Chess Cryptosystem

Alexandru Miron GATEJ

Faculty of Mathematics and Computer Science, Bucharest University
Academiei 14, sector 1, 70109, Bucharest, ROMANIA
alexandrugatej@gmail.com

Abstract: In this paper we discuss about a cryptosystem based on chess automata. First we introduce the general notions about the chess games. After that we describe the chess automata that is the main tool for building the key. Finally we describe the operation for encryption process and decryption process, an with that we can present the algorithm.

Keywords: chess cryptosystem, chess automata, chess.

1. Introduction

The chess game is very old. There are a lot of legends about the creation of this game. It was a very popular game in the last century. We present some aspects of the game. The game it's played on a board with 64 square. The lines are numbered from 1 to 8 and the columns from A to H. Usually the square have black and white colour alternative. The only rule about the colours is that each player must have on right side a white square. Each player have 16 pieces: 8 pawns,2 knights,2 Bishops, 2 Rocks, 1 Queen, 1 King.

Position:

- Pawn - The pawns are placed on the second line for white ones and on the seventh line for black ones, each one on every line.
- Knight - The two knights are placed on the columns B and G of the first line (for white) and of the eighth line (for black).
- Bishop - The two bishops are placed on the columns C and F of the first line (for white) and of the eighth line (for black).
- Rock - The two rocks are placed on the columns A and H of the first line (for white) and of the eighth line (for black).
- Queen - The queen is placed on the column D of the first line (for white) and of the eighth line (for black). It is told that queen keeps the colour, meaning that if the queen has the white colour will be placed on a white square, same for black.
- King - The king is placed on the column E of the first line(for white) and of the eighth line (for black).

The movement of the pieces:

- Pawn - The pawn can be moved only forward, with the condition that the target square will not be occupied by another piece. It can be moved on the diagonal if target square is occupied by an opponent's piece, there by capturing it. If the pawn arrive on the last line of the board it can transform in any piece, with the exception of the king. There are some exceptions from the general rule. If the pawn is on it's initial square (2 or 7), it can move two squares forward instead of one. Another one is the move "en-passant" which means: If a pawn is on the first line of the opponent half side(line four for white and five for black), and an opponent pawn was moved with under the rule of 2 square on the next left or next right column, then it can capture this pawn and advance on the diagonal. The move can be done only after the advance of two squares by the opponent pawn.
- Knight - The knight is moving in a L shape in all the possible direction. It's moving 2 square on a column or line and after that it moving on the next left or next right column respectively line. It's the only piece that can jump across other pieces.

This is a post conference paper. Parts of this paper have been published in the Proceedings of the SECITC 2009 Conference (printed version).

ISSN 2067 – 4074

- Bishop - The bishop is moving on diagonal on which it stands[1].
- Rock - The rock is moving on vertical or horizontal any square it wants*.
- Queen - The Queen have also the moves of the bishop and the rock*.
- King - The King is moving only one square in any direction. It can be moved on a square that it's attacked by an opponent's piece. Also it can capture an opponent's piece if it is another piece who defend it. The are two special move for the king who invoke the rocks. In this situation the king goes 2 squares left or right (depend on the chosen rock). And after that the rock is transferred to the square near the king in the right if the king have been moved in the left direction and in the left if the king have been moved in right direction. Those moves can not be done if one of the next situation occurred: The king, or/and the rock involved have been moved; if the square on which the king stands, or the square which it must cross it's attacking or it's occupied by one or more opponent's pieces. Between the king and the rock it's a piece.

The initial configuration is:

Fig. 1

The notation of the moves:

The pieces it's noted by a character for every piece: Space -Pawn (example : d2d4); N-Night (example : Nc1c3); B-Bishop (example : Bc1d2); R-Rock (example : Ra1d1); Q-Queen(example : Qd8e7); K-King (example : Ka2a3), concatenate with the initial square and the destination square. The captures will not be noted like the FIDE recommendation [2]. It will be omitted. Kingside castling will be noted with 0-0 and queenside castling will be noted with 0-0-0. The "en-passant" move is like an usual move. If we have a pawn transformation we will note the same but we will add the symbol corresponding for the piece in what the pawn is transform : P-Pawn, N-Night, B-Bishop, R-Rock, Q-Queen (Example: a7-a8D).

Elements that are different from chess:

- The pawn from the second and seventh line, can move on the first or eighth line. We say in this case that the pawn doesn't transform.
- The Pawn from the first or eighth line can move on circularly.
- The Pawn from the first or eighth line can move forward on the second line and seventh line.
- The square who don't have a piece on it can be any colour (white or black in our case).

2. Problem Formulation

The algorithm consist of some ordinary operation like rotation, xor and add in Z_7. The keys for this algorithm is based on the complexity of the chess game. In fact will consider a configuration of chess board a word who will be encrypted using the operation enumerated later on this paper. A chess game will be a key.

3. Problem Solution

3.1 Key generation algorithm

3.1.1 Chess automata

Let C = (Q; V; q_0;δ ; F), be DFA like the one describe in [4]:

- V arbitrary alphabet
- Q set o states
- q_0 initial state, $q_0 \in Q$

[1] If in his way it's a piece it can not go across it, if this piece is an opponent's one it can take it place capturing it.

- δ transition function, δ:Q x V → Q
- F final states, F=Q

where:

V - The alphabet is described by the moves occurred in the chess game, (described in the "Introduction" section -> notation of the moves).
Q - The set of matrix 8 x 8 which can have 14 elements: pawn, knight, bishop, rock, queen, king or free square, that can be white or black colour.

q_0 - initial state that is the initial configuration of a board in chess game.

δ - Transition function that is in fact a move in chess game.

F - The final states F = Q

The cardinal of V

To calculate the cardinal of V it is not important the colour of pieces.
We will analyse based on the moves for a piece calculated considering their position on the board. We have the following cases:

- P For the pawn: 3,4,5,6,7; for the square a2, a7, h2, h7 ; a1,a8,h1,h8 ; b1, b8, c1, c8, d1, d8, e1, e8, f1, f8, g1, g8 it can move in 3 modes.(example a2: a1a2, a3a2, b3a2 and example a1: a2a1, a8a1, a8a1), for the square b2, b7, c2, c7, d2, d7, e2, e7, f2, f7, g2, g7 ; a3, a6, h3, h6 ; b1, b8, c1, c8, d1, d8, e1, e8, f1, f8, g1, g8 it can move in 4 modes (example b2: b1b2, a3b2, b3b2, c3b2 ; example a3: a2a3, a4a3, b2a3, b4a3 ; example b1: a2b1, b2b1, b8b1, c2b1), for the square a4, a5, h4, h5 it can move in 5 modes (example a4: a2a4, a3a4, a5a4), for the square b3, b6, c3, c6, d3, d6, e3, e6, f3, f6, g3, g6 it can move in 6 modes (example b3: a2b3, a4b3, b2b3, b4b3, c2b3, c4b3). For the squares b4, b5, c4, c5, d4, d5, e4, e5, f4, f5, g4, g5 it can move in 7 modes (example b4: a3b4, a5b4, b2b4, b3b4, b5b4, c3b4, c5b4) in total we have (4*3 + 4*3) + (12*4 + 12*4 + 4*4) + (4*5)+(12*6) + (12*7) = 312.
- P For pawn transformation , the pawn is the only piece who can transform in other piece less the king (it can transform also in pawn because the new rule described in the "Introduction" move of the pawn). We have two situation: for the squares a1, a8, h1, h8 the pawn can transform in C,N,T,D in two ways (example a1: a2a1C, a2a1N, a2a1T, a2a1D, b2a1C, b2a1N, b2a1T, b2a1D). and for the square b1, c1, d1, e1, f1, g1, b8, c8, d8, e8, f8, g8 it can be transform in three ways (example b1: a2b1C, a2b1N, a2b1T, a2b1D, b2b1C, b2b1N, b2b1T, b2b1D, c2b1C, c2b1N, c2b1T, c2b1D) in total we have 4*4*2 + 4*12*3 = 176.
- N For the knight we have: 2,3,4,6,8; for the squares a1, a8, h1, h8 it can be moved in 2 ways (example: a1 Nc2a1, Nb3a1), for the squares a2, a7, b1, b8, g1, g8, h2, h7 it can be moved in 3 ways (example a2: Nb4a2, Nc3a2, Nc1a2), for the squares a3-a6, b2, b7, c1, c8, d1, d8, e1, e8, f1, f8, g2, g7, h3-h6 it can be moved in 4 ways (example a3: Nb1a3, Nb5a3, Nc2a3, Nc4a3), for the squares b3-b6, b2, b7, c2, c7, d2, d7, e2, e7, f2, f7, g3-g6 it can be moved in 6 ways (example b3: Na1b3, Na5b3, Nb1b3, Nb5b3, Nd2b3, Nd4b3), for the squares c3-c6, d3-d6, e3-e6, f3-f6 it can be moved in 8 ways (example c3: Na2c3, Na4c3, Nb1c3, Nb5c3, Nd1c3, Nd5c3, Ne2c3, Ne4c3),in total we have 4*2 + 8*3 + 20*4 + 16*6 + 16*8 = 336.
- B We can established the following recurrence rule:

*((7 + min{8 - the line on which it's positioned ,8 - column on which it's positioned}) mod 4) * 2.* (1)

This expression can have the values :7, 9, 11, 13 For the squares a1-a8, h1-h8, b1, c1, d1, e1, f1, g1, b8, c8, d8, e8, f8, g8 it can be moved in 7 ways (example a1: Bb2a1, Bc3a1, Bd4a1, Be5a1, Bf6a1, Bg7a1, Bh8a1) for the squares b2-b7, g2-g7, c2, d2, e2, f2, c7, d7, e7, f7 it can be moved in 9 ways (example b2: Ba1b2, Ba3b2, Bc1b2, Bc3b2, Bd4b2, Be5b2, Bf6b2, Bg7b2, Bh8b2) fot the squares c3-c6, f3-f6, d3, e3, d6, e6 it can be moved in 11 ways (example c3: Ba1c3, Ba5c3, Bb2c3, Bb4c3, Bd4c3, Be5c3, Bf6c3,

ISSN 2067 – 4074

Bg7c3, Bh8c3) for the squares d4, d5, e4, e5 it can be moved in 13 ways (example d4: Ba1d4, Ba7d4, Bb2d4, Bb6d4, Bc3d4, Bc5d4, Be5d4, Bf6d4, Bg7d4, Bh8d4) in total we have 28*7 + 20*9 + 12*11 + 4*13 = 560.

- R For every square it can be moved in 14 ways(7 on vertical and 7 on horizontal)having in total 14*64=896.
- Q For every square the queen can move like a bishop and like a rock having 560 + 896=1456.
- K For the king we have: 8,5,3. For the squares b2-b7, c2-c7, d2-d7, e2-e7, f2-f7, g2-g7 it can be moved in 8 ways.(example b2: Ka1b2, Kb1b2, Kc1b2, Kc2b2, Kc3b2, Kb3b2, Ka3b2, Ka2b2), for the squares b1, c1, d1, e1, f1, g1, h1, b8, c8, d8, e8, f8, g8, h8, a2-a7, h2-h7 it can be moved in 5 ways (example a2: Ka1a2, Kb1a2, Kb2a2, Kb3a2, Ka3a2), for the squares a1, a8, h1, h8 it can be moved in 3 ways (example a1: Ka2a1, Kb1a1, Kb2a1), we have in total 6*6*8 + 6*4*5 + 3*4 + 2(the last 2 add is for the king side castling and queen side castling) =422.

So the cardinal of V is: 312 + 176 + 336 + 560 + 896 + 1456 + 422=4158.

Set of states :Q

Observation: To calculate this cardinal the colour is important.

Normally we can say that the cardinal is 14^{64}, but the kings can only once on the board. We have two pieces fixed (the white and black king) which also must obey the rule that the two kings mustn't be close one to another. Then we have 12^{62} possibilities considering the 2 kings fixed.

White king we will maintain in a fixed position and we will see in how many position can the black king be. We can easily observe that we can do the same changing the colour of the kings. It's enough to increase by 2 the result.
For the squares a1, a8, h1, h8 the black king can be fixed in 60 ways, who give as 4 * 60 * 12^{62}, for the squares b1, b8, c1, c8, d1, d8, e1, e8, f1, f8,g1, g8 the king it can be fixed in 58 ways, who give 12 * 58 * 12^{62}, for the squares a2-a7, b2-b7, c2-c7, d2-d7, e2-e7, f2-f7, g2-g7 it give 36 * 55 * 12^{62}.

In total we have 2 * 12^{63} * 243 possible states (we take out a factor 12^{63}).

The initial state: q_0

The initial state is the position of the board when the game begun.

The transaction function: δ

The transaction function is exactly the sum of all possible moves during the game chess.

The final states: F

The set of final states is equal with Q.

3.1.2 The algorithm

A key is a word accepted by the chess automata that have some restriction.

We make a restriction for the final states: we chose which the keys who had the length grater or equal to 22(the number of moves in the chess games). If a key don't have at least 22 moves ,we will expand it using a random algorithm. Will repeat this algorithm until the number of moves is at least 22.

Observation: The space for the set of keys without the restriction is equal to 10^{120} [1].

3.2 Encryption algorithm

A word will be considered a matrix of 8X8 that have elements pieces of chess or blank squares(white or black).

Will note the white elements with X_A and the black one with X_N.

We have the elements: P_A, P_N, C_A, C_N, N_A, N_N, T_A, T_N, D_A, D_N, R_A, R_N, 0_A, 0_N.

We will associate for every element: 0, P, C, N, T, D, R a number from Z_7 like that: 0↔0, P↔1, C↔2, N↔3, T↔4, D↔5, R↔6.

We define the next operation:

$$X_A \oplus Y_A = Z_A (\mathrm{mod}\, 7)$$
$$X_A \oplus Y_N = Z_N (\mathrm{mod}\, 7)$$
$$X_N \oplus Y_A = Z_N (\mathrm{mod}\, 7)$$
$$X_N \oplus Y_N = Z_A (\mathrm{mod}\, 7)$$

(2)

, where the element of form X_A is a white piece and X_N is a black piece.

Let consider the next configuration:

Fig. 2

and the key:1.e2e4

The encryption will do this way: The actual configuration is applied to the operation described above with the key after each round. The key is the game:1.e2e4 and after e2e4 will applied the configuration:

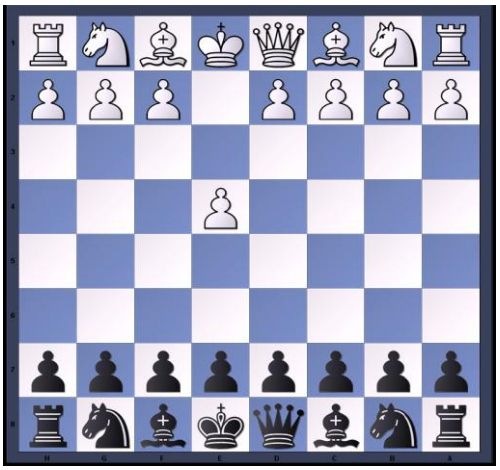

Fig. 3

to the initial configuration(Figure 2) and we have:

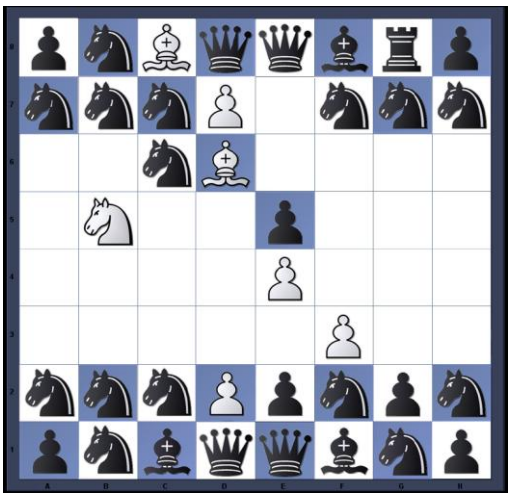

Fig. 4

Observation: After flipping the board the pieces are orientated H-A but in computation with considering them A-H.

with the operation described above.

The key have the white piece top and after each move the board is rotated and the white pieces are in the bottom of the board.

3.2 Decryption algorithm

We use the same representation and the same consideration use in the encryption process.

Will define the next operation:

ISSN 2067 – 4074

$$X_A \Theta Y_A = Z_A (\mathrm{mod}\, 7)$$

$$X_A \Theta Y_N = Z_N (\mathrm{mod}\, 7)$$

$$X_N \Theta Y_A = Z_N (\mathrm{mod}\, 7)$$

$$X_N \Theta Y_N = Z_A (\mathrm{mod}\, 7)$$

(3)

Observation: Will use only positive number (-6 will be 1).

The decryption will be made in a reverse fashion. The key will be parse in reverse way, for the last move to the first move. After the encrypted word will apply the operation described above respecting the

observation of the encryption process.

The space for the word (a configuration) is equal 64! / 32! $(8!)^2(2!)^2$ roughly 10^{43} [1].

This includes some illegal positions (e.g., pawns on the first rank, both kings in chess) and excludes legal positions following captures and promotions but we can understand that is enough to find easy for any alphabet for the text to be encrypted/decrypted.

4. Conclusion

In this paper was demonstrated how to build a new cryptosystem based on the chess game. The algorithm passed successfully the classic attack with brut force. The space of the key is huge including the restriction of 22 moves. Will also be for interest to study the compartment of the cryptosystem on other attacks.

4.1 Future improvements

Passing the Chess game to Chess960 game. The initial position for the key is always the same, that will be certainty a goal for attacks. The are some difference for the moves, but the biggest difference is that from game to game the initial position is different. (The initial position for the pieces is different, exception the pawns). Or also they are other variant like: Chess256, Corner Chess etc.

Another idea can be to generate a random position and start play randomly from that position.

Will be interesting to extend this algorithm for a board with n X n squares and n set of pieces.

References

[1] Claude E. Shannon, Philosophical Magazine, Ser.7, Vol. 41, No. 314 - March. Programming a Computer for Playing Chess, 1950

[2] www.fide.com Handbook – Laws of Chess with Appendix (http://www.fide.com/fide/handbook?id=124&view=article)

[3] http://en.wikipedia.org/wiki/Chess960

[4] G. Rozenberg, A. Salomaa, Handbook Of Formal Languages, Springer, 1997 – Chapter 2 – Regular Languages