

Hierarchical Ring Signatures

Łukasz Krzywiecki, Mirosław Kutylowski, and Anna Lauks-Dutka

Institute of Mathematics and Computer Science, Wrocław University of Technology,
lukasz.krzywiecki@pwr.wroc.pl, mirosław.kutylowski@pwr.wroc.pl,
anna.lauks@pwr.wroc.pl

1 Introduction

Ring signatures enable to sign a message but to remain hidden in some ad hoc created group of people, called a ring. This concept was introduced by Rivest et al. [1] in 2001 and later intensively studied. In [2] ring signatures were combined with deniable authentication into deniable ring authentication scheme. Linkable ring signature scheme presented in [3] allows to link signatures signed by the same person. There are identity based ring signature schemes that enable to construct rings across different identity-based master domains. Chen et al. [4] proposed confessible threshold ring signature scheme. Klonowski et al. [5] introduced step-out ring signature scheme for which non-signers from the ring can prove not being the real signers.

In case of regular ring signatures for creating a signature the signer uses his secret key and the public keys of the other ring members. The public keys of all ring members are necessary for signature verification. A verifier thus can determinate the ring members who are the potential signers, but the real signer remains hidden within them. The basic construction requires inclusion into each ring signature amount of data proportional to the number of ring members. This is a drawback since in order to strengthen anonymity level the signer increases the ring size, thus producing long signatures.

We present a ring signature scheme that yields *short hierarchical ring signatures* (SHRS) without weakening the anonymity features. These signatures form a hierarchical structure such that signatures created on a particular level utilize anonymity sets (rings) of all previously created signatures from lower levels. This construction is an alternative solution to the construction based on one-way accumulators presented by Dodis et al. in [6]. They assumed that in practical situations the ring stays the same for a long period of time or can have a short description. That allowed them to create a constant-size ring signatures based on some constant-size information (appropriate group secret and public keys). We also propose to reuse the information about previous rings in order to get the short signature. However, the hierarchical construction allows the size of the anonymity set to grow exponentially with the level number. Our construction can be adopted to some other ring scenarios. For example, it can be easily transformed to get the step-out feature described in [5].

2 Preliminaries

Our construction of SHRS is based on a cyclic group where discrete logarithm, CDH and DDH problems are hard. Namely, let p, q be prime, $q|p-1$, and $G = \langle g \rangle$ be a cyclic subgroup of \mathbb{Z}_p^* of order q . In our construction we use the following building blocks:

- NIZKP($\hat{g}, g, \hat{y}, \{y_1, \dots, y_n\}$) – a non interactive zero knowledge proof of knowledge and equality of discrete logarithms $\log_{\hat{g}} \hat{y}$ and $\log_g y'$, where y' is some element from the list $\{y_1, \dots, y_n\}$ (not indicated by the proof).
- SIG(g^x, M) – a public key based signature over a message M , where x, g^x denote, respectively, the secret and the public key of the signer.

- $\mathcal{H} : \{0, 1\}^* \rightarrow \langle g \rangle$ – ideal hash functions such that the output from \mathcal{H} is suitable for being a generator of G used in NIZKP and SIG.

We assume that there is a PKI for registering user's public keys. Let x_u denote the private key of user u , and g^{x_u} be the corresponding public key. We assume that PKI also provides a bulletin board (BB) where all SHRS signatures can be published to be available for verification and reuse.

Moreover, we use $\overline{\text{NIZKP}}(\hat{g}, \hat{y}, \{(g_1, y_1), \dots, (g_n, y_n)\})$, a slight modification of NIZKP, which is a non interactive zero knowledge proof of knowledge and equality of discrete logarithms $\log_{\hat{g}} \hat{y}$ and $\log_{g_*} y_*$, where $(g_*, y_*) \in \{(g_1, y_1), \dots, (g_n, y_n)\}$.

3 Scheme Description

During signature creation on a leaf level a signer j creates SHRS_A as

$$\overline{\text{NIZKP}}(g_A, g_A^{x_j}, \{(g, y_1), \dots, (g, y_j), \dots, (g, y_n)\}) \parallel \text{SIG}(g_A^{x_j}, M_A),$$

where the generator g_A is obtained by the means of \mathcal{H} . SHRS_A proves that the message M_A was signed with the private key hidden in $g_A^{x_j}$ and that it is the exponent taken from public keys of the ring $A = \{y_1, \dots, y_j, \dots, y_n\}$. Note that on the leaf level the length of SHRS_A signature is proportional to the cardinality of the ring A , and that its elements y_i are all public keys (with respect to generator g) of potential signers registered in PKI. Once created, the signature SHRS_A is published to the bulletin board (BB) available to all users of PKI.

During signature creation on a non-leaf (higher) level of infrastructure, the signer j can use all previously created signatures from lower levels published by BB. To illustrate this let us assume that there are two leaf level signatures available, say SHRS_A , SHRS_B , and that j was the creator of SHRS_A . Now j can create another signature SHRS_C , namely $\overline{\text{NIZKP}}(g_C, g_C^{x_j}, \{(g_A, y_A), (g_B, y_B)\}) \parallel \text{SIG}(g_C^{x_j}, M_C)$. Therefore the signature SHRS_C is the proof that message M_C was signed by a user whose private key is hidden in $g_C^{x_j}$ and that this exponent equals to one hidden in an element from the ring A or B . Now the length of signature SHRS_C is proportional to the number of previous signatures that were used for the construction of SHRS_C . The signature SHRS_C is shorter, but its anonymity set is larger as it absorbs the anonymity sets of SHRS_A and SHRS_B . Note that such a construction can be performed on higher levels of SHRS signature infrastructure providing increased anonymity without enlarging the size of the signature.

References

1. Rivest R.L., Shamir A., Tauman Y.: *How to Leak a Secret*. ASIACRYPT 2001, LNCS 2248, pp. 552–565.
2. Naor M.: *Deniable Ring Authentication*. CRYPTO 2002, LNCS 2442, pp. 481–498.
3. Tsang P.P., Wei V.K.: *Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation..* ISPEC 2005, LNCS 3439, pp. 48–60.
4. Chen Y.S., Lei C.L., Chiu Y.P, Huang C.Y.: *Confessible Threshold Ring Signatures*. ICNSC 2006, IEEE Computer Society, pp. 25.
5. Klonowski M., Krzywiecki L, Kutylowski M., Lauks A.: *Step-out Ring Signatures*. MFCS 2008, LNCS 5162, pp. 431–442.
6. Dodis Y., Kiayias A., Nicolosi A., Shoup V.: *Anonymous Identification in Ad-hoc Groups*. EUROCRYPT 2004, LNCS 3027, pp. 609–626.