

On Hierarchical Threshold Secret Sharing

Ali Aydın Selçuk¹, Kerem Kaşkaloğlu², and Ferruh Özbudak³

¹ Department of Computer Engineering
Bilkent University, 06800, Ankara, Turkey
selcuk@cs.bilkent.edu.tr

² Department of Mathematics
Atılım University, 06836, Ankara, Turkey
keremk@atilim.edu.tr

³ Department of Mathematics, and Institute of Applied Mathematics
Middle East Technical University, 06531, Ankara, Turkey
ozbudak@metu.edu.tr

Abstract. Recently, two novel schemes have been proposed for hierarchical threshold secret sharing, one based on Birkoff interpolation and another based on bivariate Lagrange interpolation. In this short paper, we propose a much simpler solution for this problem.

Keywords: Secret sharing, threshold cryptography, hierarchical access structures.

1 Introduction

A (conjunctive) hierarchical threshold secret sharing (HTSS) problem in an n -member user set \mathcal{U} is defined by a partition of the user set into m disjoint subsets (*compartments*),

$$\mathcal{U} = \mathcal{U}_1 \cup \mathcal{U}_2 \cup \dots \cup \mathcal{U}_m,$$

where $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$ for $i \neq j$, and a sequence of integers

$$0 < k_1 < \dots < k_m$$

such that the access structure (i.e., the set of authorized subsets) is

$$\Gamma = \{\mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap (\cup_{j=1}^i \mathcal{U}_j)| \geq k_i \forall i \in \{1, 2, \dots, m\}\}. \quad (1)$$

A detailed discussion of this problem and a comprehensive survey of related results can be found in [6, 7].

Tassa [6] and Tassa and Dyn [7] recently proposed two novel and sophisticated solutions based on polynomial interpolation for this problem. The former is based on Birkoff interpolation from an unstructured set of points and derivative values, and the latter is based on bivariate Lagrange interpolation. Both schemes are perfect and ideal.

In this short paper, we present a much simpler scheme that achieves the same results.

2 Proposed HTSS Scheme

Let \mathbb{F} be a finite field and $s \in \mathbb{F}$ be the secret to be shared. The dealer generates a random polynomial $P \in \mathbb{F}[x]$ of degree $k_m - 1$,

$$P(x) = \sum_{j=0}^{k_m-1} a_j x^j,$$

such that $s = a_0 + a_1 + \dots + a_{k_m-1} = P(1)$. The polynomials P_i , $1 \leq i \leq m$, are the truncated versions of $P(x)$ for compartment \mathcal{U}_i , defined as,

$$P_i(x) = \sum_{j=0}^{k_m-1-k_{i-1}} a_j x^j,$$

where we take $k_0 = 0$ for P_1 .

Each member u is given a different point $x_u \neq 1$ and a secret share $P_i(x_u)$, where i denotes his compartment number.

For a user $u \in \mathcal{U}_i$, his share gives a linear equation for the lowest degree $k_m - k_{i-1}$ coefficients of P but carries no information on the highest degree k_{i-1} coefficients.

3 Concluding Remarks

If it is desired to have a_0 as the secret, which is more common in Shamir-based secret sharing variants [4], the polynomial P can be truncated beginning from the lowest degree coefficients. In this case, the polynomial for the i th compartment will be

$$P_i(x) = \sum_{j=k_{i-1}}^{k_m-1} a_j x^j.$$

Each user u will be given a point $(x_u, P_i(x_u))$ for some $x_u \neq 0$.

Note that, for a moderately large field \mathbb{F} , the resulting matrices will be non-singular with an overwhelming probability, and the proposed scheme will be ideal and perfect.

Furthermore, the proposed scheme can easily be integrated with function sharing schemes (e.g., [5, 2, 1]) as the secret is reconstructed as the solution of a linear system of equations.

4 Epilogue

When the original manuscript was published on the Cryptology ePrint Archive, we received a number of constructive comments from our colleagues. Most importantly, it was pointed out that a scheme very similar to ours was previously published in [3]. It was also stated that the main advantage of the schemes in [6,

7] was their efficiency in certain aspects, such as the size of the finite field to be used or the number of determinants to be computed in order to check that a particular choice of vectors realizes the access structure. We would like to point out these facts here.

Acknowledgment

We would like to thank Murat Ak for helpful discussions, and to Javier Herranz, Svetla Nikova, and an anonymous Journal of Cryptology referee for their constructive feedback on an earlier version of this paper.

References

1. I. N. Bozkurt, K. Kaya, and A. A. Selcuk. Practical threshold signatures with linear secret sharing schemes. In *Proc. of AFRICACRYPT 2009*, volume 5580 of *LNCS*, pages 167–178. Springer-Verlag, 2009.
2. J. Herranz, C. Padro, and G. Saez. Distributed RSA signature schemes for general access structures. In *Proc. of ISC 2003*, volume 2851 of *LNCS*, pages 122–136. Springer-Verlag, 2003.
3. E. Kasper, V. Nikov, and S. Nikova. Strongly multiplicative hierarchical threshold secret sharing. In *2nd International Conference on Information Theoretic Security – ICITS 2007*, 2007.
4. A. Shamir. How to share a secret? *Communications of ACM*, 22(11):612–613, 1979.
5. V. Shoup. Practical threshold signatures. In *Proc. of EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 207–220. Springer-Verlag, 2000.
6. T. Tassa. Hierarchical threshold secret sharing. *Journal of Cryptology*, 20(2):237–264, 2007.
7. T. Tassa and N. Dyn. Multipartite secret sharing by bivariate interpolation. *Journal of Cryptology*, 22(2):227–258, 2009.