Threshold Ring Signatures Efficient for Large Sets of Signers

K. Maneva-Jakimoska, G. Jakimoski*and M. Burmester

Abstract

The anonymity provided by the threshold ring signature scheme proposed by Bresson et al (Crypto'02) is perfect. However, its complexity is prohibitively large even for relatively small sets of signers. We propose use of threshold schemes based on covering designs that are efficient for large groups of signers. The cost we pay is non-perfect anonymity.

Keywords: anonymity, digital signatures, ring signatures, threshold cryptography, threshold ring signatures, covering designs

1 Introduction

The notion of a ring signature was first formalized by Rivest et al [9] in order to provide means for anonymous signing that does not require group managers, setup procedures, revocation procedures and coordination. Any user can select an arbitrary set (i.e., ring) of possible signers that includes himself, and using his secret key and the public keys of the members of the ring, he can sign an arbitrary message. Given a message and a ring signature for that message, the verifiers cannot tell which member of the ring has produced the signature.

Bresson et al [2] extend the notion of a ring signature to a multi-signer threshold setting. In a threshold ring signature scheme, only the subsets of the ring whose size is above some threshold value can generate a signature for a given message. The signature is anonymous in the sense that the verifiers cannot tell which members of the ring are the actual signers.

Our contribution. The complexity of the scheme proposed in [2] is exponential in the number of actual signers, and the scheme is prohibitively expensive even for relatively small number of signers. We propose use of threshold ring signature schemes based on covering designs that are efficient even for large number of actual signers (e.g., the time complexity can be linear in the number of possible signers). The drawback of the proposed schemes is that the provided anonymity might not be perfect.

Related work. The concept of a ring signature has been informally discussed simultaneously with the appearance of group signatures [3, 4]. Some extensions of this concept can be found in [7, 10, 11]. Covering designs have been used in the past both in threshold schemes and to achieve anonymity (e.g., [5, 8]). Some efficient constructions of covering designs can be found in [6, 8].

*This work was supported in part by the National Science Foundation under Grant CCR-008588.

2 Preliminaries

2.1 Ring signature schemes

In this section, we briefly describe the ring signature scheme (RSA version) proposed by Rivest, Shamir and Tauman (see [9] for a more detailed description).

Ring signatures are used to convince any verifier that the author of the signatures belongs to some set of possible signers, while hiding the identity of the actual signer. A ring signature scheme consists of two algorithms:

- **ring-sign** produces a ring signature σ on a message m, given the public keys $v_1, \ldots, v_n$ of all the members of the ring and the secret key s_s of the s-th member (who is the actual signer).
- **ring-verify** accepts a message m and a ring signature σ (which includes the public keys of all the possible signers), and outputs either *true* or *false*.

Ring signature schemes are set-up free. The signer needs only the public keys of the non-signers. He doesn't need the knowledge, consent, or assistance of the non-signers. In order to be secure, the scheme must satisfy the usual soundness and completeness conditions. However, in addition, a ring signature scheme should be signer-ambiguous. Namely, the verifier should not be able to determine the identity of the actual signer.

Fig. 1 depicts the ring signature scheme proposed by Rivest et al [9]. The steps of the *ring-sign* algorithm in a scheme that allows for a message m to be signed by n ring members are as follows:

1. Compute a key k for a symmetric encryption scheme E_k by hashing the message $k = h(m)$.
2. Pick a random glue value v.
3. Pick randomly x_i and compute $y_i = g_i(x_i); 1 \leq i \leq n, i \neq s$, where each g_i is a trap-door permutation.
4. Solve the ring equation
$$E_k(y_n \oplus E_k(y_{n-1} \oplus E_k(\ldots E_k(y_1 \oplus v)))) = v$$
for y_s.
5. Using the trap-door s_s invert g_s on y_s to obtain the value of $x_s = g_s^{-1}(y_s)$.
6. Output the ring signature σ as a $(2n+1)$-tuple
$$(v_1, \ldots, v_n; v; x_1, \ldots, x_n).$$

It is clear that any ring member could have produced a given ring signature σ on a message m. Therefore, when the verifier receives a message m with a signature σ, the only thing that he can verify is that someone from the ring signed the message. He computes $y_i = g_i(x_i)$ for $1 \leq i \leq n$, obtains the key $k = h(m)$, and verifies the ring equation

$$E_k(y_n \oplus E_k(y_{n-1} \oplus E_k(\ldots E_k(y_1 \oplus v)))) = v.$$

If the y_i's satisfy the ring equation, the verifier accepts the ring signature as valid. Otherwise, the verifier rejects.

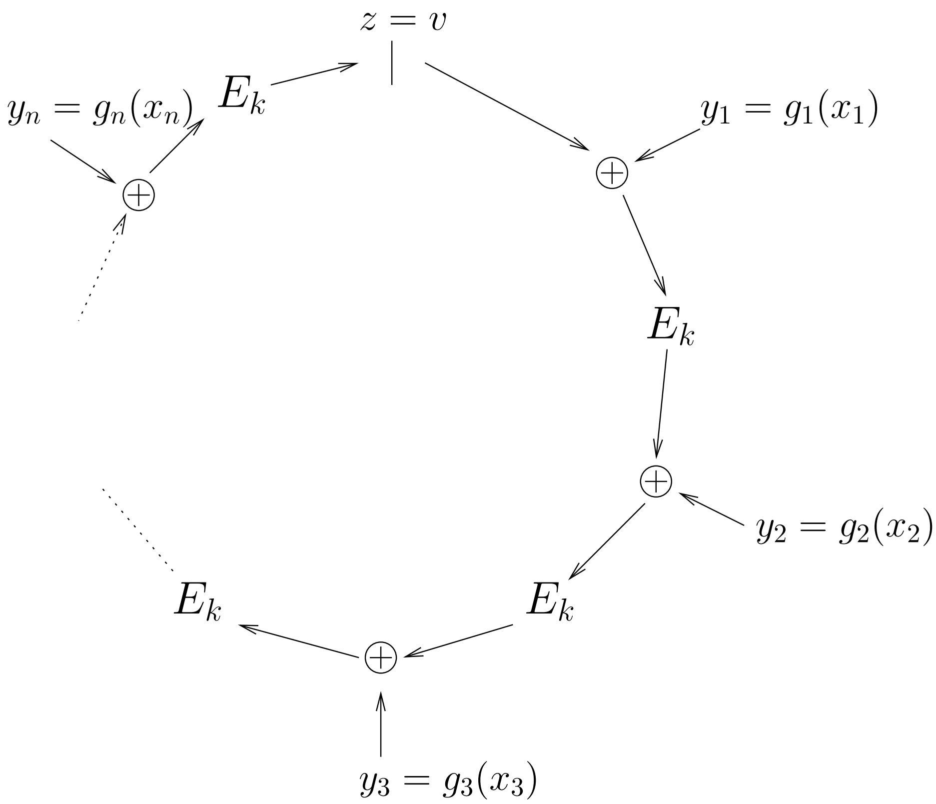

Figure 1: The ring signature scheme proposed by Rivest et al [9]

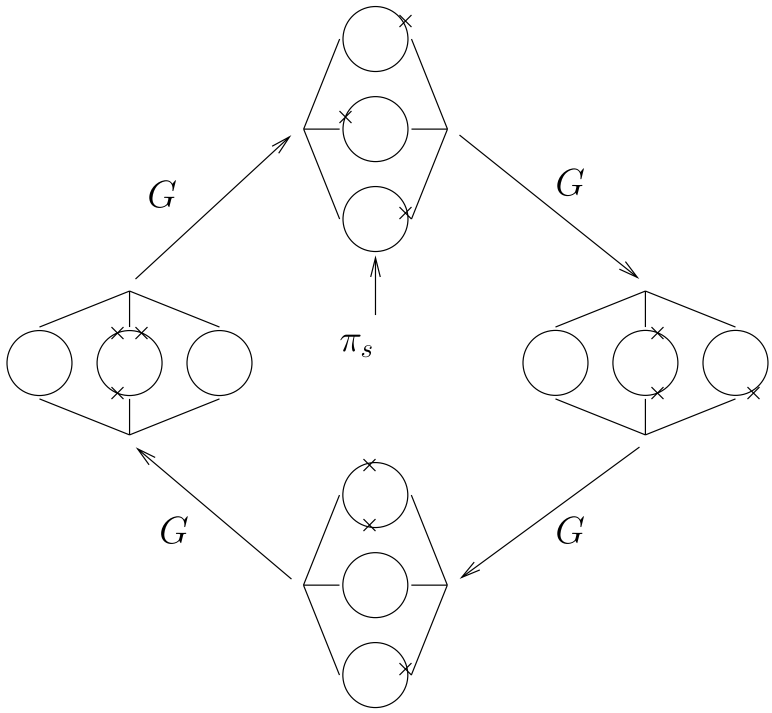

Figure 2: The super-ring composition paradigm when $t = 3$. π_s is a fair partition with respect to the three signers, and they can solve the ring equations.

2.2 Threshold ring signatures

Threshold ring signatures prove that a certain minimum number of members of a certain group must have collaborated to produce the signature, while hiding the precise membership of the subgroup of signers. A threshold ring signature scheme consists of two algorithms:

- **T-ring-sign algorithm** outputs a (t, n)-ring signature σ on the message m, given a message m, a ring of n users and their corresponding public keys, and the secret keys of t members. The number of signers t and the n public keys of the ring members are part of the signature σ.
- **T-ring-verify** outputs *true* or *false* indicating whether a given signature σ is valid or not valid for a given message m.

A threshold ring signature is secure if it is unforgeable and anonymous. That is, no group of less than t members can forge a signature in collaboration with the adversary, and the verifier cannot determine the identity of the actual signers.

Fig. 2 depicts the basic principle behind the threshold ring signature scheme proposed by Bresson et al (see [2] for details). The ring of n users is partitioned into t disjoint subsets a number of times. Each partition is one node in a super-ring and each subset of the partition is one sub-ring. A group of t users can "close" the super-ring (i.e., produce a (t, n)-ring signature) if and only if one of the partitions in the super-ring is a fair partition for the group of t users. That is, there is a partition in the super-ring such that each subset of the partition contains at least one actual signer. Bresson et al [2] suggest use of perfect hash functions [1] to construct the partitions of the super-ring. In this manner, the collection of partitions is an (n, t)-complete partitioning system meaning there is a fair partition for any subset of t users. Since any group of t users can produce a signature, the scheme provides perfect anonymity.

2.3 Covering designs

The following definitions will be useful in the next section.

Definition 1 (Set system) *A* set system *is a pair* $(X, \mathcal{B})$ *of a set* $X = \{a_1, a_2, \dots, a_v\}$ *and a multiset* $\mathcal{B}$ *whose elements are subsets (or* blocks*) of* X*.*

Definition 2 (Covering design) *The set system* $(X, \mathcal{B})$ *is a* (v, b, t)-covering design *if*

1. *all blocks in* $\mathcal{B}$ *are* b*-subsets of* X*, i.e.* $\forall_{B \in \mathcal{B}} |B| = b$*, and*
2. *any* t*-subset of* X *is contained in at least one block.*

Some efficient constructions of covering designs can be found in [6, 8].

Definition 3 (Complementary set system) *The* complementary set system *of a set system* $(X, \mathcal{B})$ *is the set system* $(X, \mathcal{B}^c)$*, where* $\mathcal{B}^c = \{X \backslash B_i | B_i \in \mathcal{B}\}$*.*

3 Threshold ring signatures based on covering designs

Let $U = \{u_1, \dots u_n\}$ be the set of possible signers, and let $U_s = \{u_{s_1}, \dots, u_{s_t}\}$ be the set of actual signers. The actual signers construct a collection of rings $\mathcal{R}$ so that each ring R_i in $\mathcal{R}$ is an r-subset of U, and it contains at least one actual signer $u_{s_j} \in U_s$. We refer to the set system $(U, \mathcal{R})$ as the *ring set system* of the scheme. Whenever the users in U_s want to anonymously leak a secret m, they use a ring signature scheme to generate a ring signature σ_i on m for each ring $R_i \in \mathcal{R}$. The threshold ring signature σ consists of the computed ring signatures $\sigma = (\sigma_1, \dots, \sigma_{|\mathcal{R}|})$. A simple example is depicted in Fig. 3.

It is clear that the t actual signers can generate a threshold ring signature as described above since there is at least one actual signer in each ring $R_i \in \mathcal{R}$. However, the verifier wants to be sure that no $t-1$ users can conspire and forge a signature. The following theorem gives an answer whether the threshold ring signatures generated as above are unforgeable.

Theorem 1 *Suppose that the underlying ring signature scheme is unforgeable. Our threshold ring signature scheme is unforgeable if and only if the complementary set system of the ring set system* $(U, \mathcal{R})$ *is an* $(n, n-r, t-1)$*-covering design.*

Proof outline. We assume the the underlying ring signature scheme is unforgeable in the following sense. The adversary has knowledge of the public keys of the r members of the ring. However, he does not know the corresponding secret keys. The adversary can query a signing oracle that given a message and a set of r public keys outputs a ring signature of the message for the ring specified by the public keys. The scheme is unforgeable if the adversary cannot produce a ring signature on a message that has not been signed previously.

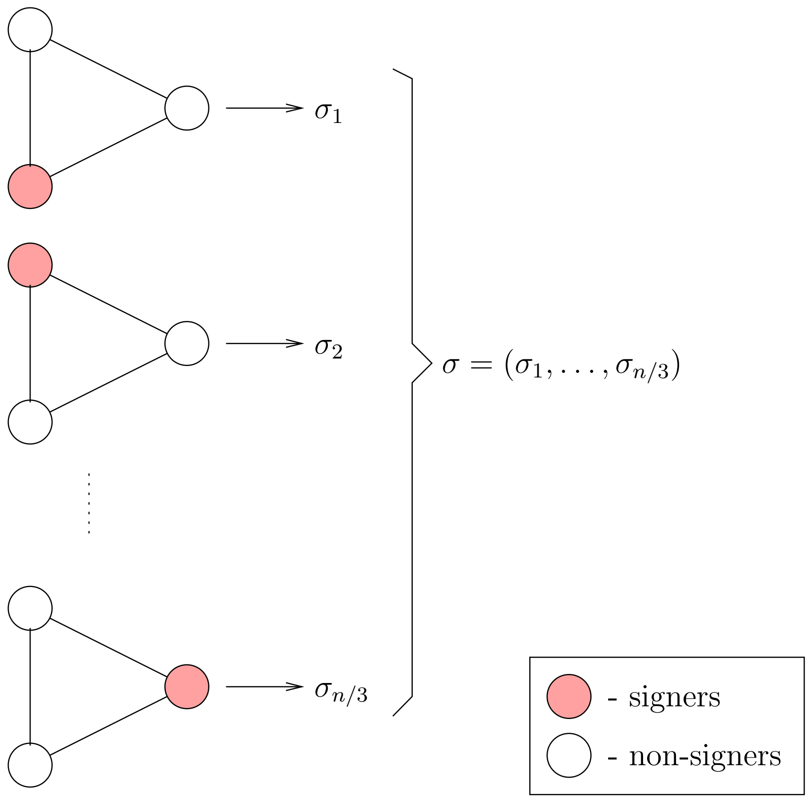

Figure 3: A threshold ring signature scheme when $t = n/3$. There are $n/3$ disjoint rings in $\mathcal{R}$. Not any t-set of users can sign a message. However, the number of t-sets of users that can sign messages grows exponentially with n (i.e., $3^{n/3}$) and the complexity of the scheme is linear in the number of users (i.e., $\theta(n)$). Furthermore, note that any of the n users is a possible signer. If the Bresson et al [2] is used, any t-set can sign messages. However, the complexity of the scheme is $\mathcal{O}(2^{n/3} n \log n)$.

In the case of a threshold ring signature scheme, we assume that the adversary has knowledge of the public keys of the n users and the secret keys of any $t-1$ users. The adversary can send signing queries to an oracle to get threshold ring signatures. The goal of the adversary is to produce a threshold ring signature on a message m that was not previously sent for signing. The scheme is unforgeable if the adversary cannot succeed (with non-negligible probability).

Suppose that the complementary set system $(U, \mathcal{R}^c)$ of the ring set system $(U, \mathcal{R})$ is not an $(n, n-r, t-1)$-covering design. This means that there is a $(t-1)$-subset $C \in U$ such that $C \bigcap R_i \neq \varnothing$ for all $R_i \in \mathcal{R}$. In other words, there is at least one conspirator (member of C) in each ring of the threshold scheme. Clearly, the $t-1$ conspirators in C can forge signatures.

Assume now that the complementary set system $(U, \mathcal{R}^c)$ of the ring set system $(U, \mathcal{R})$ is an $(n, n-r, t-1)$-covering design, but the threshold scheme is not unforgeable. We will show how a successful adversary for the threshold ring signature scheme can be converted into a successful adversary for the underlying ring signature scheme which is in contradiction with our assumption that the underlying ring signature scheme is unforgeable. The adversary for the ring signature scheme follows the same procedure as the adversary for the threshold scheme, and simulates the threshold scheme oracle. We can simulate the signing oracle for the threshold ring signature scheme using an oracle of a ring signature scheme as follows. Whenever the threshold scheme adversary sends a signing query, we construct a threshold ring signature by sending $|\mathcal{R}|$ signing queries to a ring signature scheme oracle, combining the answers and then sending the result back to the threshold scheme adversary. At the end, the threshold scheme adversary will output a threshold ring signature $\sigma^f = (\sigma_1^f, \ldots, \sigma_{\mathcal{R}}^f)$ of a message that was not signed previously by the oracle. Suppose that the adversary knows the secret keys of the users $u_{i_1}, \ldots, u_{i_{t-1}}$. Since $(U, \mathcal{R}^c)$ is a $(n, n-r, t-1)$-covering, there is a ring $R_i \in \mathcal{R}$ such that $R_i \bigcap \{u_{i_1}, \ldots, u_{i_{t-1}}\}$ is empty. In other words, there is no user in R_i whose secret key is known to the adversary. Therefore, the ring signature σ_i^f corresponding the the i-th ring R_i is a forgery for the underlying ring signature scheme. ■

We end this section with a concrete construction of a ring set system when the number of possible signers is $n = t^d$, where t is the number of actual signers and d is an integer greater than one. In this case, the n users can be arranged in a d-cube. Each user $u_{i_1,\ldots,i_d}$, where $i_1, \ldots, i_d \in \{0, 1, \ldots, t-1\}$, is a member of exactly d rings of the ring set system:

$$
\begin{array}{l}
\{u_{j_1,\ldots,j_d} | j_1 = i_1\} \\
\{u_{j_1,\ldots,j_d} | j_2 = i_2\} \\
\vdots \\
\{u_{j_1,\ldots,j_d} | j_d = i_d\}.
\end{array}
$$

The cases $d = 2$ and $d = 3$ are depicted in Fig. 4.

It is not hard to verify the following properties of the construction:

- The number of t-sets of users that can produce signature is $(t!)^{d-1}$, and it grows very fast both with t and with d.
- Each user can be an actual signer. That is, for each user u, there is a t-set of users that includes u and can produce a threshold ring signature.
- The complexity of the scheme is $\mathcal{O}(d \cdot n) = \mathcal{O}(n \log n)$.

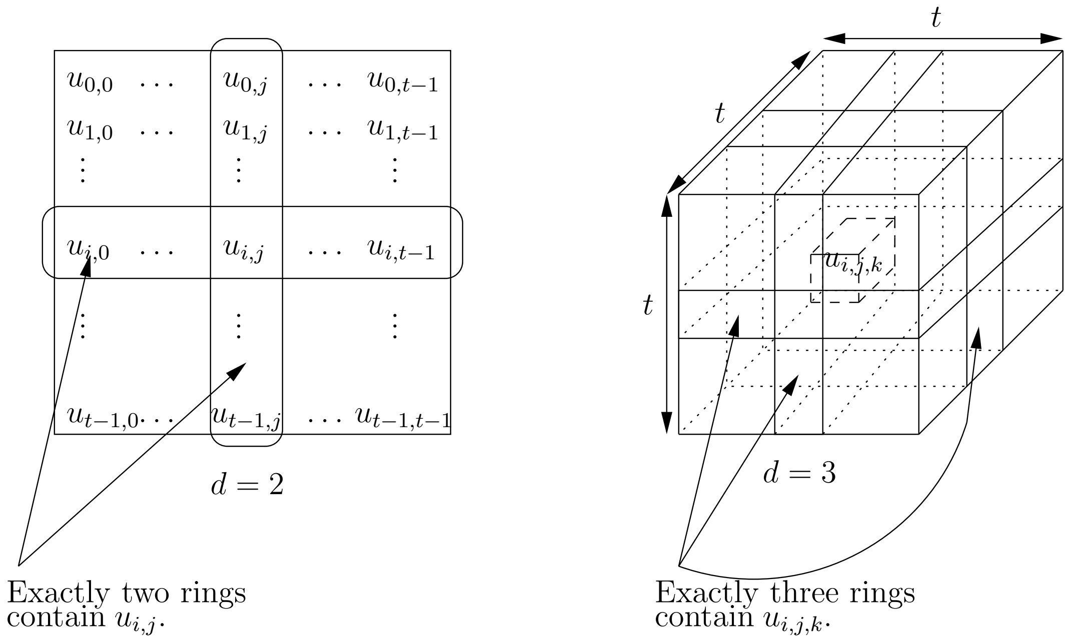

Figure 4: d-cube ring set system construction. The cases $d = 2$ and $d = 3$.

4 Conclusion

We propose threshold ring signature schemes based on covering designs. The schemes are efficient even for large groups of signers.

References

[1] N. Alon, R. Yuster and U. Zwick, "Color coding," Journal of ACM, Vol. 42, pp. 844-856.

[2] E. Bresson, J. Stern and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," In Crypto'02, LNCS 2442, pp. 465-480, Springer-Verlag, 2002.

[3] D. Chaum and E. van Heyst, "Group signatures," In Eurocrypt'91, LNCS 547, pp. 257-265.

[4] L. Chen and T. Pedersen, "New group signature schemes," In Eurocrypt'94, LNCS 950, pp. 171-181.

[5] Y. Desmedt and K. Kurosawa, "How to Break a Practical MIX and Design a New One," In Eurocrypt 2000, LNCS 1807, pp. 557-572, Springer-Verlag, 2000.

[6] W.H.Mills,"Covering design I: coverings by a small number of subsets," Ars Combin. 8, (1979), pp. 199-315.

[7] M. Naor, "Deniable Ring Authentication," In Crypto 2002, LNCS 2442, pp. 481-498, Springer-Verlag, 2002.

[8] R.Rees, D.R.Stinson, R.Wei and G.H.J. van Rees, “An application of covering designs: Determining the maximum consistent set of shares in a threshold scheme,” Ars Combin. 531 (1999), pp. 225-237.

[9] R. L. Rivest, A. Shamir and Y. Tauman, “How to leak a secret,” In Asiacrypt 2001, pp. 552-565, Springer-Verlag, 2001.

[10] P. P. Tsang, V. K. Wei, T. K. Chan, M. H. Au, J. K. Liu and D. S. Wong, “Separable Linkable Threshold Ring Signatures,” Cryptology ePrint archive: Report 2004/267.

[11] S. Xu and M. Yung, “Accountable ring signatures: a smart card approach,” IFIP CARDIS’04.