TURKISH JOURNAL OF SCIENCE
VOLUME 6, ISSUE 1, 45–49
ISSN: 2587–0971

http:/dergipark.gov.tr/tjos

An Application of Interior and Closure in General Topology: A Key Agreement Protocol

Kadirhan POLAT[a]

[a]*Department of Mathematics, Faculty of Science and Letter, Ağrıİbrahim Çeçen University, 04100, Ağrı, Turkey*

Abstract. In this paper, a new key agreement scheme is constructed using the notions of the interior of a set, the closure of a set, open function, closed function, continuous function in topological spaces. An implementation of this scheme is presented between the two parties and it is shown that they generate the common secret key.

1. Introduction

Key agreement, a protocol that enables two or more parties to create a secret key together over an unprotected channel, does not require an active role of the trusted authority, unlike most other key distribution techniques. Key agreement schemes can be divided into two categories based on private keys and based on public keys. Consider a n-user network. In a secret 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 in a key agreement scheme based public key. This indicates that public key-based key agreement is more useful. (see [1] for details).

The first work on the key agreement scheme was done by Merkle [2] in 1978. However, the article published by Diffie, Merkle's doctoral advisor, and Helmman [3] in 1976 is the first article published on this subject in the literature. This is because the study 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.

In 2017, Partala [4] published a study based on the computation of homomorphic images, which included an algebraically generalized Diffie-Hellman key-agreement scheme. The security of this scheme lies in the difficulty of solving the homomorphic image problem. This problem is the problem of computing the image of a given group element under an indefinite homomorphism.

Çağman et al. [5] introduced a key agreement scheme based on a group action of special orthogonal group on the complex projective line whose elements are 2×2 matrices with real entries.

In this paper, a new key agreement scheme is constructed using the notions of interior and closure in topological spaces.

Corresponding author: KP mail address: kadirhanpolat@agri.edu.tr ORCID:0000-0002-3460-2021
Received: 11 March 2021; Accepted: 27 April 2021; Published: 30 April 2021
Keywords. closure, interior, cryptography, key agreement
2010 *Mathematics Subject Classification*. 54A99; 94A60
Cited this article as: Polat K. An Application of Interior and Closure in General Topology: A Key Agreement Protocol. Turkish Journal of Science. 2021, 6(1), 45-49.

2. Preliminaries

Let's give some information about the general topology from [6–8].

Definition 2.1. *Let* (X, τ) *be a topological space and* $A \subseteq X$.

1. A point $x \in A$ is called *an interior point of* A if there exists an open set G such that $x \in G \subseteq X$. The set of all interior point of A, denoted by $\mathrm{Int}(A)$, is called *the interior of* A.
2. A point $x \in X$ is called *an closure point of* A if every open set containing x contains at least one point of A. The set of all closure point of A, denoted by $\mathrm{Cl}(A)$, is called *the closure of* A.

Proposition 2.2. *Let* (X, τ) *be a topological space. For every pair of subsets* A, B *of* X, *the followings hold:*

1. $\mathrm{Int}(A \cap B) = \mathrm{Int}\, A \cap \mathrm{Int}\, B$,
2. $\mathrm{Cl}(A \cup B) = \mathrm{Cl}\, A \cup \mathrm{Cl}\, B$.

Definition 2.3. *Let* (X, τ_X) *and* (Y, τ_Y) *be topological spaces,* $f : X \to Y$ *a function and let* $x \in X$.

1. f is called *a continuous function at the point* x if, for every τ_Y-open set V containing $f(x)$, $f^{-1}(V)$ is a τ_X-open set. f is called *a continuous function* if f is continous at every point of X.
2. f is called *an open function at the point* x if, for every τ_X-open set U containing x, $f(U)$ is a τ_Y-open set. f is called *an open function* if f is open at every point of X.
3. f is called *an closed function at the point* x if, for every τ_X-closed set U containing x, $f(U)$ is a τ_Y-closed set. f is called *a closed function* if f is closed at every point of X.

Proposition 2.4. *Let* (X, τ) *be a topological space,* $f : X \to Y$ *a function. The followings hold.*

1. If f is continuous, then $f(\mathrm{Cl}(A)) \subseteq \mathrm{Cl}(f(A))$ for every subset A of X.
2. If f is injective and continuous, then $\mathrm{Int}(f(A)) \subseteq f(\mathrm{Int}(A))$ for every subset A of X.
3. If f is open, then $f(\mathrm{Int}(A)) \subseteq \mathrm{Int}(f(A))$ for every subset A of X.
4. If f is closed, then $\mathrm{Cl}(f(A)) \subseteq f(\mathrm{Cl}(A))$ for every subset A of X.

3. Key Agreement Scheme

Let's assume that Alice and Bob must have a common secret key as shown in Figure 3 to communicate securely with each other.

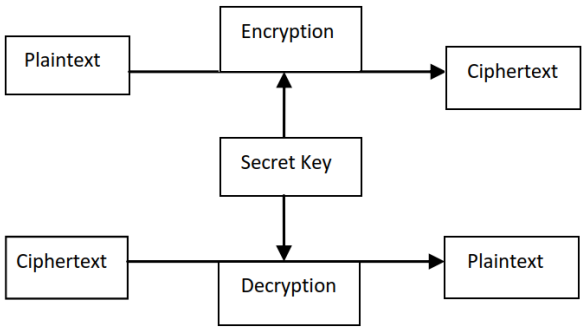

Figure 1: A communication diagram for Alice and Bob

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

Step	Alice	Bob
1	They specify arbitrary positive integers n, m as public.	
2	Choose an arbitrary topological space (X, τ_X) publicly such that $\lvert X\rvert = n$.	Choose an arbitrary topological space (Y, τ_Y) publicly such that $\lvert Y\rvert = n$.
3	They choose an arbitrary pair of m-tuples $A = (A_1, A_2, \ldots, A_m)$ and $B = (B_1, B_2, \ldots, B_m)$ whose components are subsets of X as public.	
4	Set f and g secretly as m-tuples $(f_k)_{k\leq m}$ and $(g_k)_{k\leq m}$, respectiveley, where each f_k is an injective, open and continuous functions from X to Y, and each g_k is a closed and continuous functions from X to Y.	Let G and F be m-tuples whose the general terms are $G_k = \mathrm{Int}_{\tau_Y}(A_k \cap B_k)$ and $F_k = \mathrm{Cl}_{\tau_Y}(A_k \cup B_k)$, respectively.
5	Set the m-tuples $f[A], g[A], f[B], g[B]$ whose the general terms are $f[A]_k = f_k(A_k)$, $f[B]_k = f_k(B_k)$, $g[A]_k = g_k(A_k)$, $g[B]_k = g_k(B_k)$, respectively, and send them to Bob as public.	Send m-tuples G and F to Alice.
6	By using m-tuples G and F, generate the secret key as the pair $K = (K^{\mathrm{Int}}, K^{\mathrm{Cl}})$ where K^{Int} and K^{Cl} are the m-tuples whose the general terms are $K_k^{\mathrm{Int}} = f_k(G_k)$ and $K_k^{\mathrm{Cl}} = g_k(F_k)$, respectively.	By using m-tuples $f[A]$, $g[A]$, $f[B]$ and $g[B]$, generate the secret key as the pair $K = (K^{\mathrm{Int}}, K^{\mathrm{Cl}})$ where K^{Int} and K^{Cl} are the m-tuples whose the general terms are $K_k^{\mathrm{Int}} = \mathrm{Int}_{\tau_Y}(f[A]_k \cap f[B]_k)$ and $K_k^{\mathrm{Cl}} = \mathrm{Cl}_{\tau_Y}(g[A]_k \cup g[B]_k)$, respectively.

Table 1: Key agreement scheme

In the first step, the sizes of the topologies and the tuples to be created are fixed, say n and m, respectively. In the next step, Alice chooses an arbitrary topology on an X set with n elements as public, while Bob chooses an arbitrary topology on a Y set with the same number of elements as public. In the third step, They together arbitrarily choose a pair of m-tuples whose components are subsets of X.

In the next two steps, Alice secretly and arbitrarily chooses an m-tuple f whose components are injective, open and continuous functions from X to Y, and an m-tuple g whose components are closed and continuous from X to Y, and then send m-tuples $f[A], g[A], f[B], g[B]$ to Bob whose the general terms are

$$f[A]_k = f_k(A_k), f[B]_k = f_k(B_k), g[A]_k = g_k(A_k), g[B]_k = g_k(B_k)$$

while Bob set G and F as the m-tuples whose general terms are

$$G_k = \mathrm{Int}_{\tau_Y}(A_k \cap B_k) \text{ and } F_k = \mathrm{Cl}_{\tau_Y}(A_k \cup B_k)$$

, respectively, and sends them to Alice.

The last step shows how to generate the common secret key K by each of parties. Alice computes two components of K as m-tuples with the general terms $f_k(G_k)$ and $g_k(F_k)$, respectively while Bob computes two components of K as m-tuples with the general terms

$$\mathrm{Int}_{\tau_Y}(f[A]_k \cap f[B]_k) \text{ and } \mathrm{Cl}_{\tau_Y}(g[A]_k \cup g[B]_k)$$

, respectively.

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

Example 3.1. *Alice and Bob set $n = 4$ and $m = 3$. Then, Alice set $X = \{a, b, c, d\}$ while Bob $Y = \{1, 2, 3, 4\}$. Alice and Bob set*

$$\tau_X = \{\emptyset, \{a\}, \{c\}, \{d\}, \{a, c\}, \{a, d\}, \{b, c\}, \{c, d\}, \{a, b, c\}, \{a, c, d\}, \{b, c, d\}, X\}$$

and

$$\tau_Y = \{\emptyset, \{1\}, \{2\}, \{4\}, \{1,2\}, \{1,4\}, \{2,4\}, \{3,4\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, Y\},$$

respectively. Then, They set two 3-tuples $A = (A_1, A_2, A_3)$ *and* $B = (B_1, B_2, B_3)$ *where*

$$A_1 = \emptyset, \quad A_2 = \{c\}, \quad A_3 = \{a, d\},$$
$$B_1 = \{b, c\}, \quad B_2 = \{b, c\}, \quad B_3 = \{a, c, d\}.$$

Alice sets $f = (f_1, f_2, f_3)$*, each component of which is an injective, open and continuous function from* X *to* Y *where*

$$a \overset{f_1}{\mapsto} 1, b \overset{f_1}{\mapsto} 3, c \overset{f_1}{\mapsto} 4, d \overset{f_1}{\mapsto} 2,$$
$$a \overset{f_2}{\mapsto} 1, b \overset{f_2}{\mapsto} 3, c \overset{f_2}{\mapsto} 4, d \overset{f_2}{\mapsto} 2,$$
$$a \overset{f_3}{\mapsto} 1, b \overset{f_3}{\mapsto} 3, c \overset{f_3}{\mapsto} 4, d \overset{f_3}{\mapsto} 2,$$

and $g = (g_1, g_2, g_3)$*, each component of which is a closed and continuous function from* X *to* Y *where*

$$a \overset{g_1}{\mapsto} 1, b \overset{g_1}{\mapsto} 1, c \overset{g_1}{\mapsto} 1, d \overset{g_1}{\mapsto} 1,$$
$$a \overset{g_2}{\mapsto} 2, b \overset{g_2}{\mapsto} 2, c \overset{g_2}{\mapsto} 2, d \overset{g_2}{\mapsto} 3,$$
$$a \overset{g_3}{\mapsto} 3, b \overset{g_3}{\mapsto} 1, c \overset{g_3}{\mapsto} 1, d \overset{g_3}{\mapsto} 3.$$

Then, Alice computes m-tuples $f[A], g[A], f[B], g[B]$ *whose the general terms are* $f[A]_k = f_k(A_k)$*,* $f[B]_k = f_k(B_k)$*,* $g[A]_k = g_k(A_k)$*,* $g[B]_k = g_k(B_k)$*, respectively, as*

$$f[A] = (\emptyset, \{4\}, \{1,2\}),$$
$$g[A] = (\emptyset, \{2\}, \{3\}),$$
$$f[B] = (\{3,4\}, \{3,4\}, \{1,2,4\}),$$
$$g[B] = (\{1\}, \{2\}, \{1,3\}),$$

and send them to Bob while Bob computes m-tuples G *and* F *whose the general terms are* $G_k = \mathrm{Int}_{\tau_Y}(A_k \cap B_k)$ *and* $F_k = \mathrm{Cl}_{\tau_Y}(A_k \cup B_k)$*, respectively, as*

$$G = (\emptyset, \{c\}, \{a, d\}),$$
$$F = (\{b, c\}, \{b, c\}, X),$$

and send them to Alice.

Using m-tuples G *and* F*, Alice computes the secret common key* $K = (K^{\mathrm{Int}}, K^{\mathrm{Cl}})$ *whose general terms of components are* $K_k^{\mathrm{Int}} = f_k(G_k)$ *and* $K_k^{\mathrm{Cl}} = g_k(F_k)$*, respectively, as*

$$K = ((\emptyset, \{4\}, \{1,2\}), (\{1\}, \{2\}, \{1,3\})).$$

On the other hand, by using m-tuples $f[A]$*,* $g[A]$*,* $f[B]$ *and* $g[B]$*, Bob computes the secret common key* $K = (K^{\mathrm{Int}}, K^{\mathrm{Cl}})$ *whose the general terms of components are* $K_k^{\mathrm{Int}} = \mathrm{Int}_{\tau_Y}(f[A]_k \cap f[B]_k)$ *and* $K_k^{\mathrm{Cl}} = \mathrm{Cl}_{\tau_Y}(g[A]_k \cup g[B]_k)$*, respectively, as*

$$K = ((\emptyset, \{4\}, \{1,2\}), (\{1\}, \{2\}, \{1,3\})).$$

Thus Alice and Bob have produced the same public key K *to use in communication.*

References

[1] Douglas R Stinson. *Cryptography: theory and practice*. Chapman and Hall/CRC, 2005.
[2] Ralph C Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, 1978.
[3] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.
[4] Juha Partala. Algebraic generalization of diffie–hellman key exchange. *Journal of Mathematical Cryptology*, 12(1):1–21, 2018.
[5] Abdullah Çağman, Kadirhan Polat, and Sait Taş. A key agreement protocol based on group actions. *Numerical Methods for Partial Differential Equations*, 37(2):1112–1119, 2021.
[6] Colin Conrad Adams and Robert David Franzosa. *Introduction to topology: pure and applied*. Pearson Prentice Hall Upper Saddle River, 2008.
[7] John L Kelley. *General topology*. Courier Dover Publications, 2017.
[8] James Munkres. *Topology: Pearson New International Edition*. Pearson, 2013.