Fundamentals of Contemporary Mathematical Sciences
(**2021**) **2**(2) 121 – 126

A Key Agreement Protocol Involving the Taylor Polynomials of Differentiable Functions

Abdullah Çağman *
Ağrı İbrahim Çeçen University, Faculty of Arts and Sciences, Department of Mathematics
Ağrı, Türkiye

Received: 05 June 2021 **Accepted:** 26 July 2021

Abstract: In this paper, we designed a new key agreement protocol based on some properties of Taylor polynomials. The security of our protocol is based on modular arithmetic used in some steps.

Keywords: Key agreement protocol, Taylor polynomial, cryptography.

1. Introduction

Key agreement, a protocol that enables two or more parties to create a secret key together over an unprotected channel. Key agreement schemes can be divided into two categories based on private keys and public keys. Consider an n-user network. In a private key-based key agreement scheme, it is a requirement that each user stores n-1 secret keys. On the other hand, this requirement is reduced to only one pair of public and private keys. This indicates that public key-based key agreement is more useful. More details can be found in [9].

The first work on the key agreement scheme was done by Merkle in 1978 [5]. However, in 1976, [3] is the first article published on this subject in the literature. This is because the study of Merkle submitted in 1975 was in a lengthy evaluation process.

The Diffie-Hellman key agreement scheme uses the commutativity property provided by cyclic groups. In this scheme, the associativity property of group axioms is used in the generation of a common secret key, and the cyclicity of the group is used in making it difficult to find this secret key by an adversary.

After this study, many studies on key agreement protocols have been published in the literature like [2, 6–8].

In this paper, a new key agreement scheme is constructed using the notions of Taylor polynomial.

*Correspondence: acagman@agri.edu.tr
2020 *AMS Mathematics Subject Classification*: 11T71, 41A58

2. Preliminaries

Let's give some information about the Taylor polynomials of differentiable functions from [1] and [4].

Definition 2.1 *Let f be a n times differentiable function at a. Its Taylor polynomial of degree n about a is given by*

$$P_{f,n,a}(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

The short-hand notation is

$$P_{f,n,a}(x) = \sum_{t=0}^{n} \frac{f^{(t)}(a)}{t!}(x-a)^k$$

where $f^{(0)} = f$.

Example 2.2 *Let $f = e^x$ and consider the Taylor polynomial of degree n of f about the point $a = 0$. Since $f^{(t)}(0) = 1$ for all t, then*

$$P_{f,n,0}(x) = \sum_{t=0}^{n} \frac{x^t}{t!} = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n!}.$$

The calculations related Taylor polynomials can be done easily with the help of the properties given below.

Proposition 2.3 *Let f, g be n-times differentiable at a. Then*

$$P_{f+g,n,a} = P_{f,n,a} + P_{g,n,a}.$$

Proposition 2.4 *Let f, g be n-times differentiable at a. Then*

$$P_{f\cdot g,n,a} = [P_{f,n,a} \cdot P_{g,n,a}]_n$$

where $[]_n$ stands for truncation at the n-th degree.

Proposition 2.5 *Let f be n-times differentiable at a and let g be n times differentiable at $f(a)$. Then*

$$P_{f\circ g,n,a} = \left[P_{g,n,f(a)} \circ P_{f,n,a}\right]_n.$$

3. Key Agreement Scheme

Let's assume that Alice and Bob must have a common secret key as shown in Figure 1 to communicate securely with each other.

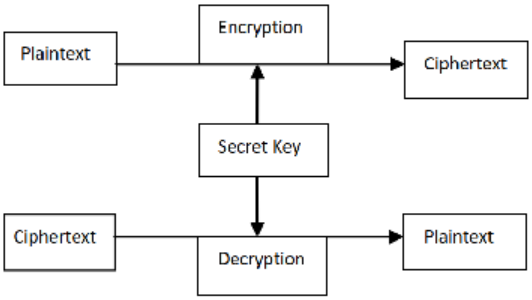

Figure 1: A communication diagram for Alice and Bob

In Table 1, they follow their steps to agree on a common secret key.

Table 1: Key agreement scheme

	Alice	Bob
1	They specify a real number a, a pair of (m,n) of positive integers, a polynomial $Q(x)$ whose degree is greater than $\max\{m,n\}$, and a positive integer N less than $\deg(Q(x))$ as public.	
2	Choose an function $f_A \in C^{m+n}$ secretly.	Choose an function $f_B \in C^{m+n}$ secretly.
3	Set $R_A(x) \coloneqq P_{f_A^{(m)},N,a}(x) \mod Q(x)$, and send it to Bob as public.	Set $R_B(x) \coloneqq P_{f_B^{(n)},N,a}(x) \mod Q(x)$, and send it to Alice as public.
4	Set $S_A(x) \coloneqq P_{f_A^{(m+n)},N,a}(x)$.	Set $S_B(x) \coloneqq P_{f_B^{(m+n)},N,a}(x)$.
5	Generate the secret key $K_A = \left(S_A(x) + R_B^{(m)}(x)\right) \mod Q(x)$.	Generate the secret key $K_B = \left(S_B(x) + R_A^{(n)}(x)\right) \mod Q(x)$.

In Table 1, C^k denotes the class of k-times differentiable functions, $P_{f,N,a}(x)$ denotes the N^{th}-order Taylor polynomial of a function $f(x)$ at a point a and $f^{(n)}(x)$ denotes the n^{th} derivative of the function $f(x)$.

In the first two step, they choose the public and private parameters. While Alice calculates the remainder of $P_{f_A^{(m)},N,a}(x)$ with respect to $Q(x)$ as public and sends it to Bob, Bob calculates the remainder of $P_{f_B^{(n)},N,a}(x)$ with respect to $Q(x)$ and sends it to Alice in the third step.

In the fourth step, they find the Taylor polynomial of the private function of their choice according to the $(m+n)$th derivative.

The last step shows how to generate the common secret key K by each of parties. They compute the remainder of the sum of the polynomial obtained in the previous step with the $R_B^{(m)}(x)$ with respect to $Q(x)$.

Let's examine the steps in the key agreement scheme on an example.

Example 3.1 *Alice and Bob set* $a = 3$, $m = 3$, $n = 5$,

$$\begin{aligned} Q(x) := &-0.401245x^{15} - 0.958083x^{14} + 0.290031x^{13} - 0.94719x^{12} \\ &- 0.690661x^{11} - 0.101595x^{10} - 0.741285x^{9} + 0.598951x^{8} \\ &- 0.957262x^{7} + 0.226571x^{6} + 0.731071x^{5} + 0.849086x^{4} \\ &+ 0.906984x^{3} + 0.0530527x^{2} - 0.816068x - 0.934274 \end{aligned}$$

and $N = 10$. *Let Alice and Bob choose* $f_A(x) = x\cos(x-1)$ *and* $f_B(x) = x\sin(x-1)$, *respectively.*

According to the above parameters, Alice evalulates

$$\begin{aligned} R_A(x) = &-1.67805 - 3.1556x + 0.999208x^{2} + 1.19371x^{3} - 0.392385x^{4} \\ &+ 0.0530208x^{5} - 0.0291861x^{6} + 0.00998872x^{7} \\ &- 0.00144603x^{8} + 0.0000939058x^{9} - 2.24256 * 10^{-}6x^{1}0 \end{aligned}$$

while Bob evalulates

$$\begin{aligned} R_B(x) = &-4.18312 + 3.15898x + 3.0712x^{2} - 0.83186x^{3} - 0.253275x^{4} \\ &+ 0.0230492x^{5} + 0.0171253x^{6} - 0.00133508x^{7} \\ &- 0.000484259x^{8} + 0.0000788666x^{9} - 3.41463 * 10^{-}6x^{1}0. \end{aligned}$$

They send them to each other. Then they calculate

$$\begin{aligned} S_A(x) = &-6.70518 + 4.77233x + 4.34389x^{2} - 1.10995x^{3} - 0.355256x^{4} \\ &+ 0.0362842x^{5} + 0.0201998x^{6} - 0.00139018x^{7} \\ &- 0.000628165x^{8} + 0.0000979783x^{9} - 4.16637 * 10^{-}6x^{1}0 \end{aligned}$$

and

$$\begin{aligned} S_B(x) = &-4.40082 - 7.28505x + 2.22036x^{2} + 2.02407x^{3} - 0.590457x^{4} \\ &+ 0.0573881x^{5} - 0.0382967x^{6} + 0.0137653x^{7} \\ &- 0.00196493x^{8} + 0.000123637x^{9} - 2.81595 * 10^{-}6x^{1}0. \end{aligned}$$

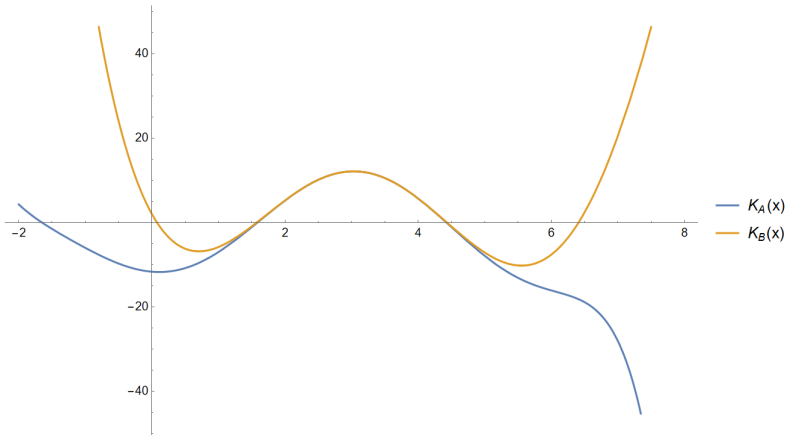

Figure 2: Graphs of key functions K_A and K_B

In the final step, they produce

$$K_A(x) = -11.6963 - 1.30627x + 5.72684x^2 + 0.945084x^3 - 0.635622x^4 - 0.126427x^5 + 0.0599485x^6 - 0.00384871x^7 - 0.000628165x^8 + 0.0000979783x^9 - 4.16637 * 10^-6x^10$$

and

$$K_B(x) = 1.96168 - 28.299x + 27.3919x^2 - 7.69326x^3 + 0.829398x^4 - 0.0104269x^5 - 0.0382967x^6 + 0.0137653x^7 - 0.00196493x^8 + 0.000123637x^9 - 2.81595 * 10^-6x^10.$$

K_A and K_B are distinct key functions but they have almost same graph around the point $a = 3$ as Figure 2.

Since the images of a certain point around $a = 3$ under the key functions K_A and K_B will be almost the same, the common key obtained by taking the digit of these images with a certain precision can be used by Alice and Bob in communication.

4. Conclusion

In this paper, we give a new key agreement protocol based on sum property of Taylor polynomials stated in Proposition 2.3. In this direction, using Proposition 2.4 and Proposition 2.5, similar protocols may be designed in the future works.

Acknowledgments

We would like to thank the anonymous reviewers for their suggestions which helped to improve our article.

References

[1] Arfken G.B., Weber H.J., Harris F.E., Mathematical Methods for Physicists, Elsevier, 2013.

[2] Çağman A., Polat K., Taş S., *A key agreement protocol based on group actions*, Numerical Methods for Partial Differential Equations, 37(2), 1112-1119, 2021.

[3] Diffie W., Hellman M., *New directions in cryptography*, IEEE Transactions on Information Theory, 22(6), 644-654, 1976.

[4] Hughes-Hallett D., Gleason A.M., McCallum W.G., et al., Calculus: Single and Multivariable, John Wiley and Sons, 2017.

[5] Merkle R.C., *Secure communications over insecure channels*, Communications of the ACM, 21(4), 294-299, 1978.

[6] Partala J., *Algebraic generalization of Diffie-Hellman key exchange*, Journal of Mathematical Cryptology, 12(1), 1-21, 2018.

[7] Polat K., *On key exchange method via topological concepts*, TWMS Journal of Applied and Engineering Mathematics, 9(1), 151-158, 2019.

[8] Polat K., *An application of interior and closure in general topology: A key agreement protocol*, Turkish Journal of Science, 6(1), 45-49, 2021.

[9] Stinson D.R., Cryptography: Theory and Practice, Chapman and Hall / CRC, 2005.