ISSN:2231-0711
www.ijcset.net

2D Key Exchange Scheme Using Morphological Dilation

Priya Nandihal and Bhaskara Rao.N

Dayananda Sagar College of Engineering, Bangalore. India.
bhaskararao.nadahalli@gmail.com

Abstract— **A new scheme for Diffie-Hellman type key exchange is presented. This method uses morphological dilation process to provide secure exchange of a 2D key between two users.**

Keywords— **2D key, key exchange, morphological dilation, imge as a key.**

I. INTRODUCTION

Diffie-Hellman [1] algorithm is the most popular secret key exchange scheme between two users. In the literature, semigroup and matrix based versions of Diffie-Hellman type key exchange schemes have been proposed [2],[3],[4]. In this paper, digital image processing techniques are used to provide the secret shared key exchange.

II. ENTITIES AND THE PROCESS OF THE PROPOSED SCHEME

All the entities participating in the scheme are binary matrices whose elements are 0's and 1's. They in turn represent corresponding black/white images which are processed to get the desired result.

A. *Symbols and Terms*

Alice and Bob are the two users communicating over an unsecured channel, who wants to exchange a secret key.

1) Private Keys: P and Q are the private keys of Alice and Bob respectively. P and Q are binary matrices of equal size mxn. Alice can choose her own P and Bob can choose his own Q. The matrices P and Q are independent of each other.

2) Base Matrix: G is the base binary matrix known to both Alice and Bob. It is in the public domain. The size hxk of G is relatively large compared to that of P or Q. (The reason for the large size of G is explained later.) Base matrix G is used to generate the public keys of Alice and Bob.

3) Public Keys: Binary matrices R and T are the public keys of Alice and Bob respectively. The sizes of R and T are same as that of G. That is hxk. R is generated using G and P while T is generated using G and Q.

4) Shared Secret Key: Binary matrix S is the shared secret key. Size of S is also hxk same as those of R and T.

B. *Main Process*

The main process used in this scheme is the Morphological Dilation [5]. Dilation thickens or expands the shape of the objects in the image. The shape and the nature of expansion depend on the *Structuring Element* used for dilation. Essentially it is a set union operation.

1) Definition of Dilation: Let C be the given binary image to be dilated by the structuring element D which is also a given binary image. Dilation is defined in terms of the corresponding sets as follows.

Here, the (x,y) co-ordinates of all the white pixels of the given image are the members of the corresponding set. The members belong to the integer space Z^2. Let the images C and D be represented by their sets designated by C and D respectively. Sets C and D are points in the 2D Eucledian space. Let c∈C and d∈D where c and d are the members of C and D respectively. The members are 2-tuples. Then the dilation is defined as [5],

$$C \oplus D = \{w \in Z^2 | w = c + d \text{ for } c \in C \text{ and } d \in D\} \quad (1)$$

The symbol ⊕ is used as the dilation operator. The dilation operation is also called the Minkowski addition [6] of the two sets. Another definition which gives the same result is [6],

$$C \oplus D = \bigcup_{d \in D} C_d = \bigcup_{c \in C} D_c \quad (2)$$

Here, C_d is the translation of set C by d and similarly, D_c is the translation of set D by c. Let us agree to write the translation of set C by d as,

$$C_d = C+d = \text{set } \{c+d \mid c \in C\}$$

and

$$D_c = D+c = \text{set } \{d+c \mid d \in D\}$$

2) Properties of Binary dilation: It is associative. This property is evident from the definition of dilation given by Eq.(1). Thus for any three sets C, D and E in Z^2, associative property yields,

$$(C \oplus D) \oplus E = C \oplus (D \oplus E) \quad (3)$$

It is commutative. Because of the additive nature of dilation, for any two sets, the commutative property yields,

$$(C \oplus D) = (D \oplus C) \quad (4)$$

But from the image processing perspective, the commutative property is conditional. In the morphological image dilation process, the size of the image after dilation is maintained same irrespective of the size of the structuring element. In this paper, we use the *imdilate* function from the Matlab Image Processing Toolbox. Let C be the binary image dilated by D which is called the structuring element. D is also a binary

image (binary matrix). Then the image processing dilation operation [7] is expressed as,

$$F = \text{imdilate}(C,D) \quad (5)$$

Here, F is the result of dilation. Even though the above function uses the definition of Eq.(1) for dilation, those output members of the result of Eq.(1), which fall outside the co-ordinate ranges of C are not included in F. This is called the 'same' size dilation opposed to the 'full' size one. In the proposed method, we use 'same' size dilation. Thus, the size of F is kept same as that of C. The size of F does not depend on the size of D. Now, consider the function G = imdilate(D,C) where the function arguments are interchanged. Then, the size of G would be that of D. Therefore if the sizes of C and D are equal, then the two results F and G would be equal. Hence when the sizes of C and D are equal, imdilate(C,D) is equal to imdilate(D,C) and the dilation operation is commutative. *Thus, for the imdilate function to be commutative, sizes of its two arguments should be same.*

III. COMMON SECRET KEY EXCHANGE

We use function imdilate along with private keys P, Q and base matrix G as described in section II, to exchange the secret key as follows.

1. User Alice choses her private key P.
2. Alice's public key R is obtained as,

$$R = \text{imdilate}(G,P) = G \oplus P \quad (6)$$

3. R is sent to user Bob over the unsecured channel.
4. User Bob choses his private key Q.
5. Bob's public key T is obtained as,

$$T = \text{imdilate}(G,Q) = G \oplus Q \quad (7)$$

6. T is sent to user Alice over the unsecured channel.
7. User Bob, having received R, generates the secret key S_B as,

$$S_B = \text{imdilate}(R,Q) \quad (8)$$

8. User Alice, having received T, generates his secret key S_A as,

$$S_A = \text{imdilate}(T,P) = T \oplus P \quad (9)$$

Now, it can be shown that the common secret key for user Alice and Bob is $S = S_A = S_B$. Substituting for R from Eq.(6) in Eq.(8),

$$S_B = \text{imdilate}(\text{imdilate}(G,P),Q) = (G \oplus P) \oplus Q \quad (10)$$

From the associative property of imdilate, Eq.(10) becomes,

$$S_B = \text{imdilate}(G,\text{imdilate}(P,Q)) = G \oplus (P \oplus Q) \quad (11)$$

Similarly, from Eqs.(7) and (9),

$$S_A = \text{imdilate}(\text{imdilate}(G,Q),P) = (G \oplus Q) \oplus P \quad (12)$$

Again, using the associative property,

$$S_A = \text{imdilate}(G, \text{imdilate}(Q,P) = G \oplus (Q \oplus P) \quad (13)$$

Since the sizes of P and Q are same (equal to mxn), by the commutative property of dilation,

$$\text{imdilate}(P,Q) = \text{imdilate}(Q,P) = P \oplus Q = Q \oplus P \quad (14)$$

From Eqs.(11),(13) and (14),

$$S_A = S_B = G \oplus Q \oplus P = G \oplus P \oplus Q$$

Calling this as S, the shared secret key is,

$$S = S_A = S_B = G \oplus P \oplus Q \quad (15)$$

Thus S is a double dilated 2D binary image. The size of S is same as that of G.

IV. CRYPTANALYSIS OF THE PROPOSED METHOD

From the definition given by Eq.(2), dilation is basically the union of translated sets. Initially let us consider the union of set C with its translated copy C+d as,

$$E = C \cup (C+d) \quad (16)$$

A. *Unique Determination of C given E and d*

Consider the problem of uniquely determining C, given E and d. In Eq. (16), taking the translation of E by (–d), we get,

$$E-d = [C \cup (C+d)] - d = (C-d) \cup C \quad (17)$$

Taking the intersection of E and (E-d), From Eqs.(16) and (17),

$$E \cap (E-d) = [C \cup (C+d)] \cap [(C-d) \cup C]$$
$$= [C \cap C] \cup [C \cap (C+d)] \cup [C \cap (C-d)] \cup [(C+d) \cap (C-d)]$$

On simplification,

$$E \cap (E-d) = C \cup [(C+d) \cap (C-d)] \quad (18)$$

Case 1: $(C+d) \cap (C-d) = \Phi$ = null set (19)

Then, From Eqs.(18) and (19),

$$C = E \cap (E-d) \quad (20)$$

Thus C can be uniquely determined from Eq.(16) provided $(C+d) \cap (C-d) = \Phi$ (null set.)

Case 2: $(C+d) \cap (C-d)$ is a subset of C.

Then $C \cup [(C+d) \cap (C-d)] = C$ and Eq.(18) becomes $E \cap (E-d) = C$ and C can be obtained as $C = E \cap (E-d)$.

Thus, when $(C+d) \cap (C-d)$ is a subset of C including the null set Φ, C can be uniquely solved as given by Eq.(20).

Case 3: $(C+d) \cap (C-d)$ is non empty and not a subset of C.

Let $F = (C+d) \cap (C-d)$ (21)

From Eqs.(18) and (21),

$$E \cap (E-d) = C \cup F \quad (22)$$

Then $C \cup F$ is bigger than C and C cannot be recovered uniquely from $C \cup F$. Therefore from the knowledge of E and d, C cannot be determined uniquely. This can be demonstrated as follows.

Let H be a subset of $(C+d) \cap (C-d)$. That is,

$$H \subseteq (C+d) \cap (C-d) \quad (23)$$

Then,

$$H \subset (C+d) \quad (24)$$

and $$H \subset (C-d) \quad (25)$$

Eq.(25) can be rewritten as,

$$H+d \subset C \quad (26)$$

Consider the set $C \cup H$. Now, it can be shown that $C \cup H$ is also a solution of Eq.(16) when C is one of its solution. This is understood by examining the RHS of Eq.(16) after replacing C by $C \cup H$ as,

$$RHS = (C \cup H) \cup ((C \cup H) + d) \quad (27)$$

By using the distributive property,

$$(C \cup H) + d = (C+d) \cup (H+d) \quad (28)$$

From Eqs.(27) and (28),

$$RHS = C \cup H \cup (C+d) \cup (H+d) \quad (29)$$

Since $H \subset (C+d)$,

$$H \cup (C+d) = C+d \quad (30)$$

From Eq.(26), $H+d \subset C$, therefore,

$$(H+d) \cup C = C \quad (31)$$

From Eqs.(27),(29),(30) and (31),

$$RHS = (C \cup H) \cup ((C \cup H) + d) = C \cup (C+d) \quad (32)$$

From Eqs.(32) and (16), it can be concluded that $C \cup H$ is also a solution of Eq.(16) when C is its solution.

If $C \cup H$ is to be different from C, H should be non-empty and H should not be a subset of C. Since $H \subseteq (C+d) \cap (C-d)$ (see Eq.(23)), these conditions imply that $(C+d) \cap (C-d)$ should be non-empty and $(C+d) \cap (C-d)$ should not be a subset of C. That is,

$$(C+d) \cap (C-d) \neq \Phi \quad (33)$$

$$(C+d) \cap (C-d) \not\subset C \quad (34)$$

Thus, Eq.(16) has many solutions for C when conditions given by Eqs.(33) and (34) are satisfied. Under these conditions, it can be shown that C is a concave set as follows.

B. Concavity of set C

Let c_1, c_2, c_3, c_4, be the 4 corners of the outer boundary of a simple example set C represented by its Venn diagram as shown in Fig.1. Note that C belongs to the 2D Eucledian space. For convenience, the outer boundary of C is taken as a square and c_4 is taken as the origin. Set C+d is represented by the north east translated set enclosed by u_1, u_2, u_3, u_4 as shown in Fig. 1. d is taken as a 45 degree (north-east pointing) vector. Similarly, C–d is represented by the southwest translated set v_1, v_2, v_3, v_4. Here,

$$c_4 + d = u_4 \quad (35)$$

$$c_2 - d = v_2. \quad (36)$$

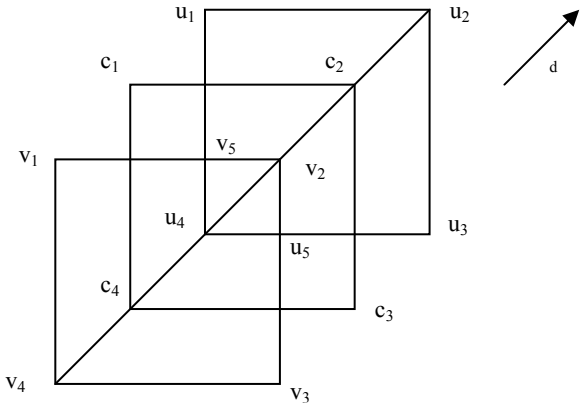


Fig. 1. Set C, C+d and C–d.

The intersection of set (C+d) represented by u_1, u_2, u_3, u_4 with set (C-d) represented by v_1, v_2, v_3, v_4 is given by the over-lapping region v_5, v_2, u_5, u_4 (see Fig. 1). For the existence of this region, v_2 should be on the north-east side of u_4. Measuring the length along the direction of d (north-east), the above condition means c_4v_2 should be greater than c_4u_4, that is,

$$c_4v_2 > c_4u_4 \quad (37)$$

Since, c_4 is taken as the origin, the above condition becomes

$$v_2 > u_4 \quad (38)$$

Eq.(38) gives the condition for $(C+d) \cap (C-d)$ to be non-empty.

From Eq.(35) ,

$$u_4 > c_4 \quad (39)$$

and from Eq.(36),

$$c_2 > v_2 \quad (40)$$

From Eqs. (40), (38) and (39),

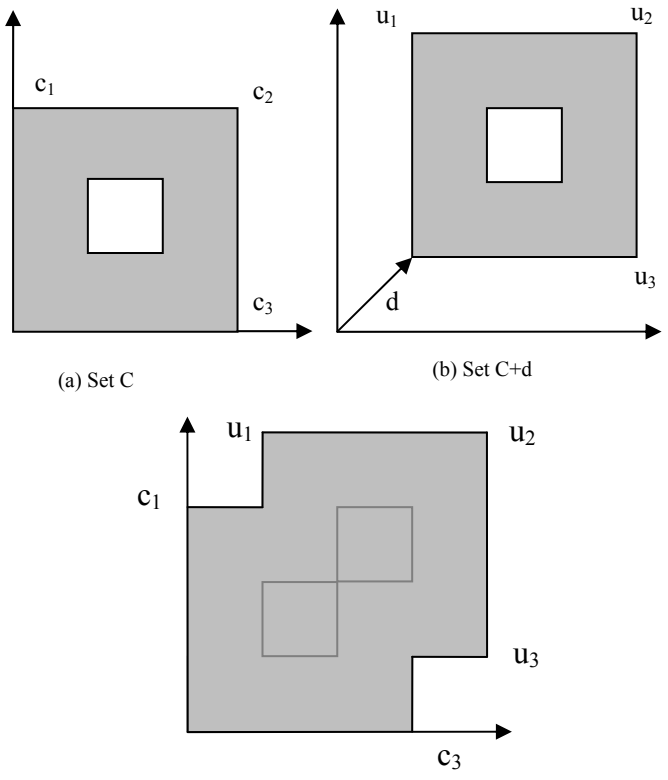
$$c_2 > v_2 > u_4 > c_4 \quad (41)$$

This means, v_2 and u_4 are the interior points on c_2c_4.

Now consider the condition given by Eq.(34) which is reproduced here,

$$(C+d) \cap (C-d) \not\subset C \quad (34)$$

In the example of Fig. 1, $(C+d) \cap (C-d)$ is represented by the square v_5, v_2, u_5, u_4. This square should not be a sub set of C if Eq.(34) is to be satisfied. This means set C should not include this square. Under this condition, the line segment u_4v_2 of c_4c_2 does not belong to C. Therefore set C is concave when conditions given by Eqs.(33) and (34) are satisfied. Such a C is shown in shaded gray in Fig. 2 (a) and the corresponding translated set C+d is shown in Fig. 2 (b). The union $C \cup (C+d)$ is shown in Fig. 2 (c).



(a) Set C (b) Set C+d

(c) Union Set $C \cup (C+d)$

Fig. 2. Set C, displaced set C+d and their union

In the union C ∪ (C+d), the hole of C is covered by the south-west region of C+d and the hole of C+d is covered by the north-east region of C. Thus both the holes are covered by the union of C and C+d. In this way, the exact shape of C is lost in the union C ∪ (C+d).

In general, if set C is concave and for a suitable d, conditions of Eqs.(33) and (34) are satisfied. Then C cannot be uniquely solved using Eq.(16). The above argument can be extended when several translated sets form a union as given below,

$$E = C \cup (C+d_1) \cup (C+d_2) \cup \ldots \cup (C+d_N)$$

Or $$E = (C+d_1) \cup (C+d_2) \cup \ldots \cup (C+d_N) \quad (42)$$

Comparing the RHS of Eq.(42) with Eq.(2), Eq.(42) can be rewritten as,

$$E = C \oplus D \quad (43)$$

Here, E is the result of dilation (Minkowski sum). The knowledge of E and D cannot uniquely determine C.

C. Discovery of Private Keys by Outsiders

Now, consider the problem of uniquely determining the private key P of user Alice, by an outsider, from the knowledge of the base matrix G and Alice's public key R. That is Eq.(6) has to be solved for P. Eq.(6) is reproduced below for convenience.

$$R = \text{imdilate}(G,P) \quad (6)$$

In terms of the corresponding sets, the above equation can be written as,

$$R = P \oplus G \quad (44)$$

where G and P are the set of white pixel co-ordinates of images G and P respectively. The resulting set R represents the image R. In view of the earlier discussion, P cannot be uniquely determined from the knowledge of R and G when G is a concave set.

D. Brute force method for solving P

Here, all possible combinations of P are substituted in Eq.(44) one at a time until it is satisfied. Since P is a binary matrix of size (mxn), the total number of distinct combinations is $2^{(mxn)}$. Even for a moderate size of (mxn) = (32x32), this number becomes 2^{1024} which is really large. Thus the brute force method of discovering the key by an outsider is infeasible.

V. EXPERIMENTAL RESULTS

In the example discussed here, G is the binary base image of size 768x768. G is obtained by randomly distributing hallow white squares and solid black squares of size 24x24 to fill the size of G. The number of black squares is intentionally kept higher than that of white squares so that adequate black regions are available for the expansion of white regions during dilation. The image G is shown in Fig. 3. The border regions of G are purposefully made black so that the expanded white regions due to dilation do not get truncated. The white squares of G contain random sized black holes in them to have a higher degree of concavity. In this example, private keys P and Q are random matrices of size 9x9. Fig.4. shows the dilated image R=G⊕ P which is the public key of Alice. S=G⊕ P ⊕ Q is the common shared key. It is shown in Fig. 5. In the experiment, G ⊕ Q ⊕ P is found exactly equal to G⊕ P ⊕ Q . In general G can be any arbitrary binary image with reasonably large black regions distributed randomly. P and Q are binary matrices of equal size. This size is kept small compared to that of G so that the dilations of G by P and Q do not merge all the white regions of G into a single white region.

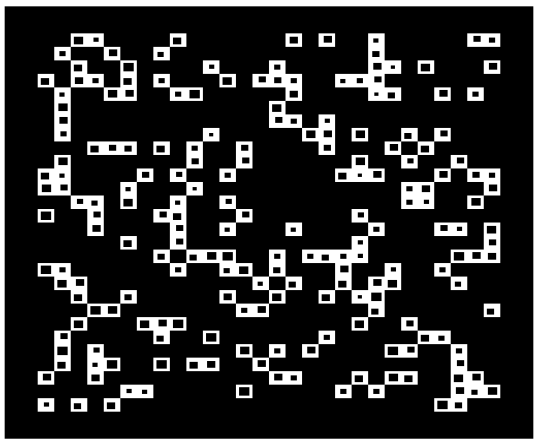


Fig. 3. Base Image G

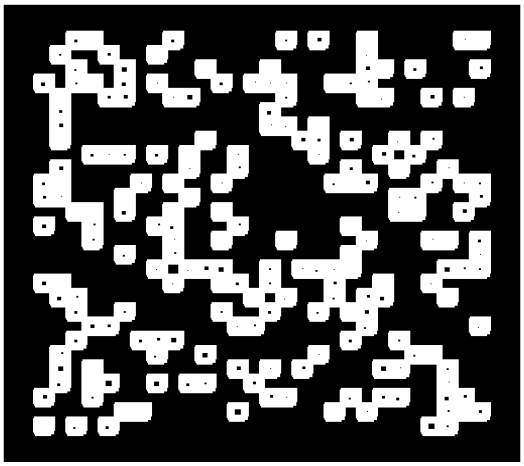


Fig. 4. Dilated Image R=G⊕ P

c

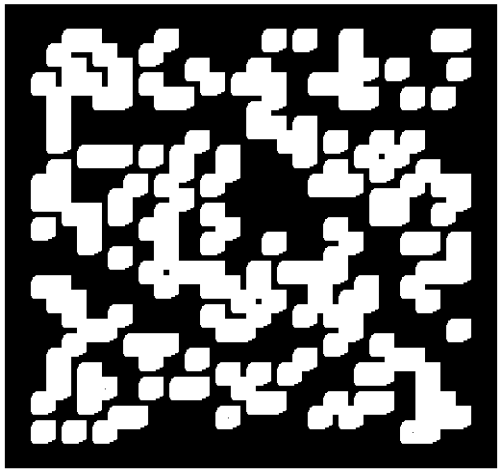


Fig. 5. Double Dilated Image S=G⊕ P ⊕ Q

VI. CONCLUSIONS

A new technique of generating Diffie-Hellman type 2D common keys is presented. The sizes of private keys P, Q and the base matrix G are easily scalable to large values. Then the consequent common secret key size also will be large so that the chances of key theft and discovery by unauthorized outsiders is very low. Since the secret key is 2D matrix, it can be used for encryption/decryption of document images and other block oriented data. The binary morphological operation *Erosion* also can be used instead of Dilation. Even though the method proposed here is computationally intensive, this technique opens up a new research area of 2D keys for further investigation.

REFERENCES

[1] William Stallings, Cryptography and Network Security Principles and Practices. Fourth Edition. Pearson Education. 2006.

[2] G. Maze, C. Monico and J. Rosenthal, "Public Key Cryptography based on semigroup actions", *Advances in Mathematics of communication.* Volume 1, No.4, 2007 pp 489-507.

[3] H. K. Pathak and Manju Sanghi, "Public key cryptosystem and a key exchange protocol using tools of non-abelian group ",/ (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 04, 2010, 1029-1033 .

[4] Benjamin Fine, Maggie Habeeb, Delaram Kahrobaei and Gerhard Rosenberger, "Aspects of Nonabelian Group Based Cryptography: A Survey and Open Problems ", arXiv/1103.4093v2 [cs.CR]. Cornell University Library . March 2011.

[5] R.C. Gonzalez and R.E. Woods, "Digital Image Processing", third Edition. Pearson Education. 2009. Chapter 9.

[6] From Wikipedia, the free encyclopedia. en.wikipedia.org/wiki /Dilation_ (morphology)

[7] imdilate, www.mathworks.com/help/toolbox/images/ref/imdilate.html