Signature Identification Scheme Based on Iterated Function Systems

Nadia M. G. AL-Saidi

***Abstract*—**Since 1984 many schemes have been proposed for digital signature protocol, among them those that based on discrete log and factorizations. However a new identification scheme based on iterated function (IFS) systems are proposed and proved to be more efficient. In this study the proposed identification scheme is transformed into a digital signature scheme by using a one way hash function. It is a generalization of the GQ signature schemes. The attractor of the IFS is used to obtain public key from a private one, and in the encryption and decryption of a hash function. Our aim is to provide techniques and tools which may be useful towards developing cryptographic protocols. Comparisons between the proposed scheme and fractal digital signature scheme based on RSA setting, as well as, with the conventional Guillou-Quisquater signature, and RSA signature schemes is performed to prove that, the proposed scheme is efficient and with high performance.

***Keywords*—**Digital signature, Fractal, Iterated function systems (IFS), Guillou-Quisquater (GQ) protocol, Zero-knowledge (ZK)

I. INTRODUCTION

SUBSEQUENT to the appearance of the first idea of a digital signature that relied on public key algorithms, many novel schemes were introduced and many new properties added. A ZK proof of identity is a novel idea in the identification schemes that relied on public key algorithms. It is cryptographic protocols provides provably secure entity authentication, without revealing any knowledge to any entity or to any eavesdropper based on hard computational problem.

Secure identification is an important security affair to avoid computer fast developments. Using a hash function, a secure digital signature scheme can be constructed. A digital signature scheme has equal complexity as the identification scheme [1]. It is used to build effective communication tools and to ensure privacy. The ZK protocol was proposed at first as a method for exchanging public keys, for creating digital signatures or for protecting digital cash on smart cards. It is considered as time-consuming than other authentication methods, but also harder to crack [2]. The identification protocol by GQ is a particular type of digital signature defined in an RSA setting, but generates its own signature, which is vulnerable compared to the digital signature generated by RSA scheme. The concept of a digital signature was introduced by Diffie and Hellman in1976. They published their landmark paper"New Directions in Cryptography" [3]. The RSA signature is the first method discovered and it is approved as a standard system and is popular and most widely used.

Nadia M.G. Al-Saidi is with Applied Sciences Department-Applied Mathematics University of Technology -Baghdad-Iraq.e-mail: nadiamg08@gmail.com

The signature works in Z_n where n is the product of two large primes' p and q, and its security is based on the hardness of the modeling and factorization problem. The ZK Proof was first introduced by Goldwasser, Micali and Rackoff [4] in 1985. The wide applicability of ZK was demonstrated by Goldreich, Micali and Wigderson in [5]. Fiat and Shamir [6] introduced an identification and signature scheme that helps to prove the identity and the authenticity of the messages. The system generate signature which is vulnerable compared to the digital signature generated by the RSA scheme. Guillou and Quisquater (GQ) presented an identification and signature scheme [7]. It is an extension of the RSA protocol which reduces the number of rounds needed to 1, and its security is based on intractability of RSA problem.

Unlike the identification and signature scheme of previous studies which based on factorization problem or discrete logarithm problem on a finite field, new systems for identification and signature based on infinite fields pose as new challenges in modern cryptosystems. Alia, M. and A. Samsudin in [8] proposed a new ZK proof of identity protocol based on Mandelbrot and Julia Fractal sets. They identified that the security of the proposed fractal ZK proof of identity is based on the NP-hard problem and the randomness of the output generated. Shuichi Aono, Yoshifumi Nishio, in [1] proposed an authentication protocol by using of three times the authentication interaction. This authentication protocol is based on iterations of the logistic map in public-key cryptography. Al-Saidi N. and Rushdan M. in [9] proposed a new digital signature scheme based on IFS. They generate the new digital signature system, based on fractal attractor.The remaining sections of this paper are organized as follows. The mathematical preliminaries about the iterated function system are presented in the materials and methods section. Following this the concepts of digital signature schemes, and GQ signature are summarized. A new digital signature identification scheme, based on IFS as a generalization of (GQ) identification and signature schemes is proposed. An example, and the performance analysis, are analyzed in the results and discussions section. Finally conclusions are drawn.

II. MATERIALS AND METHODS

A- Iterated Function Systems

The term "iterated function system" (abbreviated: IFS) was coined in [10] by Barnsley & Demko to describe a general framework of dynamics. However, most of the results about the IFS model are presented in [11]-[12]. This section provides an overview of the major concepts and results of Iterated Function System (IFS) and their

INVITATION LETTER

July 09, 2011

Assoc. Prof. Dr. Nadia Al-saidi
University Of Technology
Iraq

To Whom It May Concern,

We are pleased to inform you that your peer-reviewed & refereed full paper entitled "Signature Identification Scheme Based On Iterated Function Systems" is accepted for oral presentation at the ICMCSSE 2011 : International Conference on Mathematical, Computational and Statistical Sciences, and Engineering to be held in Paris, France during August 24-26, 2011.
This letter serves as confirmation of your participation in the conference.
We would greatly appreciate if you could facilitate granting the conference delegate the necessary visa.

Sincerely Yours,

C. Ardil,
Conference Secretariat
ICMCSSE 2011 Paris
France

Holiday Inn Paris
Montparnasse-Av.Du Maine
79-81 Avenue Du Maine
Paris, 75014 France
Phone: +33-1-43201393
Fax: +33-1-43209560
www.holidayinn.com/parisgare

WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY

WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY

www.waset.org

CERTIFICATE OF PRESENTATION

This certificate is awarded to

NADIA AL-SAIDI

in oral and technical presentation, recognition and appreciation of research contributions to ICMCSSE 2011 : International Conference on Mathematical, Computational and Statistical Sciences, and Engineering

INTERNATIONAL SCIENTIFIC RESEARCH AND EXPERIMENTAL DEVELOPMENT

CEMAL ARDIL

WASET CHAIR

PARIS, FRANCE

AUGUST 24-26, 2011