Should Chess Players Learn Computer Security?

Gildas Avoine, Cédric Lauradoux, Rolando Trujillo-Rasua

Abstract—The main concern of chess referees is to prevent players from biasing the outcome of the game by either colluding or receiving external advice. Preventing third parties from interfering in a game is challenging given that communication technologies are steadily improved and miniaturized. Chess actually faces similar threats to those already encountered in computer security. We describe chess frauds and link them to their analogues in the digital world. Based on these transpositions, we advocate for a set of countermeasures to enforce fairness in chess.

Index Terms—Security, Chess, Fraud.

1 Introduction

Chess still fascinates generations of computer scientists. Many great researchers such as John von Neumann, Claude Shannon, and Alan Turing to name a few have spent time studying chess programming. John Conway was also attracted by the game of chess and, in general, by combinatorial game theory. He introduced a popular chess fraud known as the *chess grandmaster problem*, where a little girl Anne-Louise, who has never heard of chess, wants to face two grandmasters, Bobby Fischer and Boris Spassky, in correspondence chess. Has she lost her mind? Not really, she has a clever strategy which consists in playing Black against Fischer and White against Spassky. Once Fischer sends his first move, Anne-Louise copies this move and sends it to Spassky. Then, she waits Spassky's move and forwards it to Fischer. And so on, until she either wins one of the games or draws both of them. Anne-Louise only relays the moves between the two grandmasters. So the two grandmasters are indeed playing against each other, instead of playing against a little girl as one's would expect.

Conway's work on the chess grandmaster problem was pursued and extended to authentication protocols by Desmedt, Goutier and Bengio [3] in order to break the Feige-Fiat-Shamir protocol [4]. The attack was called *mafia fraud*, as a reference to the famous Shamir's claim: "I can go to a mafia-owned store a million times and they will not be able to misrepresent themselves as me." Desmedt *et al.* proved that Shamir was wrong via a simple application of Conway's chess grandmaster problem to authentication protocols. Since then, this attack has been used in various domains such as contactless credit cards, electronic passports, vehicle keyless remote systems, and wireless sensor networks.

The origin of this article comes from recent news about cheating in top-level chess tournaments. A famous case is the Georgian chess champion and grandmaster Gaioz Nigalidze who was caught in April 2015. He used a smartphone with a headset in the restroom during the Dubai Open Chess Tournament. He was banned for three years and his grandmaster title was revoked.

In 2010, several French grandmasters, including the coach of the national team cheated during the chess Olympiad at Khanty-Mansiysk. The grandmaster Sébastien Feller was helped by his fellows Arnaud Hauchard and Cyril Marzolo to win his games by using a combination of cell phones, computer, and body language to inform the grandmaster of the best moves to play.

In the same year, Veselin Topalov accused Vladímir Krámnik of cheating during their match for the world chess title at Elista. Topalov's accusations against Krámnik were motivated by his opponent's suspicious behavior: he visited the restroom with an unusual frequency. Topalov's supporters claimed that Krámnik received help in the restroom.

G. Avoine is a member of INSA Rennes, IRISA, and the Institut Universitaire de France.
C, Lauradoux is a member of Inria Rhône-Alpes
R. Trujillo-Rasua is with the University of Luxembourg and the Interdisciplinary center of Security, Reliability, and Trust.

An interesting cheating allegation occured at the 2006 World Open in Philadelphia. After an impressive streak of wins, an unknown player was caught bearing several electronic devices including a cover earring device. He was accused of getting help from an accomplice.

Certainly, chess fraud has a long history and did not wait for the new technologies to be implemented. All a cheating player needs is to be aided by a stronger chess player. The challenge is that nowadays we all have access to the strongest chess player ever: the computer. The question therefore is whether the next world chess champion will be a human player or a computer. We put our two cents in this question by analyzing chess fraud from a computer security perspective.

2 Over-the-board chess

When computers started to be stronger than grandmasters, some players have seized this opportunity to cheat. Instead of using their brain on the board, they use it to elaborate strategies to receive computer advices during their games. This is strictly forbidden by the rules of chess, but dishonest players have been extremely cunning and have developed different types of covert channels to transmit information without being caught. This section addresses this fraud by considering the game of chess in its simplest form, that is, in a face-to-face battle.

We assume that chess games are setted up in such a way that the players are convinced of the identity of their opponents. This can be achieved by face recognition, identity document verification, or any other biometrics authentication mechanism. Thus, cheating strategies such as allowing a twin brother or sister to play on one's behalf are out of our scope. We do not cover either unethical behaviours such as rate manipulation, intentional draws, kicking/insulting a player, or touching pieces. The chess fraud we focus on consists in the use of external help during a game. Whether such help is useful to perform better or not is regarded irrelevant; in the same way that many drugs in sport competitions are banned even though they do not enhance performance. Given that referees (if any) are considered to be honest, it follows that any communication channel between a player and a third party must go through a covert channel.

2.1 Covert channels

A covert channel is a communication channel that was not intended for information transfer. One of the earliest documented use of a covert channel can be found in the Greek book *Histories* by Herodotus written in 440 BC; a slave was used to secretly transmit a message by shaving the slave's head, tattooing the message, letting the hair growing, and sending the slave to the intended recipient who has to shave the slave's head again in order to retrieve the message.

Practically, any ordinary thing can be used as a covert channel. In chess, players who are used to play with pieces they have taken during a game, can use this apparently inoffensive behaviour to exchange information with somebody else.

The use of covert channels in chess is actually nicely illustrated through the famous cheating scandal during the 2010 FIDE Olympiad Tournament at Khanty-Mansiysk, where the French coach used movement patterns within the playing venue to communicate with his team. The fraud works as follows. The coach stops in front of a given chessboard. If he is by the side of the black or of the white, the player understands a different coordinate. The coach and the player agree on 64 positions in the playing area before the tournament. The move representation associated to the coach position is the long algebraic chess notation: the rows of the board are identified by a number and the columns by a letter. The symbol (letter, number)-(letter, number) indicates the starting square and the destination square (see Figure 1). Such a scheme requires twelve bits to communicate a move. The French grandmasters used an inefficient board representation. Indeed, by using standard techniques in computer sciences a chess move can be encoded with less bits, implying that this type of chess fraud can be quite hard to prevent.

To illustrate this, we remark that the compact communication of a chess move is fully answered by Shannon's works on communications and chess [11]. Entropy or uncertainty is for the chess player the branching number of the position, i.e., the number of legal moves he can make on the board and denoted b_p. The player and the accomplice needs to agree on a method to enumerate all the moves, for instance from left (a) to right (h) and top (8) to bottom (1). So, the accomplice needs to communicate $\lceil \log_2(b_p) \rceil$ bits to the player. Note that there is no ambiguity with such a coding system: two pieces can reach the same square but these two different moves have different numbers. Shannon estimated that the maximum number of available moves in a given position is $\max(b_p) \approx 35$. Consequently, only six bits instead of twelve are needed in

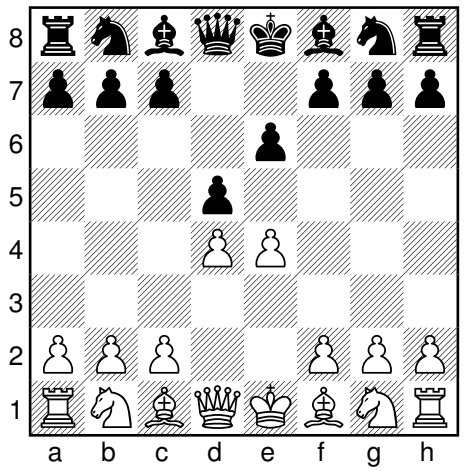

Fig. 1. Long algebraic chess notation. Each move is described by the starting coordinate of the piece and by the destination. This figure corresponds to the following move order: 1.e2-e4 e7-e6 2.d2-d4 d7-d5. The starting square is often omitted in the algebraic notation if there is no ambiguity.

the worst case to encode a chess move. For example, Figure 2 provides a valid chess position and Table 1 enumerates the associated legal moves.

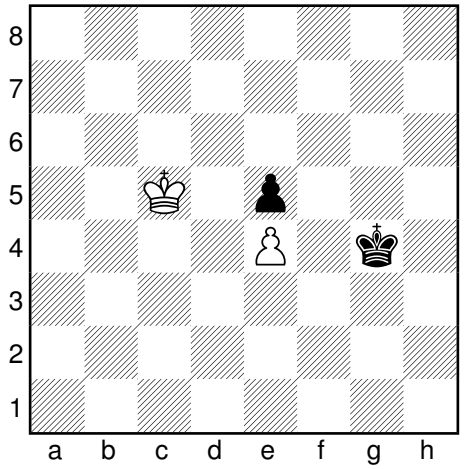

Fig. 2. Seven legal moves exist for white in this position, which can be transmitted by using only three bits.

TABLE 1
Enumeration of the legal moves in Figure 2.

Move	♔b6	♔b5	♔b4	♔c6	♔c4	♔d6	♔d5
Number	0	1	2	3	4	5	6

2.2 Mitigating the use of covert channels

Four fundamental steps are applied in computer security to deal with unpredictable attacks: protect the system, detect the attack, react to the attack, and mitigate the damage. FIDE already has a comprehensive set of rules to react to chess fraud and mitigate their impact. Ergo we focus next on protection and detection.

Discarding Any Channel. A fundamental countermeasure in computer security to prevent the use of covert channels consists in isolating the system. For example, tempest shielded rooms are commonly used in sensitive areas to circumvent covert channels [9]. Isolation is also used in smartcards to make them tamper-resistant. In chess, it is rather difficult to make tournament venues tempest-certified because not only the playing area must be tempest-certified, but also the facilities, including the restroom, which contain water pipelines that could carry the signals.

Instead of using a tempest-certified area, other approaches consist in ensuring that no communicating devices can penetrate the playing area using for example metal detectors (this approach is not highly resilient, though) or jammers to perturb any unauthorized radio signal. There exist countries where jammers are allowed under special circumstances, for example in jails or theaters. Therefore, jammers seem to be a practical solution to restrict communication with third parties.

Electronic covert channels are not the only ones, though. For example, at the prestigious Sofia M-Tel masters tournament, the playing area was a sound-proof glass cube; the audience can observe the players without disturbing them. The use of visual covert channels can however be partially eliminated by a one-way mirror, where the audience can observe the players but not the other way around.

Increasing Channel bandwidth. Another approach to mitigate the use of covert channels is by increasing the entropy of the messages or, in other words, requiring a larger channel bandwidth. As a rule of thumb, the shorter a message the easier is to transmit it through a covert channel. Since increasing the size of the board is not a practical option, we propose attaching to every move a couple of variants. Recall that a variant in chess describes a sequence of moves that may follow from a given position. That is to say, a chess player will be required to provide, in addition to a move, a variant where the player shows his intention with the move. Of course, variants should only be revealed to a trusted third party

and not to the opponent. Moreover, the relation between variants and the course of the game needs to be established, because any player with minimal knowledge of chess can provide a couple of valid variants. What can be hard for a cheater is to find the correct variant, that is, the one intended by the computer. This solution is an additional burden for chess players, but, if proven effective, honest players might be happy to adopt it.

Requiring Many Channels. In a playing venue a player typically moves between two different zones: the playing area and the restroom. While the former is highly monitored by referees, cameras, journalists, and even the attendees, the restroom totally lacks surveillance. Consequently any covert channel deployed in the restroom, such as a smartphone with a chess engine, can be easily exploited by a player pretty much regardless of the message length. Allowing the installation of this type of covert channel in a restroom is thus a security vulnerability, and should be treated as such.

There exist many techniques that can be used to ensure up to some extent the integrity of a restroom facility, such as surveillance, visual inspection, and metal detectors. When all that fail, we can still make use of a rather new trend in computer security called *moving target defense*. The moving target concept attempts to flip around the current imbalance between the efforts needed to attack and defend a system. In a static system, a single vulnerability can lead to a devastating attack. The defender's task is consequently hard, namely assessing one by one all vulnerabilities. Moving target techniques advocate for dynamic, diverse, and somehow unpredictable systems, making harder the finding and exploitation of a vulnerability.

A moving target technique in chess consists, for example, in randomizing the access to the restroom. That is to say, every time a player needs to go to the restroom he is assigned with a random stall (out of many). Such a technique forces a dishonest player to install a covert channel in all stalls, which might be unpractical. We show later in a tournament scenario a similar technique, where pairings are setup randomly and players are unaware against who they are playing to.

Making Channels Faster. In computer security there exist communication protocols designed in such a way that the use of a covert channel makes the protocol to abort or fail. Distance bounding protocols [1] so aim to ensure that a prover is indeed in the close proximity of a given verifier during an authentication process. Such protocols are typically useful to avoid relay attacks against a credit card or and access control card, which are the modern version of the chess grandmaster problem introduced by Conway. The fundamental principle of distance bounding protocols consists in measuring the round-trip time of a message exchanged between the prover and the verifier. Given the speed of light cannot be exceeded, the measured time provides a proven upper-bound in the distance between the parties.

Time is also an important dimension in chess. Transposing distance bounding protocols to solve chess problems can be done by setting up a restrictive time control. In rapid chess game, *e.g.*, blitz, getting external help is clearly more difficult than in standard time control (typically 90 minutes for the first 40 moves). We observe a notable raise in popularity of rapid chess tournaments in recent years, to such an extent that the World Rapid and Blitz Championships is already in the FIDE's official calendar since 2012. Notwithstanding, quality of chess games tend to decrease quickly with the reduction of time control.

3 Tournament chess

The countermeasures proposed in the previous section can prevent players from receiving advices from external parties, but they can be hardly applied to prevent collusion between players in a given tournament. A famous allegation of this type of fraud occurred at the 5th Candidates Tournament at Curaçao in 1962. In the middle of the cold war, five USSR grandmasters (Petrosian, Keres, Geller, Korchnoi, and Tal), two Americans (Fischer and Benko) and a representative of Czechoslovakia (Filip) battle to get the right to challenge Mikhaïl Botvinnik who was the world chess champion at that time. After the victory of USSR grandmaster Petrosian, three allegations of cheating were put forward. Fischer claimed that the USSR grandmasters Petrosian, Keres, and Geller colluded to prevent him from finishing in the first three places (granting a direct access to the next cycle for the world title). He also claimed that Korchnoi lost on purpose against the previous three grandmasters in order to grant them the top places. It was also said that Petrosian and Geller helped Benko in his game against Keres to grant Petrosian overall victory.

3.1 Round-Robin Tournament

In 1962, FIDE decided to switch from round-robin tournaments to elimination matches in order to determine the opponent to the world chess champion. This is perhaps the first countermeasure against collusion in chess tournaments. A round-robin tournament is actually a competition where each player meets all other players in turn. Although such tournaments may seem to be fair at first glance, players who perform poorly can be eliminated early from title contention. They are forced to play the remaining games, though, which significantly degrades their incentive to play fairly.

3.2 Jail Tournament

Inspired by concepts in computer security we can actually design a chess tournament where collusion becomes extremely difficult. We call such a tournament the *jail tournament*, as it is largely inspired by the *prisoners problem* [12] introduced by Gustavus Simmons in 1983.

The prisoners problem describes the situation of two accomplices who have committed a crime, and have been caught. Now, they are locked in separate cells. They want to escape, so they need to agree on details. However, the only way for them to communicate is through the warden. The latter wants to avoid the escape. So, the two accomplices need to find a *subliminal channel* to discuss the details of their escape without revealing anything about their plan to the warden. We make the distinction between covert and subliminal channel, as the latter is a standard communication channel that can be used to transmit information unnoticed.

Players in a jail tournament, as the two prisoners above, are isolated in individual cells. Each cell contains a screen, a mouse and all the commodities needed for the duration of the tournament. The screen displays the chessboard of the player game and the game clock (his adversary time and his own time left to complete the game). The screen displays no information on the identity of the adversary, meaning that all games rely on a secret pairing system controlled by the referee.

3.3 Discovering the Secret Pairing

With jail tournaments, a coalition of dishonest players is in the same situation than the two prisoners. They need to establish a subliminal channel that allows then to execute the intended plan. However, due to the secret pairing, players in a jail tournament face an additional problem: they can only send chess moves to an anonymous player. Therefore identifying the opponent becomes essential for dishonest players. In 1944, the Allies faced a similar problem during the invasion, as paratroopers needed to distinguish friend from foe without being noticed, specially during the hours of darkness. For that, they used a signalling device called *airborne cricket* originally intended for keeping the tempo in music.

Dishonest chess players in a jail tournament aiming at uncovering the secret pairing cannot use an audio subliminal channel. They can communicate through the chess games, though. A coalition may agree on predefined move orders prior going into their cells. These move orders are then used during the tournament to signal the coalition membership. The principle of this method is illustrated in the following example about subliminal identification.

Example. We show that it is relatively easy to find a way for coalition members to identify themselves over the board. The position described in Figure 3 can be reached by four different move orders:

(a) **1 e4 c5 2 ♘f3 d6**,
(b) **1 e4 d6 2 ♘f3 c5**,
(c) **1 ♘f3 c5 2 e4 d6**,
(d) **1 ♘f3 d6 2 e4 c5**.

A database exploration of more than four million games [2] shows that 273 247 games reached the position of Figure 3: 99.45% of games used the move order (a), 0.03% (b), 0.45% (c) and 0.07% (d). A

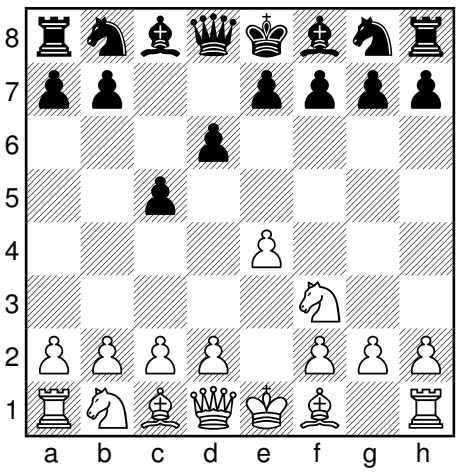

Fig. 3. A variant of the Sicilian opening.

coalition of players can decide that they all start their games with ♘**f3**. If they reach the position

of Figure 3 using move order (c) or (d) they conclude that they are playing against a member of the coalition. However, if all the players used the same moves to reach a position, the referee might be suspicious. Each player of the coalition can then be assigned a unique set of move orders. This set will act as a signature to all the other members of the coalition. At the end, the referee can only conclude that the players have decided to use unusual move orders. As a consequence, anonymous pairing is not sufficient to thwart collusion.

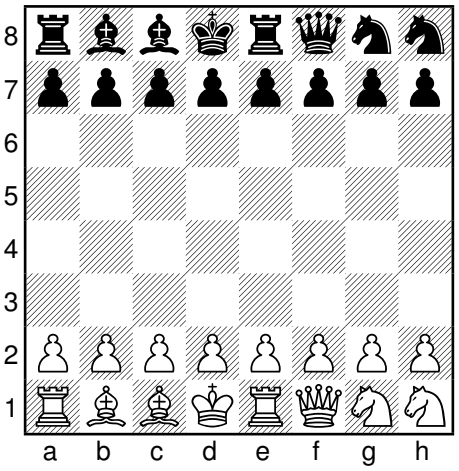

Fig. 4. A starting position at FRC (SPID 147).

3.4 Fischer Random Chess

To prevent players from using the initial chess board configuration to transmit subliminal information, the starting position could be randomized as advocated in [7]. This variant of chess is known as Fisher Random Chess or Chess960. The positions of the pawns are the same as in classical chess and the differences are the positions of the other pieces and the way of castling (Figure 4). There are 960 different starts which is not impressive for a computer but already difficult to handle for a human.

3.5 Timing Attacks

It is worth noting that Fisher Random Chess can mitigate subliminal channels over the chess board but cannot avoid timing attacks. Indeed, given that players can observe when their opponent plays his moves, the timing can be used to convey information. Timing channels are risky, though, because dishonest players going too quickly or too slowly may have a disadvantage against fair opponents.

In the computer security field, timing attacks are very similarly used to set up cross-core covert channels: two virtual machines running on different cores can communicate through the cache memory of the processor [8]. For example, two processes running in the cloud can determine whether they are executed on the same physical computer using such a timing-based covert channel.

4 Detection of Chess Frauds

While reaching this point it becomes clear that the use of covert channels can be fought, but not prevented. In most situations, indeed, the risk of covert channels is actually accepted for the sake of the show. Nevertheless, fraud can still be detected without the need of uncovering the covert channel that is being use, in the same way that attacks to computer networks can be detected without the need of identifying the source of the attacks. That is the task of Intrusion Detection Systems (IDS) in computer security, which are monitoring tools that can detect anomalies, outliers, or suspicious behaviors in a computer system or network.

4.1 Game Analysis

Similar to cyberattacks, cheating in chess may exhibit behaviors that significantly deviate from regular games. Great advances have been made on this direction by Kenneth Regan and his team [10]. They proposed several techniques with strong statistical foundations that correlate players ELO with computer-like moves. Avoiding not a few details, we can intuitively explain their idea as follows: the weaker the player the fewer computer-like moves he would play. In 2014, FIDE officially announced the FIDE Internet-based Game Screening Tool. This tool, as Regan's work, aims at detecting potential outliers in tournaments, which helps the referee to focus more on those games that are found suspicious by the tool. In any case, this tool is not aimed at providing strong evidences of cheating, but insights on potential fraud.

4.2 Player Analysis

We propose a rather different detection mechanism looking at the player himself, focusing more precisely on his brain. Ultimately, is the human brain the muscle being challenged by a game of chess. Our idea is based on proof-of-work verification techniques used in computer security. A proof-of-work typically consists of a problem and its solution. If the problem is moderately hard, then a

solution can be seen as a measure on the processing time required to solve the problem. One popular system based on proof-of-work is Bitcoin, which is based on cryptographic hash functions and consists in finding preimages. With Bitcoin, the work can be arbitrarily hard depending on the output length of the hash function.

Solving chess positions, i.e., finding a good move, can be extremely hard and demanding for humans, while it is trivial for today's computers. We therefore propose to evaluate the brain workload with electroencephalography to decide whether the player actually solved the chess position himself or was aided by a third party. Indeed, we expect the cognitive load to be significantly different when the player focuses on finding a good move, and when he waits for the aid from the third party. Evaluating the cognitive load during problem solving was introduced by John Sweller in 1988 [13]. This technique was for example already successfully used to evaluate the user experience when he interacts with a system using either a keyboard or a touch-based interface [5].

Note that other human body properties can be subject to anomaly detection analysis, e.g. eyes movement, blood pressure, heart rate, etc. However, analysing the root of the problem, namely the brain, should make the analysis more accurate.

5 Conclusion

Grandmaster Gligoric advocates in his book *Shall We Play Fischerandom Chess?* [6] for the end of the classic chess era to the benefit of Fischer Random Chess. He argued that computers plague classical chess even in fair games: players make deep training on chess openings, rendering games boring. He points out that Fischer Random Chess provides more room for creativity and reduces the impact of computerized training.

We also go into that direction, and deeper, disclosing several chess frauds and providing countermeasures to avoid or mitigate them. Our work highlights similarities between chess and computer security, in order to identify how frauds can be mounted in chess, but also to find countermeasures, althought not all of them can be easily put into practice. Given the technology advances, in particular on the miniaturization of computing devices, learning computer security is certainly a way for chess players to stay aware of future attacks.

Acknowledgement

We would like to kindly thank Guillaume Salagnac for making us aware of an article in a newspaper making the connection between the chess Olympiad fraud and the allegation of poker frauds. We would also like to thank Julio Hernandez-Castro for long discussions on chess frauds.

References

[1] S. Brands and D. Chaum. Distance-Bounding Protocols. In *Advances in Cryptology – EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359, Lofthus, Norway, May 1993. Springer-Verlag.

[2] ChessBase. Big Database 2011 , 2011. http://www.chessbase-shop.com/en/products/5852.

[3] Y. Desmedt, C. Goutier, and S. Bengio. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. In C. Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 21–39, Santa Barbara, CA, USA, August 1988. Springer-Verlag.

[4] U. Feige, A. Fiat, and A. Shamir. Zero Knowledge Proofs of Identity. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing – STOC*, pages 210–217, New York City, NY, USA, May 1987. ACM.

[5] J. Frey, M. Daniel, J. Castet, M. Hachet, and F. Lotte. Framework for electroencephalography-based evaluation of user experience. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, May 7-12, 2016*, pages 2283–2294, 2016.

[6] S. Gligoric. *Shall We Play Fischerandom Chess?* Batsford, 2003.

[7] W.-M. Hu. Reducing Timing Channels with Fuzzy Time. In *IEEE Symposium on Security and Privacy*, pages 8–20, Oakland, CA, USA, 1991. IEEE.

[8] C. Maurice, C. Neumann, O. Heen, and A. Francillon. C5: cross-cores cache covert channel. In M. Almgren, V. Gulisano, and F. Maggi, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment - 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings*, volume 9148 of *Lecture Notes in Computer Science*, pages 46–64. Springer, 2015.

[9] NSA. TEMPEST: A signal problem. *Cryptologic Spectrum*, 2(3):26–30, 1972.

[10] K. W. Regan and G. M. Haworth. Intrinsic chess ratings. In *Proceedings of the Twenty-Fifth AAAI Conference on Artificial Intelligence*, AAAI'11, pages 834–839. AAAI Press, 2011.

[11] C. E. Shannon. Programming a computer for playing chess. *Philosophical Magazine (7)*, 41(314):256–275, March 1950.

[12] G. J. Simmons. The Prisoners' Problem and the Subliminal Channel. In *Advances in Cryptology – CRYPTO '83*, pages 51–67. Plenum Press, 1983.

[13] J. Sweller. Cognitive load during problem solving: Effects on learning. *Cognitive Science*, 12(2):257–285, 1988.