Bibliography on Mental Poker

Heiko Stamer
HeikoStamer@gmx.net

Version 1.6

Abstract

This bibliography maintains some references to scientific papers on the so-called "Mental Poker" problem: it asks whether it is possible to play a fair game of poker without physical cards and without a trusted dealer, i.e., by phone or over the Internet. This question has raised some interesting solutions in the early days of public research in cryptography and stimulated some important considerations like semantic security. Nowadays it gains again some attention due to the freaky hype of cryptocurrencies.

References

[AskarovSabelfeld:2005] Aslan Askarov and Andrei Sabelfeld. Security-Typed Languages for Implementation of Cryptographic Protocols: A Case Study of Mutual Distrust. Technical Report 2005-13, Department of Computer Science and Engineering, Chalmers University of Technology and Göeborg University, 2005.

[AskarovSabelfeld:2005:ESORICS] Aslan Askarov and Andrei Sabelfeld. Security-Typed Languages for Implementation of Cryptographic Protocols: A Case Study. In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, *Computer Security - ESORICS 2005, Proceedings of the 10th European Symposium on Research in Computer Security*, volume 3679 of *Lecture Notes in Computer Science*, pages 197–221. Springer Verlag, 2005.

Abstract: Security protocols are critical for protecting modern communication infrastructures and are therefore subject to thorough analysis. However practical implementations of these protocols lack the same level of attention and thus may be more exposed to attacks. This paper discusses security assurance provided by security-typed languages when implementing cryptographic protocols. Our results are based on a case study using Jif, a Java-based security-typed language, for implementing a non-trivial cryptographic protocol that allows playing online poker without a trusted third party. The case study deploys the largest program written in a security-typed language to date and identifies insights ranging from security guarantees to useful patterns of secure programming.

[AuYoungTuttle:2004] Alvin AuYoung and Christopher Tuttle. Cryptographic Blackjack. Final Project Report CSE 207, University of California at San Diego, 2004.

Abstract: Internet casinos have become a billion dollar industry. The increasing popularity of online gaming is surprising given its weak guarantees of fairness compared to those offered by physical casinos. We apply a bit commitment protocol to an online blackjack game that provides strong fairness guarantees between the player and casino without compromising the play of the game. We introduce a set of experiments that capture the fairness guarantees of the protocol, and describe how this protocol can be extended to other online games.

[BaranyFuredi:1983] Imre Bárány and Zlotán Füredi. Mental Poker with Three or More Players. *Information and Control*, 59(1–3):84–93, 1983.

[BarnettSmart:2003:IMA] Adam Barnett and Nigel P. Smart. Mental Poker Revisited. In Kenneth G. Paterson, editor, *Cryptography and Coding, Proceedings of the 9th IMA International Conference,*

volume 2898 of *Lecture Notes in Computer Science*, pages 370–383. Springer Verlag, 2003.

> **Abstract:** We discuss how to implement a secure card game without the need for a trusted dealer, a problem often denoted "Mental Poker" in the literature. Our solution requires a broadcast channel between all players and the number of bits needed to represent each card is independent of the number of players. Traditional solutions to "Mental Poker" require a linear relation between the number of players and the number of bits required to represent each card.

[Castella-Roca:2005] Jordi Castellà-Roca. *Contributions to Mental Poker*. PhD thesis, Universitat Autònoma de Barcelona, 2005.

> **Abstract:** Computer networks and especially the Internet have allowed some common activities such as shopping or gambling to become remote (e-shopping and e-gambling). The poker game played over a network is known as mental poker. The problem with mental poker is the difficulty of keeping it practical while guaranteeing the same standards of security, fairness and auditability offered by standard casinos for physical poker. The important aspects to take into account when designing mental poker protocols are: functionality, security, and computational and communication cost. Proposals in the literature usually focus on the first two items only. This makes comparisons difficult. This thesis starts with a formal cost analysis of the main proposals in the literature. The analysis is not limited to costs, though; security is also analyzed and, in fact, our study detected a fundamental weakness in one of the compared mental poker protocols. The attack is presented in a separate chapter after the global comparative analysis. The three following chapters of this thesis present three new protocols that enhance the proposals in the literature in different ways. The first proposal belongs to the family of TTP-free

protocols and does not preserve the confidentiality of player strategies; it reduces the computational cost by avoiding the use of zeroknowledge proofs. The second proposal is TTP-free, preserves the confidentiality of player strategies and reduces the computational cost by requiring players to perform less mathematical operations. The third proposal addresses a novel functionality usually not offered in the literature, namely player dropout tolerance, i.e. the ability to continue the game even if some players leave it.

[Castella-RocaDazaDomingo-FerrerSebe:2006] Jordi Castellà-Roca, Vanesa Daza, Josep Domingo-Ferrer, and Francesc Sebé. Privacy Homomorphisms for E-Gambling and Mental Poker. In *Proceedings of the IEEE International Conference on Granular Computing*, pages 788–791, 2006.

> **Abstract:** With the development of computer networks, situations where a set of players remotely play a game (e-gaming) have become usual. Often players play for money (e-gambling), which requires standards of security similar to those in physical gambling. Cryptographic tools have been commonly used so far to provide security to e-gambling. Homomorphic encryption is an example of such tools. In this paper we review the mental poker protocols, where players are assumed to remotely play poker. We focus on the key advantage of using cryptosystems with homomorphic properties (privacy homomorphisms) because they offer the possibility of manipulating cards in encrypted form.

[Castella-RocaDomingo-Ferrer:2004:ITCC] Jordi Castellà-Roca and Josep Domingo-Ferrer. On the Security of an Efficient TTP-Free Mental Poker Protocol. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC '04)*, volume 2, pages 781–784. IEEE Computer Society, 2004.

> **Abstract:** Using commutative cryptosystems is a way to obtain efficient mental poker protocols which do not require using a trusted third party (TTP). However, the security of such protocols depends on the particular cryptosystem used. We show that a TTP-free mental poker protocol using an ElGamal-like commutative cryptosystem is insecure.

[Castella-RocaDomingo-FerrerRieraBorrell:2003:INDOCRYPT] Jordi Castellà-Roca, Josep Domingo-Ferrer, Andreu Riera, and Joan Borrell. Practical Mental Poker Without a TTP Based on Homomorphic Encryption. In Thomas Johansson and Subhamoy Maitra, editors, *Progress in Cryptology - INDOCRYPT 2003*, volume 2904 of *Lecture Notes in Computer Science*, pages 280–294. Springer Verlag, 2003.

> **Abstract:** A solution for obtaining impartial random values in on-line gambling is presented in this paper. Unlike most previous proposals, our method does not require any TTP and allows e-gambling to reach standards of fairness, security an auditability similar to those common in physical gambling. Although our solution is detailed here for the particular case of games with reversed cards (e.g. poker), it can be easily adapted for games with open cards (e.g. blackjack) and for random draw games (e.g. keno). Thanks to the use of permutations of homomorphically encrypted cards, the protocols described have moderate computational requirements.

[Castella-RocaDomingo-FerrerSebe:2005] Jordi Castellà-Roca, Francesc Sebé, and Josep Domingo-Ferrer. Dropout-Tolerant TTP-Free Mental Poker. In Sokratis Katsikas, Javier López, and Günther Pernul, editors, *Trust, Privacy, and Security in Digital Business, Proceedings of the Second International Conference TrustBus 2005*, volume 3592 of *Lecture Notes in Computer Science*, pages 30–40. Springer Verlag, 2005.

> **Abstract:** There is a broad literature on distributed card games over communications networks, col-

lectively known as mental poker. Like in any distributed protocol, avoiding the need for a Trusted Third Party (TTP) in mental poker is highly desirable, because really trusted TTPs are not always available and seldom free. This paper deals with the player dropout problem in mental poker without a TTP. A solution based on zero-knowledge proofs is proposed. While staying TTP-free, our proposal allows the game to continue after player dropout.

[Castella-RocaDomingo-FerrerSebe:2006] Jordi Castellà-Roca, Josep Domingo-Ferrer, and Francesc Sebé. On the Security of a Repaired Mental Poker Protocol. In *Information Technology: New Generations, Proceedings of the Third International Conference (ITNG 2006)*, pages 664–668, 2006.

Abstract: In 2003, Zhao, Varadharajan and Mu proposed a mental poker protocol whose security was shown to be flawed in 2004: any player (or any outsider knowing the deck coding) is able to decrypt encrypted cards without knowing the encryption key. In 2005, the first two authors published a repaired version of this TTP-free mental poker protocol. We show here that this second version is also flawed: the first player can find all cleartexts of the final encrypted shuffled deck of cards. Both protocols are similar to Shamir-Rivest-Adleman's mental poker, but they replace an exponential commutative cipher with an ElGamal-like commutative cipher. We conclude that changing the underlying commutative cipher is the reason of their weakness.

[Castella-RocaDomingo-FerrerSebe:2006:CARDIS] Jordi Castellà-Roca, Josep Domingo-Ferrer, and Francesc Sebé. A Smart Card-Based Mental Poker System. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *Smart Card Research and Advanced Applications, Proceedings of 7th IFIP WG 8.8/11.2 International Conference (CARDIS 2006)*, volume 3928 of *Lecture Notes in Computer Science*, pages 48–61. Springer Verlag, 2006.

Abstract: On-line casinos have experienced a great expansion since the generalized use of Internet started. There exist in the literature several proposals of systems allowing secure remote gaming. Nevertheless, the security requirements of some game families lead to the use of complex and costly cryptographic protocols. A particularly challenging game family is mental poker. In this paper we present a smart card-based e-gaming system for mental poker with a low computational cost.

[Castella-RocaDomingo-FerrerSebe:2017:ASIACRYPT] Iddo Bentov, Ranjit Kumaresan, and Andrew Miller. Instantaneous Decentralized Poker. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017 – 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part II*, volume 10624 of *Lecture Notes in Computer Science*, pages 410–440. Springer Verlag, 2017.

Abstract: We present efficient protocols for amortized secure multiparty computation with penalties and secure cash distribution, of which poker is a prime example. Our protocols have an initial phase where the parties interact with a cryptocurrency network, that then enables them to interact only among themselves over the course of playing many poker games in which money changes hands. The high efficiency of our protocols is achieved by harnessing the power of stateful contracts. Compared to the limited expressive power of Bitcoin scripts, stateful contracts enable richer forms of interaction between standard secure computation and a cryptocurrency. We formalize the stateful contract model and the security notions that our protocols accomplish, and provide proofs in the simulation paradigm. Moreover, we provide a reference implementation in Ethereum/Solidity for the stateful contracts that our protocols are based on. We also adapt our off-chain cash distribution protocols to the special case of stateful duplex micropayment channels, which are of independent interest. In comparison to Bitcoin based payment channels, our duplex channel implementation is more efficient and has additional features.

[ChouYeh:2002] Jue-Sam Chou and Yi-Shiung Yeh. Mental Poker Game based on a Bit Commitment Scheme through Network. *International Journal of Computer and Telecommunications Networking*, 38(2):247–255, 2002.

Abstract: There are many schemes proposed on mental poker so far. Most of them are based on the composition of each player's private permutation of cards. Yet, each one is either too complex or has some drawbacks in it. In other words, no solution has come to reality. In this paper, we propose a permutation-free method, i.e. a bit commitment scheme, along with the RSA cryptosystem (Cryptography-Theory and Practice, CRC Press, Boca Raton, 1995; Public-key Cryptography, Springer, Berlin, 1996) to implement the mental poker game. It is not only simple but also concise in concept.

[Coppersmith:1985:CRYPTO] Don Coppersmith. Cheating at Mental Poker. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85: Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 104–107. Springer Verlag, 1985.

Abstract: We review the "mental poker" scheme described by Shamir, Rivest and Adleman [SRA]. We present two possible means of cheating, depending on careless implementation of the SRA scheme. One will work if the prime p is such that $p-1$ has a small prime divisor. In the other scheme, the names of the cards "TWO OF CLUBS" have been extended by random-looking bits, chosen by the cheater.

[Crepeau:1985:CRYPTO] Claude Crépeau. A Secure Poker Protocol that Minimizes the Effect of Player Coalitions. In Hugh C.

Williams, editor, *Advances in Cryptology - CRYPTO '85: Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 73–86. Springer Verlag, 1985.

> **Abstract:** What can we expect from a poker protocol? How close to reality can we come? From the outset of this research, we realized that a cryptographic protocol could achieve more security than its real life counterpart (with physical cards). But every protocol proposed until now was far from offering all the possibilities of a real deck of cards or could not acheive the full security we were expecting.

[Crepeau:1986:CRYPTO] Claude Crépeau. A Zero-Knowledge Poker Protocol that Achieves Confidentiality of the Players' Strategy or How to Achieve an Electronic Poker Face. In Andrew M. Odlyzko, editor, *Advances in Cryptology - CRYPTO '86: Proceedings*, volume 263 of *Lecture Notes in Computer Science*, pages 239–247. Springer Verlag, 1986.

> **Abstract:** Many attempts have been previously made to achieve a protocol that would allow people to play mental poker [SRA, GM1, BF, FM, Yu, Cr] (I would rather say electronic poker). Unfortunately no solution has ever come close to reality with respect to poker strategy. Poker players usually claim that luck has nothing to do with their gains. In fact, poker is a very strategic game. Often, an inexperienced player will loose a lot of money when playing against an experienced player, only because the former cannot hide so easily his emotions. The experienced player can easily know whether his opponent has a good hand or not. Electronic poker is an ideal way of hiding one's emotions. But, in fact, every protocol proposed thus far ruins this perfect poker face since their security is based on the fact that all hands are revealed at the end of the game. This means that the strategy of the players is known to all his opponents. In particular, if one bluffs with a bad hand in the hope that all his opponents will give up,

he still has to reveal his hand at the end, in order to participate in the verification part of the protocol. Moreover, when a player opens his hand, he does not want his opponents to learn the moment at which each of his cards was drawn, since this would give them some information about his strategy. This paper proposes a new poker protocol that allows players to keep secret their strategy. This protocol is an extension of the one given by Crépeau in [Cr]. The security will not be based on the knowledge of the entire deck of card at the end of the game, but rather on some independent information linked to the entries of the deck. This protocol achieves every constraints of a real poker game. It is the first complete solution to the mental poker problem. It achieves all the necessary conditions suggested in [Cr]: Uniqueness of cards Uniform random distribution of cards Absence of trusted third party Cheating detection with a very high probability Complete confidentiality of cards Min imal effect of coalitions Complete confidentiality of strategy.

[CrepeauKilian:1993:CRYPTO] Claude Crépeau and Joe Kilian. Discreet Solitary Games. In Douglas R. Stinson, editor, *Advances in Cryptology - CRYPTO '93, Proceedings of the 13th Annual International Cryptology Conference*, volume 773 of *Lecture Notes in Computer Science*, pages 319–330. Springer Verlag, 1993.

Abstract: Cryptographic techniques have been used intensively in the past to show how to play multiparty games in an adversarial scenario. We now investigate the cryptographic power of a deck of cards in a solitary scenario. In particular, we show how a person can select a random permutation satisfying a certain criterion discreetly (without knowing which one was picked) using a simple deck of cards. We also show how it is possible using cards to play games of partial information such as POKER, BRIDGE and other cards games in solitary.

[DavidDowsleyLarangeira:2017] Bernardo David, Rafael Dowsley, and Mario Larangeira. Kaleidoscope: An Efficient Poker Protocol with Payment Distribution and Penalty Enforcement. Cryptology ePrint Archive: Report 2017/899, 2017.

> **Abstract:** The research on secure poker protocols without trusted intermediaries has a long history that dates back to modern cryptography's infancy. Two main challenges towards bringing it into real-life are enforcing the distribution of the rewards, and penalizing misbehaving/aborting parties. Using recent advances on cryptocurrencies and blockchain technologies, Andrychowicz et al. (IEEE S&P 2014 and FC 2014 BITCOIN Workshop) were able to address those problems. Improving on these results, Kumaresan et al. (CCS 2015) and Bentov et al. (ASIACRYPT 2017) proposed specific purpose poker protocols that made significant progress towards meeting the real-world deployment requirements. However, their protocols still lack either efficiency or a formal security proof in a strong model. Specifically, the work of Kumaresan et al. relies on Bitcoin and simple contracts, but is not very efficient as it needs numerous interactions with the cryptocurrency network as well as a lot of collateral. Bentov et al. achieve further improvements by using stateful contracts and off-chain execution: they show a solution based on general multiparty computation that has a security proof in a strong model, but is also not very efficient. Alternatively, it proposes to use tailor-made poker protocols as a building block to improve the efficiency. However, a security proof is unfortunately still missing for the latter case: the security properties the tailor-made protocol would need to meet were not even specified, let alone proven to be met by a given protocol. Our solution closes this undesirable gap as it concurrently: (1) enforces the rewards' distribution; (2) enforces penalties on misbehaving parties; (3) has efficiency comparable to the tailor-made proto-

cols; (4) has a security proof in a simulation-based model of security. Combining techniques from the above works, from tailor-made poker protocols and from efficient zero-knowledge proofs for shuffles, and performing optimizations, we obtain a solution that satisfies all four desired criteria and does not incur a big burden on the blockchain.

[Edwards:1994] Jonathan Edwards. Implementing Electronic Poker: A Practical Exercise in Zero-Knowledge Interactive Proofs. Master's thesis, Department of Computer Science, University of Kentucky, 1994.

[FortuneMerritt:1984:CRYPTO] Steven Fortune and Michael Merritt. Poker Protocols. In G.R. Blakley and David Chaum, editors, *Advances in Cryptology: Proceedings of CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 454–466. Springer Verlag, 1984.

Abstract: The situation is quite serious. After four years of research, there has been no satisfactory way for a group of card sharks to play poker over the phone. Until now. In this paper, we present a new method for playing 'mental poker,' discuss its significance, and mention some of the further questions it raises. Ante up. The rules for mental poker are just like regular poker, except that players communicate over the phone, and there are no physical cards. The hard part of mental poker is dealing the cards. Hands must be random and disjoint, and players should not be able to claim to have any cards but those dealt (a sleeve will hold as many 'virtual cards' as angels will fit on the head of a pin). Playing mental poker is a difficult problem for a number of reasons. The foremost reason is that it is impossible, a result due to Shamir, Rivest and Adleman. Of course, this is an information-theoretic result, and the same reference presents a method for playing mental poker that relies on the difficulty of inverting certain cryptographic transformations. Unfortunately, a cryptographic flaw allows players to

determine the color of each other's cards. This set the stage for a new implementation devised by Goldwasser and Micali, which was proven to hide all partial information (up to an explicit cryptographic assumption). Unfortunately, this implementation works only for two players, which is a very restricted kind of poker. Next, Barany and Furedi devised a protocol that permits three or more players to play poker, but only if players are not permitted to form coalitions. If two players conspire, they can learn the contents of everyone else's hands. The following section discusses this history of mental poker in more detail, outlining the key ideas, contributions and limitations of this earlier work. This paper presents a new way of playing mental poker. Unlike earlier solutions, it is secure against coalitions, permits any number of players, and uses inexpensive, highly secure cryptographic techniques. The protocol does require the participation of a trusted party to shuffle the cards. However, thereafter the trusted party does not participate in the protocol. The protocol can be easily adapted to play almost all types of poker known to the authors. Of course, poker is a metaphor for any system in which users should have only partial information about the dynamic allocation of resources. Beyond this, the poker protocol presented here takes on a broader significance because of the simple tools used in its implementation.

[GoldreichMicaliWigderson:1987:STOC] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play ANY mental game. In *Proceedings of the 19th Annual ACM Conference on Theory of Computing (STOC '87)*, pages 218–229. ACM Press, 1987.

Abstract: We present a polynomial-time algorithm that, given as a input the description of a game with incomplete information and any number of players, produces a protocol for playing the game that leaks no partial information, provided the

> majority of the players is honest. Our algorithm automatically solves all the multi-party protocol problems addressed in complexity-based cryptography during the last 10 years. It actually is a completeness theorem for the class of distributed protocols with honest majority. Such completeness theorem is optimal in the sense that, if the majority of the players is not honest, some protocol problems have no efficient solution.

[GoldwasserMicali:1982:STOC] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption & How To Play Mental Poker Keeping Secret All Partial Information. In *Proceedings of the 14th Annual ACM Symposium on Theory of Computing (STOC '82)*, pages 365–377. ACM Press, 1982.

> **Abstract:** This paper proposes an Encryption Scheme that possess the following property: An adversary, who knows the encryption algorithm and is given the cyphertext, cannot obtain any information about the clear-text. Any implementation of a Public Key Cryptosystem, as proposed by Diffie and Hellman in [8], should possess this property. Our Encryption Scheme follows the ideas in the number theoretic implementations of a Public Key Cryptosystem due to Rivest, Shamir and Adleman [13], and Rabin [12].

[Golle:2005:ITCC] Philippe Golle. Dealing Cards in Poker Games. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC '05)*, volume 1, pages 506–511. IEEE Computer Society, 2005.

> **Abstract:** This paper proposes a new protocol for shuffling and dealing cards, that is designed specifically for games of mental poker. Our protocol takes advantage of two features of poker games that are overlooked by generic card-shuffling protocols: 1) cards in poker games are dealt in rounds, with betting in-between, rather than all at once and 2) the total number of cards dealt in a game of poker is small (it depends on

the number of players but is typically less than half the deck). With these observations in mind, we propose a protocol that spreads the computational cost of dealing cards more evenly across rounds. Compared to protocols that shuffle the whole deck upfront, our approach offers a dramatic decrease in latency and overall computational cost. Our protocol is fair, private and robust. It is ideally suited for resource-constrained devices such as PDAs.

[HarnLinGong:2000] L. Harn, H.-Y. Lin, and G. Gong. Bounded-to-Unbounded Poker Game. *Electronics Letters*, 36(3):214–215, 2000.

> **Abstract:** The bounded-to-unbounded poker game is a fair poker game that can be played over the Internet. It allows both dealer and player to distribute cards in a fair and secure manner. In addition, the presented protocol assumes that the player is computationally bounded: however, the dealer is computationally unbounded.

[KurosawaKatayamaOgata:1997] Kaoru Kurosawa, Yutaka Katayama, and Wakaha Ogata. Reshufflable and Laziness Tolerant Mental Card Game Protocol. *IEICE Transactions Fundamentals*, E80-A(1):72–78, 1997.

> **Abstract:** This paper presents a reshufflable and laziness tolerant mental card game protocol. First, our protocol can reshuffle any subset of cards. For example, some opened cards and some face down cards can be shuffled together. Next, we consider two types of honest players, currently active and currently nonactive. A player is currently nonactive if he dropped out the game or he declared ″pass″ and has not declared ″rejoin″ yet. In the proposed protocol, if more than half of the players are currently active, they can play the game. In this case, the privacy of the currently nonactive players are kept secret.

[KurosawaKatayamaOgataTsujii:1990:EUROCRYPT] Kaoru Kurosawa, Yutaka Katayama, Wakaha Ogata, and Shigeo Tsujii. General Public Key Residue Cryptosystem and Mental Poker Protocols. In Ivan B. Damgård, editor, *Advances in Cryptology - EUROCRYPT '90, Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques*, volume 473 of *Lecture Notes in Computer Science*, pages 374–388. Springer Verlag, 1990.

> **Abstract:** This paper presents a general method how to construct public key cryptosystems based on the r-th residue problem. Based on the proposed method, we present the first mental poker protocol which can shuffle any set of cards. Its fault tolerant version is given, too. An efficient zero knowledge interactive proof system for quadratic non-residuosity is also shown.

[Lipton:1979] Richard J. Lipton. How to Cheat at Mental Poker. Technical Report, Computer Science Department, Berkeley University, 1979.

[Lipton:1981] Richard J. Lipton. How to Cheat at Mental Poker. Proceedings of the AMS Short Course on Cryptology, 1981.

[Pinna:2002] Michael Pinna. A Secure Card Game. BA Thesis, Gonwille & Caius College, University of Cambridge, 2002.

[Schindelhauer:1998] Christian Schindelhauer. A Toolbox for Mental Card Games. Technical Report A-98-14, Medizinische Universität Lübeck, 1998.

> **Abstract:** Mental card games are played without a trusted party and without cards. It is well known that the problem of mental card games can be solved in principle. But the schemes known so far are too messy to be used in practice. Only for the mental poker game a suitable solution is known [Crép 87] that achieves security against player coalition and complete confidentiality of a player's strategy. Here, we present a general-purpose scheme that may be used as basic toolbox for straight-forward implementations of card

games. We present a data structure for cards and decks that is secure against player coalitions and enables standard operations like picking up a card, opening it, and (re-)mixing stacks. Furthermore, we introduce tools for special operations like inserting a card into the deck, splitting the deck, parting the game. The correctness of all operations is testified by zero-knowledge proofs. Finally, we discuss security problems that are typical for mental card games and suggest solutions to enable all players maximum possible fairness.

[ShamirRivestAdleman:1979] Adi Shamir, Ronald L. Rivest, and Leonard M. Adleman. Mental Poker. Technical Report MIT-LCS-TM-125, Massachusetts Institute of Technology, 1979.

Abstract: Is it possible to play a fair game of 'Mental Poker'. We will give a complete (but paradoxical) answer to this question. We will first prove that the problem is intrinsically insoluble, and then describe a fair method of playing 'Mental Poker'.

[ShamirRivestAdleman:1981] Adi Shamir, Ronald L. Rivest, and Leonard M. Adleman. Mental Poker. *The Mathematical Gardner*, pages 37–43, 1981.

Abstract: Can two potentially dishonest players play a fair game of poker without using any cards—for example, over the phone? This paper provides the following answers: No. (Rigorous mathematical proof supplied.) Yes. (Correct and complete protocol given.)

[SooSamsudinGoh:2002] Wai Han Soo, Azman Samsudin, and Alwyn Goh. Efficient Mental Card Shuffling via Optimised Arbitrary-Sized Benes Permutation Network. In Agnes Hui Chan and Virgil Gligor, editors, *Information Security, Proceedings of the 5th International Conference (ISC 2002)*, volume 2433 of *Lecture Notes in Computer Science*, pages 446–458. Springer Verlag, 2002.

Abstract: The presumption of player distrust and untrustworthiness in mental card gaming results in the formulation of complex and compute-intensive protocols, particularly for shuffling. We present a robust, verifiable and efficient card shuffling protocol based on an optimisation of Chang-Melham arbitrary-sized (AS) Benes permutation network (PN), which can flexibly accommodates variable pack sizes, achieving optimal shuffling performance. We also outline the use of these PNs in a distributed (among h players) construction, which combines the best attributes of Abe and Jakobsson-Juels mix-net formalisms. Card shuffling can therefore be executed on a structurally simple mix-net – with only $t + 1$ PNs required for operational robustness against collusion by t cheating players, and efficient zero knowledge proofs (ZKP) to verify correct shuffling by each player. Shuffling efficiency is also enhanced by our limited application of verifiable secret sharing (VSS) on the ElGamal keys. The resultant protocol achieves an asymptotic complexity of $O(tNlgN)$ for N inputs; which is comparable or superior to previous schemes.

[Stamer:2005:WEWoRC] Heiko Stamer. Efficient Electronic Gambling: An Extended Implementation of the Toolbox for Mental Card Games. In Christopher Wolf, Stefan Lucks, and Po-Wah Yau, editors, *Proceedings of the 1st Western European Workshop on Research in Cryptology (WEWoRC 2005)*, volume P-74 of *Lecture Notes in Informatics*, pages 1–12. Gesellschaft für Informatik e.V., 2005.

Abstract: There are many wonderful protocols in cryptography which are still waiting for their realization. Here we consider efficient solutions for secure electronic card games. Our contribution seems to be the first known practical implementation that requires no trusted third-party and simultaneously keeps the players' strategies confidential. The provided open source library

LibTMCG can be used for creating secure peer-to-peer games and furthermore for some unusual applications, e.g., secure multi-party computation or simple electronic voting schemes.

[Tetikoglu:2007] Ipek Tetikoglu. The Elgamal Cryptosystem is better than the RSA Cryptosystem for Mental Poker. Master's thesis, Department of Computational Mathematics, Duquesne University, 2007.

Abstract: Cryptosystems are one of the most important parts of secure online poker card games. However, there is no research comparing the RSA Cryptosystem (RC) and Elgamal Cryptosystem (EC) for mental poker card games. This paper compares the RSA Cryptosystem and Elgamal Cryptosystem implementations of mental poker card games using distributed key generation schemes. Each implementation is based on a joint encryption/decryption of individual cards. Both implementations use shared private key encryption/decryption schemes and neither uses a trusted third party (TTP). The comparison criteria will be concentrated on the security and computational complexity of the game, collusions among the players and the debate between the discrete logarithm problem (DLP) and the factoring problem (FP) for the encryption/decryption schemes. Under these criteria, the comparison results demonstrate that the Elgamal Cryptosystem has better efficiency and effectiveness than RSA for mental poker card games.

[Wei:2014] Tzer-jen Wei. Secure and practical constant round mental poker. *Information Sciences*, 273:352–386, 2014.

Abstract: We present a new mental poker protocol, which achieves negligible probability of cheating in constant round. All of previous secure mental poker protocol use L-round zero-knowledge protocols to ensure the probability of successful active cheating to be $O(2^{-L})$. Our protocol uses a

different way to verify the integrity of the shuffle. The cryptosystem and the basic structure of our protocol is based on Castellà-Roca's mental protocol, which is very efficient and secure. The L-round zero-knowledge shuffle verification is replaced by a checksum-like framework. There are two kinds of checksums used in our shuffle: linear checksum and double exponentiation. The "linear checksum" is used to make sure that every card in the deck is distinct. The "double exponentiation checksum" is used to make sure that every card has a legitimate face value. The security can be proved under DDH assumption. The probability of successful cheating is negligible, even if the adversary can actively corrupt the majority of players. It is also very fast. For a 9 player game, the computation cost of our shuffle is comparable to the L-round verification with $L = 4$. The time complexity of our shuffle is $\Theta(MN + N^2)E$ (compares to $\Theta(MN^2L)E$ for a L-round shuffle), where N is the number of players, M is the number of cards, and E is the computation cost of one modular exponentiation. The communication cost is also reduced. Compares to the L-round protocol we based on, number of messages is reduced from $\Theta(N^3L)$ to $\Theta(N^2)$, and the total length of messages is reduced from $\Theta(N^2L(M + N))\eta$ to $\Theta(MN2)\eta$, where η is the length of an encryption key. For a 9-player game, our shuffle requires only 53% messages, and total length of messages is only 7% (compares to the case $L = 30$ and all L rounds of shuffle verification are allowed to run in parallel). It is the first constant round mental poker protocol that is provably secure and efficient enough to satisfy the practical needs. The probability of successful cheating is negligible.

[WeiWang:2012] Tzer-jen Wei and Lih-Chung Wang. A fast mental poker protocol. *Journal of Mathematical Cryptology*, 6(1):39–68, 2012.

Abstract: In this paper, we present a fast and se-

cure mental poker protocol. The basic structure is the same as Barnett & Smart's and Castellà-Roca's protocols but our encryption scheme is different. With this alternative encryption scheme, our shuffle is not only twice as fast, but it also has different security properties. As such, Barnett & Smart's and Castellà-Roca's security proof cannot be applied to our protocol directly. Nevertheless, our protocol is still provably secure under the DDH assumption. The only weak point of our protocol is that reshuffling a small subset of cards might take longer than Barnett & Smart's and Castellà-Roca's protocols. Therefore, our protocol is more suitable for card games such as bridge, most poker games, mahjong, hearts, or black jack, which do not require much partial reshuffling.

[Yung:1982] Mordechai Yung. K-Player Mental Poker. Master's thesis, Tel-Aviv University, 1982.

[Yung:1984:CRYPTO] Mordechai Yung. Cryptoprotocols: Subscription to a Public Key, the Secret Blocking and the Multi-Player Mental Poker Game. In G.R. Blakley and David Chaum, editors, *Advances in Cryptology: Proceedings of CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 439–453. Springer Verlag, 1984.

Abstract: Investigating the capabilities of public key and related cryptographic techniques has recently become an important area of cryptographic research. In this paper we present some new algorithms and cryptographic protocols (Cryptoprotocols) which enlarge the range of applications of public key systems and enable us to perform certain transactions in communication networks. The basic cryptographic tools used are Rabin's Oblivious Transfer Protocol and an algorithm we developed for Number Embedding which is provably hard to invert. We introduce the protocol "Subscription to a Public Key", which gives a way to transfer keys over insecure communication channels and has useful applications to cryptosystems.

We develop the “Secret Blocking Protocol”, specified as follows: ‘A transfers a secret to B, B can block the message. If B does not block it, there is a probability P that he might get it. ($1/2P \leq 1$, where we can control the size of P). A does not know if the message was blocked (but he can find out later)’. The classic cryptotransaction is the “Mental Poker Game”. A cryptographically secure solution to the “Multi Player Mental Poker Game” is given. The approach used in constructing the solution provides a general methodology of provable and modular “Protocol Composition”.

[ZhaoVaradharajan:2005:ITCC] Weiliang Zhao and Vijay Varadharajan. Efficient TTP-Free Mental Poker Protocols. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC ’05)*, volume 1, pages 745–750. IEEE Computer Society, 2005.

Abstract: Zhao et. al proposed an efficient mental poker protocol which did not require using a trusted third party (TTP). The protocol is efficient and suitable for any number of players but it introduces a security flaw. In this paper, we propose two mental poker protocols based on Zhao’s previous work. The security flaw has been removed and the additional computing cost is small.

[ZhaoVaradharajanMu:2003] Weiliang Zhao, Vijay Varadharajan, and Yi Mu. A Secure Mental Poker Protocol Over The Internet. In Chris Johnson, Paul Montague, and Chris Steketee, editors, *ACSW Frontiers 2003, Proceedings of the Australasian Information Security Workshop*, volume 21 of *Conferences in Research and Practice in Information Technology*, pages 105–109. Australian Computer Society, 2003.

Abstract: An effcient and secure mental poker scheme is proposed in this paper. It is based on multiple encryption and decryption of individual cards. The protocol satisfies all major security requirements of a real mental poker. It gets rid of the Card Salesman and guarantees minimal effect due

to collusion of players. The protocol is secure and more effcient compared with other known protocols. The strategies of players can be kept confidential with the introduction of a Dealer. The protocol is suitable to be implemented in an on-line card game.