Abdelal

Dr. Hassan Aly

Head of the Department:

Prof. Dr. M. Amer M. Amer
May 9, 2002

Mailing addresses

The supervisors

- Prof. Dr. Laila F. Abdelall
  Department of Mathematics,
  Faculty of Science,
  Cairo University,
  Giza, Egypt.
  email:laila@math-sci.cairo.eun.eg

- Dr. Hassan Aly
  Department of Mathematics,
  Faculty of Science,
  Cairo University,
  Giza, Egypt.
  email:haly@math-sci.cairo.eun.eg

The author

- Tamer Hashem Farag
  Department of Mathematics,
  Faculty of Science,
  Cairo University,
  Giza, Egypt.
  email: hftamer@acm.org

Contents

List of Tables

List of Figures

Preface

In our life, the skillful use of information is the key to success in every profession. Whether one is a teacher, a lawyer, a doctor, a politician, a manager, or a corporate president; the main ingredient in the work involved is how to get, how to use, how to manage, how to develop, how to protect, and how to disseminate information. Today, most information is stored in electronic form. This medium offers many potential advantages: data can be stored and communicated very cheaply and massive amounts of data can be accessed instantaneously using databases. On the other hand, data stored in this way faces new and heightened threats; an asset of the system may become unavailable, an unauthorized party may gain access to an asset, or an authorized party may insert counterfeit objects into the system.

Throughout all structures that use information in electronic form, security aspects in the case of computer networks need special attention, because of the inclusion of many different components, operations, resources, and entities. As a matter of fact communication over open networks is very cheap, but represents easy pickings for an adversary who wants to intercept, modify, or inject data.

To benefit from the advantage offered by electronic data storage and open networks, information security must therefore provide techniques capable of supplying confidentiality, integrity, and availability in this new environment.

Information security focuses on four general security services that encompass the various functions required for an information security. The most common known services are privacy, data integrity, authentication, and nonrepudiation.

Our issue here is the authentication service. Authentication ensures from the

message source and the message substituting during transmission. In other words, it prevents the substitution[1] and impersonation[2] attack.

Authentication service can be computationally secure, which depends on the existing computational power. Or unconditional secure, which is independent on the power of computation; it is with fixed maximum probability of attack. Unconditional authentication service is called authentication code (*A-code*).

One can observe that the traditional *A-code* takes place in point-to-point connection. That is, each authenticated message is sent from one transmitter to one receiver. There are multi-points-to-point, point-to-multi-points, and multi-points-to-multi-points transmissions in the real network transmissions. Desmedt *et al.* [9], introduced the authentication code for multi-points-to-point and point-to-multi-points transmissions, while *et al.* [12], studied the group authentication code, which deal with multi-points-to-point. In 1999, Safavi-Naini and Wang [34], introduced a formal definition of Multireceiver authentication code, which is an authentication service in point-to-multi-points transmissions.

The goal of this work is to examine multireceiver authentication code. It is an authentication code like that of Simmons's [35], where the transmitted massage is to be received by a finite number of receivers. These communications take place in the presence of an eavesdropper or opponent.

Desmedt *et al.* [9], showed that (k, n) multireceiver authentication code in which an opponent and any $k-1$ receivers cannot cheat any other receiver. Kurosawa and Obana [24] derived a combinatorial lower bounds on the probability of success in impersonation and substitution attacks, and characterized Cartesian multireceiver authentication code that satisfies the bounds with equality. Safavi-Naini and Wang [34] derived information theoretic lower bounds on the probability of success in impersonation and substitution attacks against a single receiver by a group of receivers, obtained a lower bound on the number of encoding rules of transmitter and receivers, and also lower bounds on the message length of the transmitter in terms of the deception probability. Also they discussed two extensions of multireceiver authentication code, which are defined by them in a formal way, and they gave constructions for

[1]The transmitted message is substituted by another before delivering.

[2]The attacker sends a message to the receiver instead of the sender.

each.

The authentication service in point-to-multi-point scenarios is treated within this work in two ways: *A-code* with inside attacker, and a new direction of multireceiver authentication code MRA-code.

The *A-code* with inside attacker is an *A-code*, however each message is to be transmitted to any selected receiver out of n receivers. A distributed operating system selects an idle processor to run the user command. In this situation the *A-code* with inside attacker will prevent that processor from being used by an unauthorized machine.

The MRA-code is also an *A-code*, but with m receivers for the transmitted message out of n legal receivers. Again consider the case of distributed operating system, assume that the system wants to send a common piece of information to his currently working machines; the MRA-code will prevent these machines from losing the integrity of the transmitted message.

Any MRA-code has ordinary opponent which is called outside attacker, and a new type of attackers with respect to the traditional authentication code, which is called inside attacker. Actually the multireceiver authentication code, that was introduced in [34], has studied the case in which a group of receivers attacks another single receiver. In this work we study the case in which one receiver cheat other group of receivers, he acts as the transmitter by impersonation or substitution attacks.

In this thesis, information theoretic and combinatorial lower bounds on the probability of success in impersonation and substitution attacks have been derived in each new *A-code*. Other combinatorial and information theoretic bounds have been computed on the sizes of the source states set and the encoding rules set. Constructions that met these lower bounds are given. Definitions of the perfect schemes and some other theorems related to them have been stated.

Parts of this thesis are included in:

- H. Aly and T. Farag, *New Directions in Multireceiver Authentication Codes*, submitted to Information and Computation [3].

- H. Aly and T. Farag, *A-code with inside attacker*, submitted to International journal of Information Security [2].