On Hierarchical Threshold Secret Sharing

Ali Aydın Selçuk[1], Kerem Kaşkaloğlu[2], and Ferruh Özbudak[3]

[1] Department of Computer Engineering
Bilkent University, 06800, Ankara, Turkey
selcuk@cs.bilkent.edu.tr
[2] Department of Mathematics
Atilim 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 which is also perfect and ideal.

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*),

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

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

$$0 < k_1 < \ldots < k_m$$

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

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

A detailed discussion of this problem and a comprehensive survey of related results can be found in [4, 5].

Tassa [4] and Tassa and Dyn [5] 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 $k_m - 1$,

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

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

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

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. Hence, a user set is authorized iff it satisfies the condition in (1).

3 Concluding Remarks

If it is desired to have a_0 as the secret, which is more common in Shamir-based secret sharing variants [2], the polynomial P can be truncated beginning from the lowest degree coefficients. In this case, the polynomial for the ith compartment will be

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

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

Note that the proposed schemes are ideal and perfect.

Furthermore, they can easily be integrated with function sharing schemes (e.g., [3, 1]) as the secret is reconstructed as the solution of a linear system of equations.

Acknowledgment

We would like to thank Murat Ak for a helpful discussion.

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. A. Shamir. How to share a secret? *Communications of ACM*, 22(11):612–613, 1979.
3. V. Shoup. Practical threshold signatures. In *Proc. of EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 207–220. Springer-Verlag, 2000.
4. T. Tassa. Hierarchical threshold secret sharing. *Journal of Cryptology*, 20(2):237–264, 2007.
5. T. Tassa and N. Dyn. Multipartite secret sharing by bivariate interpolation. *Journal of Cryptology*, 22(2):227–258, 2009.