On the RS-Code Construction of Ring Signature Schemes and a Threshold Setting of RST

Duncan S. Wong, Karyin Fung, Joseph K. Liu, and Victor K. Wei

Department of Information Engineering
The Chinese University of Hong Kong
Hong Kong, China
{duncan,kyfung2,ksliu9,kwwei}@ie.cuhk.edu.hk

Abstract. We propose a Reed-Solomon (RS) code construction of the 1-out-n (ring) signature scheme. It is obtained from the observation of the equivalency between the erasure correction technique of the RS code and the polynomial interpolation. The structure is very simple and yields a ring equation that can appropriately denoted by $z_1 + \cdots + z_n = v$, which represents the summation of n evaluations of a polynomial. We also show how to extend the generic RST scheme [6] to a t-out-n threshold ring signature scheme.

Keywords: Signature Schemes, Coding Theory

1 Introduction

The notion of ring signature was first formalized by Rivest, et al. [6] in 2001. The scheme concerns about the generation of a signature on a message by some signer who uses its own private key and some other parties' public keys without their consent or assistance. Essentially, any signer can choose any set of possible signers that includes himself, and sign any message by using his secret key and the others' public keys. Any verifier who has all the public keys can verify if a ring signature is actually produced by at least one of the possible signers. However, the verifier does not know who the real signer is. It is called a ring signature scheme and distinguishes itself from a group signature scheme as it does not have a group manager to predefine certain groups of users or revoke the identity of the actual signer, nor does require any cooperation among those parties whose public keys are included in a ring signature.

In 2002, Bresson, et al. [3] extended the notion to a threshold setup. A (t, n)-threshold ring signature scheme is defined to be a ring signature scheme of which at least t corresponding private keys of the n public keys are needed to produce a signature. Applications of ring signature and threshold signatures include leaking authoritative secrets in an anonymous way [6], communicating sensitive data among parties in ad-hoc groups [3], and some others.

In this paper, we propose a new approach of constructing a ring signature scheme and also a new construction of a threshold ring signature scheme. We obtain the new ring signature scheme from the observation of the equivalency

S. Qing, D. Gollmann, and J. Zhou (Eds.): ICICS 2003, LNCS 2836, pp. 34–46, 2003.
© Springer-Verlag Berlin Heidelberg 2003

between the erasure correction technique of the Reed-Solomon (RS) code [5] and the polynomial interpolation. By modifying and considering a special case (when $t = 1$) of a (t, n)-threshold ring signature scheme using secret sharing[1], we obtain a new ring signature scheme with the ring structure being so simple that it can be represented by a summation of evaluations of a polynomial at n distinct nodes. In [6], the authors investigated the feasibility of using simple combining functions such as bitwise exclusive-or operations or simple summations. However, they fell short to obtain a secure one. In this paper, we propose to use simple summations as the combining function and discuss what additional requirements are needed in order to make the scheme secure.

About the new construction of a threshold ring signature scheme, our approach can be described as a natural extension of the RST scheme [6] using a tandem construction technique. We will see that the extension retains the original ring-like structure of RST and the security proofs can be carried out without any major deviations. Our scheme is efficient for moderate number of possible signers n and small number of participating signers t. In addition, our technique can also be used to extend other ring signature schemes to threshold forms.

The rest of the paper is organized as follows. In the next section, we review some ring signature schemes and threshold ring signature schemes. This is followed by the RS code construction of the ring signature scheme in Sec. 3. In Sec. 4, we review the RST scheme and propose a threshold extension to it using a tandem construction technique. Its security and complexity are also discussed. We conclude the paper in Sec. 5.

2 Related Work

A ring is a set of n parties, each of them is called a ring member. We assume that each ring member (indexed by) i, $1 \leq i \leq n$, is associated with a publicly known trapdoor one-way permutation g_i and a secret trapdoor information T_i which is known only by the ring member i. That is, only ring member i knows how to compute the inverse g_i^{-1} efficiently, using the trapdoor information T_i.

2.1 Ring Signature

RST [6] is the first ring signature scheme ever proposed. Not only the notion is portrayed to a ring due to its geometric characteristics such as uniform periphery and the absence of center, their construction is also very well illustrated as a ring structure which consists of n nodes. In their construction, the real signer uses the public keys of other possible signers to construct an *open* ring with a gap. Then he uses his own private key to *close* the gap.

Although ring signature was first formalized in 2001 by Rivest, et al., similar concept was actually raised earlier. In 1994, Cramer, et al. [4] proposed a proof of knowledge protocol which consists of the properties of a threshold ring

[1] Due to Bresson, et al. in the full version of [3]. Available at `www.di.ens.fr/~bresson`