MENTAL CARD GAMING PROTOCOLS SUPPORTIVE OF GAMEPLAY VERSATILITY, ROBUSTNESS AND EFFICIENCY

by

SOO WAI HAN

Thesis submitted in fulfilment of the
requirements for the degree
of Master of Computer Science

March 2003

ACKNOWLEDGEMENTS

My heartfelt gratitude to my supervisors Dr. Azman Samsudin, Mr. Alwyn Goh and Assoc. Prof. Dr. Syed Sibte Raza Abidi for their dedication, valuable guidance and tremendous support. I am deeply indebted to Mr. Alwyn Goh, who sparked my interest in cryptography, for devoting much of his time and expertise to help me in this research and in writing. This work would not have come into existence without him. Dr. Azman, who has kept an eye on the progress of my work, has also inspired me with his thought-provoking ideas and constructive advice.

I have learnt a lot from Wai Kuan, Chin Kiong and Geong Sen. Thanks for the many enlightening discussions and constant motivations. To friends at the HIRG lab, especially Kok Meng, Yu-N, Stephen and Selva, I am grateful for their friendship, laughter and sympathetic ears. A special thank goes to Yu-N, the walking dictionary. I am also extremely fortunate to have many dear friends who always provide timely and necessary distractions, besides being a great source of support and encouragement. A very partial list includes Kim, Li Chuen, Mee Mee, Keng Tung, Mosleh and Mohan.

I would like to acknowledge the School of Computer Sciences and Institute of Postgraduate Studies for the financial support through the Special Scholarship (Biasiswa Khas) Schemes, and for offering an excellent research environment and kind assistance.

Above all, I am most thankful to my family, especially my parents, for their unconditional love, understanding and support. Also to my husband Soon Ann, I thank him for his love and patience, and for sharing my life.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LISTS OF ABBREVIATIONS

ANDOS	All-or-nothing disclosure of secrets
AS	Arbitrary-sized
DDH	Decision Diffie-Hellman
DKG	Distributed key generation
DL	Discrete logarithm
DLEP	DL equality proof
DLP	DL problem
D-PEP	Disjunctive PEP
EC	Elliptic curve
HVZKP	Honest verifier ZKP
IF	Integer factorisation
IFP	IF problem
NIZKP	Non-interactive ZKP
OAS	Optimised AS
PEP	Plaintext equivalence proof
PK	Public key
PN	Permutation network
PRP	Prime residuosity problem
QR	Quadratic residuosity
QRP	QR problem
ROM	Random oracle model
SS	Secret sharing
TTP	Trusted third party
VSS	Verifiable SS
ZKIP	Zero-knowledge interactive proof
ZKP	Zero-knowledge proof

ABSTRAK

PROTOKOL PERMAINAN KAD MENTAL YANG MENYOKONG KESERBAGUNAAN, KETEGUHAN DAN KECEKAPAN

Permainan kad mental merupakan protokol kriptografi yang membolehkan permainan yang disahkan adil di kalangan parti-parti jauh yang penyangsi dan berpotensi menipu. Permainan kad ini setidak-tidaknya patut menyokong—tanpa memperkenalkan parti ketiga yang dipercayai (TTP)—rahsia kad, pengesanan penipuan dan keselamatan bersyarat ke atas pakatan pemain. Tambahan kepada keperluan asas ini, kami meninjau isu-isu permainan kad mental yang berkaitan dengan fungsian permainan, keteguhan operasional dan kecekapan implementasi. Pengkajian kami diberangsang oleh potensi permainan berasaskan komputer dan rangkaian yang melewati batas kemampuan kad fizikal, terutamanya pembongkaran maklumat terperinci kad (seperti warna, darjat, simbol atau kebangsawanan) sambil merahsiakan nilai keseluruhan kad tersebut. Namun, perangkaian menyasarkan protokol kepada serangan penyahsambungan (sama ada diniatkan mahupun tidak), dan tipu muslihat yang lain. Oleh itu, keteguhan operasional adalah intrinsik kepada permainan kad mental yang praktikal, membenarkan permainan berakhir dengan sempurna oleh suatu ambang pemain yang jujur. Kecekapan pengkomputan tidak kurang kepentingannya, memandangkan kesulitan—akibat daripada perseteruan di kalangan pemain dan the ketidakhadiran TTP—dalam memastikan kerahsiaan sifat rawak yang merupakan teras kepada permainan seumpama ini.

Tesis ini membentangkan suatu skema permainan kad mental yang selamat dan adil dengan menggunakan kad bercirikan atribut, yang mana keselamatan berlandaskan kriptosistem homomorfik and probabilistik, keteguhan menerusi mekanisme perkongsian rahsia ambang

yang berdasarkan polinomial, dan pengocokan kad yang cekap berteraskan rangkaian pilihatur bersaiz arbitrari (AS PN). Deskripsi bercirikan atribut merealisasikan pembongkaran atribut (dan bukan kad) yang mustahil dalam permainan fizikal; struktur datanya yang fleksibel mendorong keserbagunaan permainan. Dalam pada itu, keselamatan pada tahap protokol bergantung kepada kriptosistem logaritma diskret dan kriptografi ambang. Kedua-dua ini diintegrasikan dalam operasi-operasi lazim seperti membancuh, mendapatkan atau memberi kad, dan pembongkaran atribut kad. Keteguhan permainan berasas ambang juga menyumbang kepada toleransi terhadap sebilangan kecil penyelewengan protokol (umpamanya pakatan haram serta keguguran pemain). Kami memajukan operasi yang paling memakan kuasa pengkomputan, yakni pengocokan kad, dengan menyusulkan suatu pengoptimuman ke atas AS PN, dan mengadunkan struktur minimum suatu rangkaian-aduk berteraskan PN dengan kecekapan pengkomputan pada tahap suis, yang amat menarik dari segi operasi praktikalnya. Protokol kami mencapai kecekapan $O(\eta\mu \lg\mu)$ bagi input bersais μ and pemain sebanyak η, berbandingkan $O(\kappa\eta\mu)$ bagi penyelesaian yang sedia-ada, dengan κ sebagai parameter keselamatan.

ABSTRACT

Mental card games are cryptographic protocols which permit verifiably fair gameplay among a priori distrustful and potentially untrustworthy remote parties and should minimally provide—without the introduction of a trusted third party (TTP)—for card confidentiality, fraud detection and conditional security against collusion. In addition to these basic requirements, we explore into gameplay functionality, operational robustness and implementation efficiency issues of mental card gaming. Our research is incited by the potential of computer-based and network-mediated gameplay beyond the capability of physical cards, particularly fine-grained information disclosure (such as colour, rank, symbol or courtliness) with preservation of card secrecy. On the other hand, being network connected renders the protocol susceptible to (accidental or intentional) disconnection attack, as well as other malicious behaviours. Operational robustness is therefore intrinsic to practical mental card gaming, allowing the completion of game by a configurable threshold of trustworthy players. Computational efficiency is no less important, considering the difficulties—due to the adversarial players and the absence of a TTP—of ensuring secret randomisation at the heart of these games of chance.

This thesis presents a secure and fair mental card gaming scheme, featuring attribute-based cards, with security predicated on homomorphic probabilistic cryptosystem, robustness via polynomial-based threshold secret sharing mechanisms and efficient shuffling underpinned by arbitrary-sized (AS) permutation networks (PN). The attribute-based description realises physically impossible attribute (as opposed card) disclosure; its flexible data structure promotes gameplay versatility. Meanwhile, protocol-level security is reliant on discrete logarithmic cryptosystem and threshold cryptography, both of which are integrated into commonly

encountered operations such as shuffling, drawing or giving cards, and card-attribute disclosure. The inherent threshold-based gameplay robustness also provides tolerance against a minority of protocol deviation (such as collusion and player dropouts). We improve on the most computation-expensive operation, which is card shuffling by proposing an optimisation on an AS PN, and incorporating structural minimisation of a PN-based mix-net with switch-level computation efficiency, which is of interest from the viewpoint of practical operability. Our protocol achieves $O(\eta\mu \lg\mu)$ efficiency for μ inputs and η players, compared to $O(\kappa\eta\mu)$, with κ being the security parameter, of existing solution.

Chapter 1

INTRODUCTION

1.1 Online Gaming

Internet connectivity as the medium for high value transactions provides a substantive motivation for gaming companies. According to New York worldwide investment banking firm Bear, Stearns & Co. Inc., there is an estimate of 1700 virtual gaming sites on the internet. Even with the current problem of major credit card companies rejecting online gaming transactions, still, $4.2 billion in revenues was projected by Bear Stearns for 2003, pared down from a previous growth forecast of $5 billion (Ader, 2001; Bear, Stearns & Co. Inc., 2002). Besides credit card problem, other major impediments are the questionable security of private information, fairness of online games and trust in the gaming site operators.

In physical gaming environment, players can scrutinise the exchange of physical tokens or money to ensure correctness, but not in online gaming. Devoid of face-to-face contact, players need to be reassured of the privacy of personal information (such as credit card number), security of gaming transactions (such as betting, payoffs) and fairness of gaming operations (such as card shuffling, dice rolling, random number generation). These requirements demand protocols that, at least, endorse secure online payment, commitment of actions, verifiability or audit trail. In addition, the gaming solution should be robust to handle disconnections—either voluntary interruption by players or a simple network breakdown. However, the manifestation of security in the current gaming environment usually just revolves around payment.

Conventional gaming solutions—casino softwares developed by leading suppliers such as Starnet, Boss Media, Cryptologic and Microgaming—rely on the existence of a trusted third party (TTP), or the dealer, to facilitate gameplay. This TTP would then possess knowledge of the game-state, which provides an unfair advantage to the site operator and also renders it an attractive target for subversion. TTP-centred protocols would therefore not be satisfactory to a priori distrustful players and are furthermore insufficiently generic. Such protocols would, for example, not be useful for games in which the site operator is also an active participant. One approach applied in recent software by SCYTL (2002) is to reduce the amount of trust on the site operator by supporting multiparty computation for random events (like card shuffling, dice casting), such that these results are only obtainable with the consent of all involved parties. However, this gives rise to the concern of information availability in the event of disconnection.

This thesis explores the online gaming issues from the perspective of fair game playing, in particular protocols required to support card games—usually referred to as *mental card game* protocols. To circumvent the issue of trust, we divert from the regular client-server framework to a peer-to-peer environment, without assuming any trusted dealer or operator. Thus, this necessitates protocols that enable a high degree of transactional versatility, security, reliability and efficiency.

1.2 Mental Card Gaming

Mental card game is a classic problem where cryptography can be fruitfully applied. The notion of security within mental card gaming context would need to address:

- *Self-enforcement*: without unconditional dependence on a TTP, in either the actual protocol or any adjudication after the completion of the protocol.
- *Cheat resistance*: so that attempts are straightforwardly discovered.
- *Privacy*: of a player's hand, the common deck, as well as the player's strategy.

- *Collusion resistance*: whereby no useful information can be gained about the other players' secrets than what can be inferred from the knowledge of the collusion.
- *Operational robustness*: against dropped sessions or *sore loser* behaviours.

Meanwhile, viability of the mechanisms and protocols for the intenet or wireless (such as mobile network) setting should consider:

- *Computational feasibility*: for implementation on devices of varying computing capabilities.
- *Functional versatility*: in order to be broadly applicable to a wide range of card games, even to the extent of enabling operations impossible in physical gameplay.

The first four security properties are generally considered to be the universal requirements in our area of interest. Thus, we present our research into mental card gaming among distrustful and potentially untrustworthy players, exploring gameplay functionality, operational robustness and implementation efficiency issues, while ensuring operational fairness (which concerns card confidentiality and fraud detection):

- *Gameplay functionality*: We note that mental gaming—without presumption on player trustworthiness—is probably always going to result in algorithmically complex and computationally expensive protocols. Our motivation therefore stems from the potential of computer-based and network-mediated gameplay impossible (or at least highly impractical) with physical cards, in particular, configurable information disclosure (of colour, rank, symbol or courtliness) without divulging the entire card.

- *Operational robustness*: The dependence on distributed computation—rather than player localisation at a gaming table—does, however, raise the issues of protocol hazards related to player errors, malicious behaviours (such as collusion or frauds due to unfavourable cards) or even simple network disconnection (be it accidental or otherwise). Practical mental

gaming must therefore be fault-tolerance, usually implemented via polynomial-based secret sharing (SS) techniques (Blakley, 1979; Shamir, 1979), thereby allowing game completion conditional on a threshold of honest players.

- *Implementation efficiency*: Computational efficiency is no less important, particularly given the varied computing powers of the players and the emergence of mobile gaming. This effort is especially focussed on shuffling operation due to its complexity.

As mention earlier, the absence of a trusted dealer results in the formulation of complex and compute-intensive protocols, which is aggravated for card shuffling, as it requires the deck to be composed of every player's shuffled output for maximum fairness. Earlier approaches to mental card gaming (Goldwasser & Micali, 1982; Crépeau, 1986, 1987; Schindelhauer, 1998) have been too computationally heavy to satisfy viability due to usage of bitwise encryption based on quadratic residuosity (QR) computation, which incurs logarithmic message expansion. Although in those schemes card shuffling is a simple protocol for every player to sequentially apply a private random permutation to the set of cards, it is unfortunately coupled with expensive zero-knowledge proofs (ZKP) to verify correctness of the player's behaviour. Furthermore, in attempt to preclude collusion, Crépeau (1986, 1987) and Schindelhauer (1998) permit recovery of card only with cooperation by all players, which is operationally fragile depending on players not resorting to *sore loser* behaviour like dropping-out, and the reliability of network connection.

Nevertheless, the QR computation can be extended to higher order (r^{th}) residues (Kurosawa *et al.*, 1990; Benaloh, 1994), thereby enabling more efficient wordwise encryption. This approach is implemented by Kurosawa *et al.* (1997), who also introduced the notion of gameplay robustness via Benaloh (1986) verifiable SS (VSS) with a threshold selected for tolerance against both collusion and dropouts. Shuffling, in their scheme, adopts mix-net mechanism of Ogata *et al.* (1997) such that the input-output correspondence is obscured even to parties

involved in the mixing. However, the required VSS on every card as well as intermediate values would still result in high overheads on storage and computation.

We propose a secure and robust mental gaming scheme with attribute-based cards, inspired by Schindelhauer (1998) binary card representation, in which security is predicated on homomorphic probabilistic cryptosystem based on discrete logarithm (DL) (ElGamal, 1985), and robustness via polynomial-based threshold SS (Shamir, 1979). Our formulation facilitates various operations such as card shuffling, drawing, transfer and card-attribute disclosure, the last of which is a distinctive feature of our attribute-based card representation. Card shuffling, the most compute-expensive operation by a wide margin, is given special attention. For efficient implementation, we employ robust mix-net mechanism (Abe, 1999; Jakobsson & Juels 1999; Abe & Hoshino, 2001) with arbitrary-sized (AS) permutation network (PN) (Chang & Melham, 1997), so as to minimise the resultant overhead while still maintaining a high degree of operational robustness (Soo & Samsudin, 2002; Soo *et al.*, 2002).

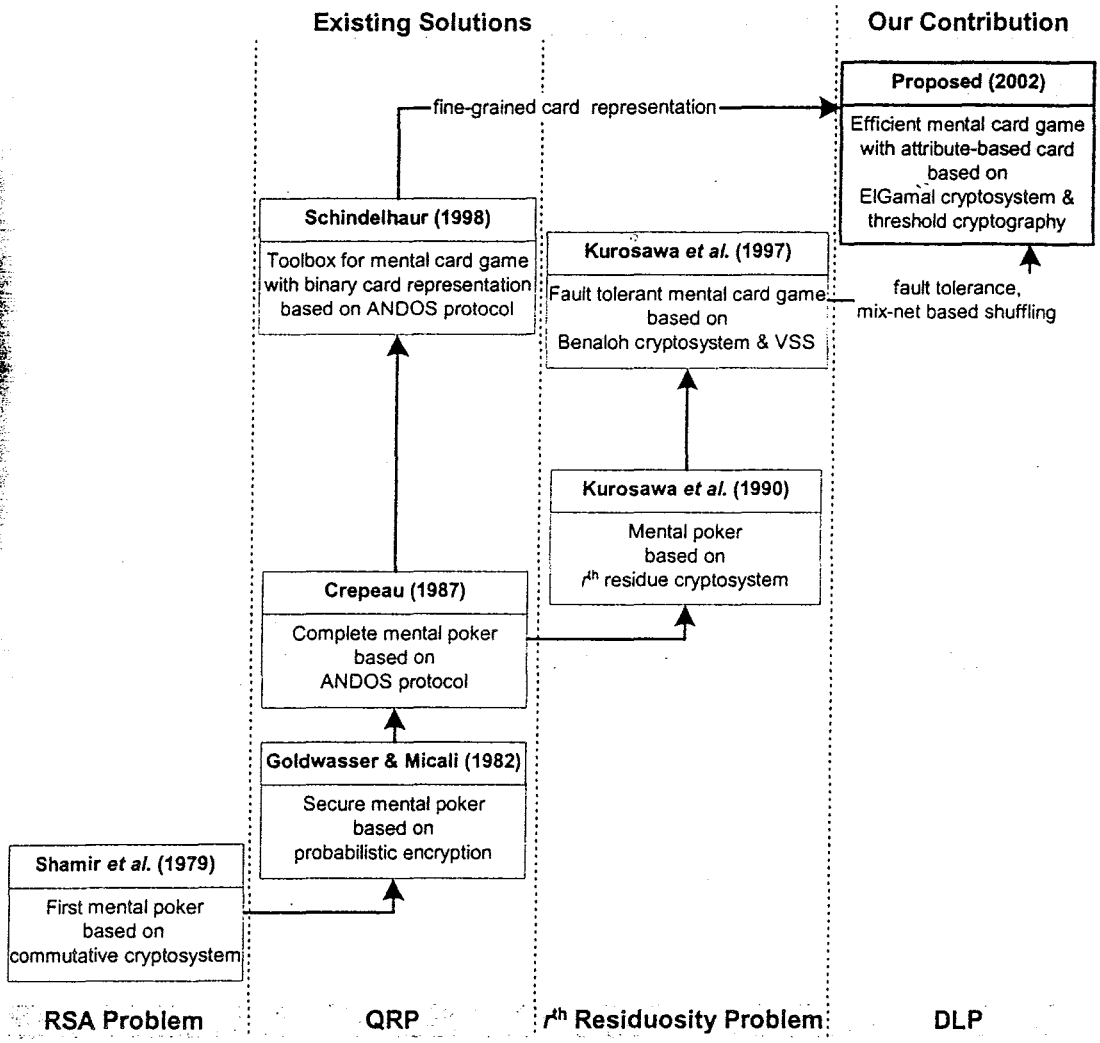

Figure 1.1: Direction in mental card gaming schemes

1.3 Thesis Contributions

1.3.1 Problem Statement

Based on the cursory overview of existing mental card gaming schemes as presented in Table 1.1, we conclude that the hitherto most complete and efficient solution is Kurosawa *et al.* (1997). However, the scheme still suffers a few shortcomings, which provides the motivation for our research work:

- *Inappropriate encryption algorithm*: Employment of wordwise encryption based on the difficulty of r^{th} residuosity problem (where r is a prime) does gain much performance improvement from the previous QR bitwise computation. However, due to r being reliant on the number of cards in play—thereby resulting in an $r \geq 53$ for a standard deck—the corresponding decryption complexity of $O(r)$ becomes impractical as r grows (for example in cases where a double-deck is in play).

- *Ineffective robustness support*: The scheme allows completion of game—ensuring correctness of outcome—under the presence of a minority of faulty players, which is achieved via distribution of representative cryptographic parameters (or card information) among the players, such that reconstruction of card is possible conditional on a threshold of t active honest players. Unfortunately, such SS incurs heavy computation, communication and storage, for generating, transferring and keeping each card-dependant secret-shares respectively; the worst-case scenario being card shuffling, which involves processing the whole deck of μ cards.

- *Inefficient shuffling operation*: Based on Ogata *et al.* (1997) robust verifiable mix-net mechanism, its efficiency is however decreased by the underlying cryptosystem and the sharing of every card. Coupled with its associated interactive correctness proofs, which computation and communication needs are logarithmic in the length of the security parameter κ, the operation suffers $O(\kappa\eta\mu)$ cost for an error probability of $2^{-\kappa}$, η players and a deck of μ cards.

- *Inextensible gameplay*: Computer-based gaming is interesting in that it allows game tokens that cannot physically exist or, in other words, execution of familiar games in a manner impossible with physical cards. This results from implicit predication of gameplay on card representation. A simple set of $\{1, 2, \ldots, 52\}$ for the standard deck is insufficient to express

a card, unlike the later formulation by Schindelhauer (1998) featuring binary card representation that enables bit level information disclosure, via a *glue-and-separate* operation. Schindelhauer, however, does not provide details on verifiability of the operation.

- *Infeasible correctness proving*: Usage of interactive proof techniques (Goldwasser *et al.*, 1985)—via a series of questions and answers—to assert the correctness of the gaming protocols can convince the verifier with overwhelming probability, but at the expense of high bandwidth consumption. Specifically, for a negligible failure probability of $O(2^{-\kappa})$, the prover would have to engage in κ conversations with the verifier. Thus, the resultant proof system requires a very high round complexity. What is more, due to the need for interaction, validity of the proof does not extend beyond the players, thus the proof does not convince external verifiers such as the bank.

Table 1.1: Brief survey of existing solutions

Scheme	Improvements	Limitations
Shamir *et al.* (1979)	First mental poker	2-player only Leakage of partial information
Goldwasser & Micali (1982)	Secure mental poker for multiplayer	Logarithmic message expansion Revelation of strategy
Crépeau (1987)	Complete mental poker supporting confidentiality of player's strategy	Logarithmic message expansion Susceptible to disconnection attacks
Kurosawa *et al.* (1990, 1997)	Robust mental poker/card game with efficient wordwise encryption and configurable operational robustness	VSS of high overheads Costly interactive proof system Local verifiability
Schindelhauer (1998)	Extended mental card gaming functionality based on binary card representation	Logarithmic message expansion Susceptible to disconnection attacks Local verifiability

1.3.2 Proposed Solution

Our research emphasises on efficiency, robustness and gameplay functionality as a solution to the problems identified in the previous subsection:

- *DL cryptosystem*: Contrary to conventional reliance on the difficulty of integer factorisation (IF) (or the determination of r^{th} residuosity) for security (Shamir *et al.*, 1979; Goldwasser &

Micali, 1982; Crépeau, 1986, 1987; Kurosawa *et al.*, 1990, 1997; Schindelhauer, 1998), we build our framework upon the equivalently secure DL cryptography; its major attractiveness being facilitation of straightforward portability to an elliptic curve (EC) DL (Miller, 1986; Koblitz, 1987) basis which allows more compact storage and faster computation.

- *VSS on decryption key*: We also depart from Kurosawa *et al.* (1997) formulation in our limited use of VSS only on the decryption key. Thus, instead of dealing (with respect to generation, distribution and storage) with a handful of card-dependant secret-shares each time a card is in play, player only needs to handle one single key-share, generated and distributed at setup stage, thereby resulting in substantial overhead reduction while still providing robustness against collusion and disconnection.

- *Shuffling based on PN*: Our shuffling mechanism (Soo & Samsudin, 2002; Soo *et al.*, 2002) follows Kurosawa *et al.* (1997) in their use of robust verifiable mix-net, but adopts mix-net based on PN constructions (Abe, 1999; Jakobsson & Juels 1999; Abe & Hoshino, 2001) that are more appropriate for small input size (like a deck of cards). However, instead of relying on Benes PN (Benes, 1965; Waksman, 1968)—the constituent element of the mix-nets—which rigidly requires the input size to be a power of 2, we employ an optimised PN that can accommodate arbitrary number of input in conjunction with Abe (1999) structural optimisation and Jakobsson-Juels (1999) efficient correctness proofs.

- *Attribute-based card representation*: To support operation such as partial information disclosure, we extend Schindelhauer (1998) data structure to an attribute-based card representation in which each attribute can be individually disclosed without complete card exposure or transfer of card ownership. This is essentially a cryptographically enabled *card peeking* operation, and is rendered secure and verifiable via polynomial-based VSS (Feldman, 1987).

- *Non-interactive ZKPs*: The three-move ZKP (the commit-challenge-response protocol) of Goldwasser *et al.* (1985) used in Kurosawa *et al.* (1997) can be collapsed into one single move based on the Fiat-Shamir (1986) technique to output a transitive proof transcript. This would also enable offline correctness verification, contributing to a much lower round complexity, as well as public verifiability.

1.3.3 Methodology

This thesis therefore demonstrates the construction of a mental card gaming framework via integration with the following building blocks or cryptographic constructs:

- *ElGamal (1985) cryptosystem*: a discrete logarithmic encryption scheme to ensure confidentiality of cards, particularly to provide indistinguishability of facedown cards. It also accommodates secret exchange of information between players. Its probabilistic nature is most desirable given the small message space of card game (for example 52 cards) and its homomorphic property supports randomisation of ciphertexts, allowing action hiding.

- *Pedersen (1991a) distributed key generation (DKG) protocol*: enables formulation of ElGamal key-pair by all players distributively. As the joint private key is unknown to any player, decryption therefore requires the collaboration of a subset of honest players. The generation of key-pair and the decryption process are publicly verifiable based on Feldman (1987) VSS technique. It should be noted that the DKG protocol are executed once per gaming session (during the setup stage) and thereafter the joint private key remains obscure, even during decryption; the cards are recovered via a combination of decryption shares instead of using the decryption key.

- *Mix-nets based on PN*: for efficient shuffling of cards, in which our mix-net construct or shuffling mechanism (Soo & Samsudin, 2002; Soo *et al.*, 2002) capitalises on:

- *Chang and Melham (1997) AS PN*: for support of arbitrary deck sizes. We further scale down the number of switches required based on Waksman (1968) to reduce computation; the resultant optimised AS (OAS) PN is the fundamental component of our mix-net.
- *Abe (1999) mix-net*: for structural optimisation. Up to t cheaters among η players can be tolerated by employing minimally $t + 1$ PNs, whereby each player will be assigned some columns or stages of the networks, rather than working on a whole PN individually.
- *Jakobsson and Juels (1999) millimix*: for compute-efficient correctness proofs that operate on a per switch basis.

- *Feldman (1987) VSS*: provides the commitment and verification mechanisms for linkage—via (n, n)-SS of Shamir (1979)—of a card with its attributes. In this case, the card being the secret is only recoverable if all attributes are known. Nevertheless, each attribute is verifiable to be related to a card and hence its correctness.

- *Fiat and Shamir (1986) proof technique*: facilitates transformation of an interactive ZKP into its non-interactive version without jeopardising the security of the original proof (Feige & Shamir, 1990). In a nutshell, the trick is to transform the interactive challenges into hashed values of multiple commitments, so as to enable offline verification. In our scheme, this is applied into the proofs of Chaum-Pedersen (1992) for equality of DL and variants of Schnorr (1991) signature scheme for equivalence of plaintexts.

1.3.4 Contributions

This thesis makes several contributions to mental card gaming particularly pertaining to efficiency and gameplay extensibility, which can be measured along these dimensions:

- *Mental card gaming framework*: We have formulated a secure gaming framework based on the hardness of DL Problem (DLP), which security level is comparable to the IF problem (IFP). Furthermore, DLP can be defined over an EC group, which is more difficult to solve than over a residue class ring. Cryptosystem based on EC is therefore believed to be more secure, with significantly reduced computing, storage and bandwidth overheads.

- *Card data structure*: We have designed a meaningful data structure for cards—a binary string composed of each card attribute's bits—adaptable to different card games, with fine-grained information disclosure is also possible.

- *Gaming operation*: We have introduced physically impossible gameplay of *card peeking* operation using our attribute-based cards. The correctness and verifiability of the operation is underpinned by Shamir (1979) SS techniques. Such limited information disclosure would, for instance, provide for poker gameplay impossible with physical cards via controlled and nuanced ambiguity with respect to possession of an ordinary, straight or royal flush.

- *Shuffling efficiency*: We have reduced the costs—with respect to computation, communication and storage overheads—for card shuffling, which is rendered efficient via gameplay-flexible AS PNs with optimisation based on Waksman (1968) and incorporation of the most attractive features of Abe (1999) and Jakobsson-Juels (1999) formulations.

- *Gameplay fairness*: We have ensured fair playing and the correctness of gaming outcome with the provability—via efficient ZKP and VSS methods—of every important game step. This eliminates the need to reveal cards, which would expose a player's strategy, at the end of the game. Verifiability is universally available as long as the communication channel is publicly accessible.

- *Game management*: We have outlined robust protocols, catering for overall game management, particularly concerning player's participation and withdrawal, supporting flexible tradeoffs between collusion resistance and accommodation of dropouts.

- *Implementation feasibility*: We have considered the resources requirement and tradeoffs for viable implementation. In particular, we avoid unnecessary cumbersome interaction by using non-interactive proving techniques in ZKPs and VSS, although we have to bear with an increased bit size for the challenge (hash function) to preclude offline attacks. Nevertheless, non-interactivity saves on computation and communication, and is therefore well-suited for online gaming, mobile gaming or other lightweight platforms.

1.4 Thesis Organisation

The rest of this thesis is organised as follows:

Chapter 2 gives the essential cryptographic background for comprehension and appreciation of mental card gaming; some of these basic primitives or protocols are building blocks for the construction of our solution. There are four main concepts discussed: public-key (PK) cryptosystems, threshold cryptography, ZKP and mix-nets. The chapter also contains some definitions and notational conventions used in the technical part of this thesis.

Chapter 3 discusses existing schemes, beginning with a brief review of the literature related to mental gaming, which is intended as an overview of the area. We then focus on four noteworthy schemes: Shamir *et al.* (1979) being the first mental poker protocol, Crépeau (1987) as deemed complete for mental poker, Kurosawa *et al.* (1997) with its introduction of gameplay robustness and Schindelhauer (1998) for having an innovational card representation. For each scheme, we present its models and the cryptographic building blocks used. Some significant card operations

are outlined next, followed by a high-level analysis of the scheme. The chapter concludes with a summary of our findings and a discussion of insights gained.

Chapter 4 synthesises ideas from the previous two chapters to construct mental card gaming protocols supportive of gameplay versatility, robustness and efficiency. We detail a few fundamental card operations: shuffling cards, drawing a card, giving a card and disclosing card-attribute, the last of which fully demonstrates the flexibility of our attribute-based card representation. Our innovation of mix-net underpinning shuffling operation (Soo & Samsudin, 2002; Soo *et al.*, 2002) is carefully delineated, which incorporates our optimisation of Chang-Melham (1997) AS PN, Abe (1999) mix-net architecture and Jakobsson-Juels (1999) correctness verification.

Chapter 5 presents rigorous proofs that the properties claimed, namely privacy, fairness, robustness and verifiability, are attained accordingly. We also provide an analysis of the required complexity and compare the performance with existing scheme, Kurosawa *et al.* (1997) in particular. Finally, Chapter 6 concludes the thesis, reflects on our contributions, and proposes directions for future research work.

Chapter 2

CRYPTOGRAPHIC BACKGROUND

2.1 Introduction

In this chapter, we discuss some cryptographic protocols necessary for the understanding of mental card gaming, which at the same time are also useful as building blocks for the construction of our proposed scheme. This review also serves as a means of introducing notations. We begin with some PK encryption schemes, which provide privacy and security for the gaming protocols. We then look at threshold cryptography, a tool for supporting distributed trust among mutually suspicious card players, and the notion of ZKP as one of the anti-fraud mechanisms. We also discuss the application of PN-based mix-nets with respect to card shuffling. Lastly, we conclude the chapter with a discussion on the relation of these tools with our proposed scheme.

2.2 Public-Key Cryptosystem

Encryption is fundamental in mental card gaming to ensure privacy, which is much needed, especially in the representation for the backs of cards to support their indistinguishability, and in exchanging cards operation between players. PK cryptosystem—first identified by Diffie and Hellman (1976)—involves different keys for encryption and decryption. Let K be the key space and $k \in K$, we denote $E_k(m, \cdot)$ and $D_k(m, \cdot)$ the encryption-decryption transformations on plaintext m using the public and private keys; it is infeasible to compute the latter from the former.

For implementation of mental gaming protocols, a few properties are desired from the underlying PK encryption scheme, considering the small message space of the playing cards. Let R be the randomisation set, M and C the plaintext and ciphertext spaces respectively.

Probabilistic encryption: This notion was invented by Goldwasser and Micali (1982), with the encryption function given by E_k: $M \times R \rightarrow C$ while decryption is D_k: $C \rightarrow M$, such that

$$D_k(E_k(m, r)) = m \text{ for } \forall m \in M, r \in R.$$

Decryption only requires that E_k be partially invertible as the recovery of the random number is not necessary. Thus, for large R, a plaintext may have many—exponential in the security parameter—different ciphertexts.

Semantic security: It is infeasible for a passive adversary with polynomially bounded computing power to obtain partial information about the plaintext from the ciphertext; and the encryptions of an arbitrary (known) pair of messages is indistinguishable (Yao, 1982; Goldwasser & Micali, 1984; Micali *et al.*, 1988).

Homomorphic property: For $\forall(m_1, r_1), (m_2, r_2) \in M \times R$, let $(m_1, r_1) \otimes (m_2, r_2) \triangleq (m_1 m_2, r_1 r_2)$,

$$\Rightarrow E(m_1, r_1) \otimes E(m_2, r_2) = E(m_1 + m_2, r_0) \text{ for some } r_0;$$

that is, the decryption of a sum of ciphers is the sum of the corresponding plaintexts. This algebraic property—discovered by Benaloh (1987)—allows direct operation on cryptograms without knowledge of the corresponding decryption functions.

Randomisability of ciphertext: By depending only on public parameters, a ciphertext can be changed, $C \times R \rightarrow C$, while preserving the plaintext. Furthermore, the ciphertexts $c = E(m, r)$ and $c' = E(c, r')$ are indistinguishable.

In the following subsections, we review three PK cryptosystems related to mental card gaming that satisfy the requirements above, the last of which is employed in our proposed scheme.

2.2.1 Goldwasser-Micali Cryptosystem

This scheme by Goldwasser and Micali (1982, 1984) achieves randomness via bitwise probabilistic encryption of a message, based on the trapdoor hardcore predicate of QR. We first introduce some basic number theoretic backgrounds and notations before defining the computational problem:

- $\mathbb{Z}_n \in [0, n)$, a group under addition modulo n; $\mathbb{Z}_n^* = \{x: \gcd(x, n) = 1, x \in \mathbb{Z}_n\}$, a multiplicative group modulo n.
- $QR_n = \{z: \exists x \in \mathbb{Z}_n^*, z \equiv x^2 \bmod n\}$, set of *quadratic residue* modulo n and $QNR_n = \mathbb{Z}_n^* \setminus QR_n$, the set of *quadratic non-residue* modulo n.
- The *Legendre symbol* of x mod p where p is a prime and $x \in \mathbb{Z}_p^*$, is defined as

$$J_p(x) = \begin{cases} +1 & \text{if } x \in QR, \\ -1 & \text{otherwise.} \end{cases}$$

- Given the prime factorisation of a composite integer n, $n = \prod_{i=1}^{k} p_i^{e_i}$ where p_i are distinct primes and $e_i \geq 1$, *Jacobi symbol* of x mod n is defined as $J_n(x) = \prod_{i=1}^{k} J_{p_i}(x)^{e_i}$.

The cryptosystem is semantically secure assuming the intractability of *QR Problem* (QRP):

Definition 2.1. Let n be an odd composite integer of unknown factorisation and given $z \in \mathbb{Z}_n^*$ having $J_n(z) = 1$, QRP is to decide whether $z \in QR_n$.

Goldwasser-Micali scheme has the following properties:

Private key: two large random prime, p and q

Public key: $n = pq$ and $y \in QNR_n$ with $J_n(y) = 1$

Plaintext: $M = m_1 m_2 \ldots m_t$, a binary string of length t

Encryption: $C = c_1 c_2 \ldots c_t$ where $c_i \leftarrow y^{m_i} x_i^2 \bmod n$; $x_i \in_R \mathbb{Z}_n^*$ ($\in_R$ denotes uniform random selection.)

Decryption: For $i = 1$ to t, $m_i \leftarrow \begin{cases} 0 & \text{if } J_p(c_i) = 1, \\ 1 & \text{otherwise.} \end{cases}$

The cryptosystem satisfies stringent security requirements. However, its bitwise encryption induces logarithmic message expansion, thus hinders its practicality.

2.2.2 Benaloh Cryptosystem

Exploiting related trapdoor techniques based on the common algebraic setting of high degree residuosity classes, Benaloh (1987, 1994) presented a generalisation of Goldwasser-Micali scheme to allow arbitrary prime r values, thereby enabling wordwise encryption. The motivation is to reduce the required bitwise computation via selection of a residue r so as to be only slightly larger than any possible plaintexts. Therefore, the size of a plaintext represented by a single ciphertext is much larger, reducing the expansion rate. Before proceeding to the computational problem, we describe some related backgrounds and notations (Benaloh, 1987):

- $\mathbb{Z}_n^r = \{z: \exists x \in \mathbb{Z}_n^*, z \equiv x^r \bmod n\}$, set of r^{th} *residue* modulo n and $\overline{\mathbb{Z}_n^r} = \mathbb{Z}_n^* \setminus \mathbb{Z}_n^r$, the set of r^{th} *non-residue* modulo n.
- $R_{r,n,y}^s = \{w: w \equiv y^s z \bmod n, w \in \mathbb{Z}_n^*, z \in \mathbb{Z}_n^r\}$, the set of all elements of *residue class* s with respect to the consonant triplet (r, n, y). $[\![w]\!]$ denotes the residue class where w is a member of $R_{r,n,y}^s$ for a unique s.
- A triplet (r, n, y) of integers is *consonant* if and only if $y^s \in \mathbb{Z}_n^r \Leftrightarrow s \equiv 0 \bmod r \Rightarrow R_{r,n,y}^0$.

Benaloh cryptosystem attains semantic security assuming the intractability of *Prime Residuosity Problem* (PRP):

Definition 2.2. For every prime r, the PRP addresses the determination of r^{th} residuosity modulo n or the residue class for random elements in $\mathbb{Z}_n^*$; PRP is computationally difficult when n is a composite integer of unknown factorisation.

It is easy to see that for the minimally simple case of $r = 2$, PRP is equivalent to QRP (cf. subsection 2.2.1, Definition 2.1). We review Benaloh's cryptosystem as follows:

Private key: two large random prime, p and q, such that $r \mid p\text{-}1$, $r^2 \nmid p\text{-}1$ and $r \mid q\text{-}1$

Public key: $n = pq$ and $y \in \overline{\mathbb{Z}_n^r}$

Plaintext: $M \in \mathbb{Z}_r$

Encryption: $C = E(M) = y^M x^r \bmod n$, where $x \in_R \mathbb{Z}_n^*$. Note that $\bigcup_{M=0}^{r-1} \{E(M)\} = \mathbb{Z}_n^*$. In fact, $E(0), \ldots, E(r-1)$ forms a partition of $\mathbb{Z}_n^*$.

Decryption: $M = j$ if $C^{(p-1)(q-1)/r} = (y^{(p-1)(q-1)/r})^j \bmod n$ where $j \in \mathbb{Z}_r$

Based on the fact that ciphertext $z \in E(0)$ if and only if $z^{(p-1)(q-1)/r} \equiv 1 \bmod n$, $[\![C]\!]$ can be decided. For small r, we can perform exhaustive search for the smallest $M \in \mathbb{Z}_r$ such that $y^{-M} C \bmod n \in E(0)$. This process can be accelerated by precomputing $(y^{(p-1)(q-1)/r})^j \bmod n$ for $\forall j \in \mathbb{Z}_r$, thus decryption can be a mere look-up process on $C^{(p-1)(q-1)/r} \bmod n$. This method, however, is impractical as r grows due to its $O(r)$ complexity. Hence, for moderate sized r, the baby-step giant-step algorithm (Knuth, 1973)—a combination of exhaustive search and table look-up—can be applied to lower decryption complexity to $O(\sqrt{r})$.

Obviously, the computational problem of r^{th} residuosity has much potential. Zheng *et al.* (1988, 1989) presented further generalisation of PRP investigating the case for odd r, which was later extended by Kurosawa *et al.* (1990) for any r. Recent cryptosystems belonging to this family of techniques by Naccache and Stern (1997), Okamoto and Uchiyama (1998) and Paillier (1999)

achieve even higher efficiency admitting dramatically reduced expansion rate, by exploring residuosity of smooth degree over $\mathbb{Z}_n^*$, prime degree p over $\mathbb{Z}_{p^2q}^*$ and composite degree over $\mathbb{Z}_{n^2}^*$ respectively.

2.2.3 ElGamal Cryptosystem

ElGamal (1985) scheme leverages on the hardness of DL in a prime order group. Nevertheless, it can also operate over EC group (Miller, 1986; Koblitz, 1987) to take advantage of the increased speed and reduced key size. The cryptosystem is probabilistic but unlike Goldwasser-Micali and Benaloh cryptosystems, randomisation is added to the whole message instead of at bit or byte level. We present some necessary backgrounds and notations to facilitate understanding of further discussion:

- x mod n is said to have *order* k if k is the smallest positive integer such that $x^k \equiv 1 \bmod n$. Similarly, a group generated by x has order k mod n means k is the lowest power of x such that $x^k \equiv 1 \bmod n$.
- Given large primes p and q such that $q \mid p - 1$, G_q is a unique subgroup of prime order q of $\mathbb{Z}_p^*$, if for some generator g, $G_q = \{g^x \bmod p : x \in [1, q]\} \subset \mathbb{Z}_p^*$.
- In other words, g is a *generator* of G_q if the powers of g reproduce the subgroup. Since G_q's order is prime, every element in $G_q \backslash \{1\}$ is a generator. Note that g is of order $p - 1$.

ElGamal cryptosystem is semantically secure under the *Decision Diffie-Hellman* (DDH) assumption (Brands, 1993; Boneh, 1998):

Definition 2.3. Informally, DDH problem for G_q is to distinguish between two distributions $\langle g^a, g^b, g^{ab} \rangle$ and $\langle g^a, g^b, g^c \rangle$ where $a, b, c \in_R \mathbb{Z}_q$; DDH assumption states its infeasibility.

For a typical setting, we let $q = 2p + 1$. As the QR of any given x mod p can be computed easily, thereby gaining one bit of information, we set $G_q = QR_p$ in $\mathbb{Z}_p^*$ to eliminate such information

leakage. ElGamal cryptosystem is shown as follows, with p, q and g considered as system parameters:

Private key: $x \in_R \mathbb{Z}_q$

Public key: $y = g^x \bmod p$

Plaintext: $M \in G_q$. Note that $M \notin G_q$ can be mapped onto G_q via manipulation of J_p.

Encryption: $C = (a, b) = (My^\alpha, g^\alpha)$ for some $\alpha \in_R \mathbb{Z}_q$

Decryption: $M = a/b^x$

Its multiplicative homomorphic property, $E(M_1) \otimes E(M_2) = E(M_1M_2)$, allows for plaintext-preserving random re-encryption of a ciphertext $C = (a, b)$ via computation of $C' = (a, b) \otimes (a', b')$ where $(a', b') = E(1) = (y^\beta, g^\beta)$ with $\beta \in_R \mathbb{Z}_q$. The correlation, or the plaintext equivalence of C and C' is denoted as $C \equiv C'$.

2.3 Threshold Cryptography

The idea of threshold cryptography in mental gaming is motivated by the standard presumption of player distrust and untrustworthiness, necessitating distribution of trust among the players to protect information or computation. It is, however, reasonable to presume a majority of honest players in which the integrity of gameplay can be derived from. The fundamental ingredient of threshold cryptography is SS (Blakley, 1979; Shamir, 1979), particularly VSS (Benaloh, 1986, 1987; Feldman, 1987; Pedersen, 1991b). However, these *threshold schemes* (which will be outlined in subsections 2.3.1 and 2.3.2) usually involve a TTP for secret generation and recovery, with consequence risk of single point of failure.

To preclude this problem, *threshold cryptosystems*, the non-trivial extension of threshold schemes, avoid the use of TTP. The main component of a threshold cryptosystem is DKG (such as Pedersen, 1991a; Canetti *et al.*, 1999; Gennaro *et al.*, 1999; Jarecki & Lysyanskaya, 2000 for

DL-based cryptosystems), with application to threshold signature or decryption protocols; the fault-tolerant distribution is defined by the underlying PK cryptosystem. As computation, storage and reconstruction of the secret key are not performed at a single location, confidentiality and availability are assured in the presence of malicious attacks or local computer failure. We discuss DKG in subsection 2.3.3 and threshold decryption, which provides robustness in our proposed scheme, in 2.3.4.

2.3.1 Threshold Secret Sharing

(t, n)-threshold SS ($t \leq n$) addresses the division of a secret into n shares such that any subset of shares equal to or exceeding configurable size t (the threshold) enables secret reconstruction, while $t - 1$ or fewer discloses no information on the secret. Shamir's (1979) formulation of this notion is based on *polynomial interpolation*, which is the unambiguous parameterisation of $(t - 1)$-degree polynomial $f(x)$, which can succeed only if t distinct coordinate points $(x_i, f(x_i))$ are available. This allows secret definition using the polynomial intercept $f(0)$. The scheme is outlined below:

- *Secret Distribution*: Shares related to secret $S \in \mathbb{Z}_p$, where p is a prime chosen by the dealer, is distributed to the participants. The dealer first defines a $(t - 1)$-degree polynomial $f(x) = \sum_{k=0}^{t-1} a_k x^k$ over $\mathbb{Z}_p$ with $f(0) = a_0 = S$ and other coefficients, $a_{k\neq 1} \in_R \mathbb{Z}_p$ randomly generated. Each secret-share is a point on $f(x)$, that is, $(x_i, f(x_i))$ with $x_i \neq 0$, which is subsequently dealt to the shareholders via a private channel.

- *Secret Recovery*: This requires possession of at least t distinct points $(x_i, f(x_i))$. The encoding polynomial can be computed via Lagrange interpolation $f(x) = \sum_{j=1}^{t} f(x_j)\left(\prod_{k=1,k\neq j}^{t} \frac{x - x_k}{x_j - x_k}\right)$ thereby enabling disclosure of $f(0) = S$.

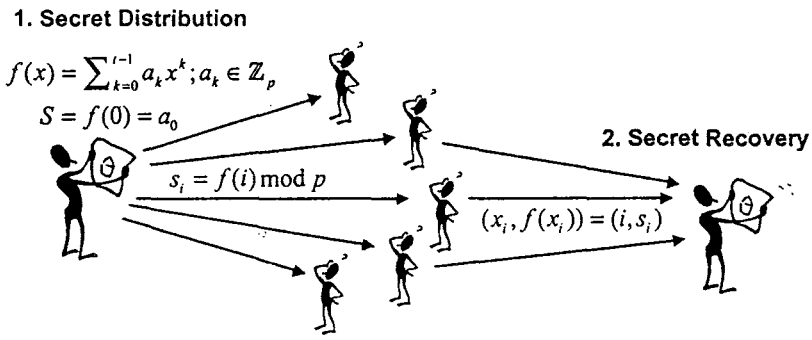

Figure 2.1: Threshold secret sharing scheme

Shamir threshold scheme is *perfect* since collaboration of at most $t - 1$ shareholders has no advantage in guessing the secret over an outsider. However, a misbehaving dealer can give incorrect shares to sabotage secret reconstruction. The solution to this problem lies in VSS.

2.3.2 Verifiable Secret Sharing

VSS, first introduced by Chor *et al.* (1985), to ensure meaningfulness of the shares without revealing them, achieving SS in the presence of malicious dealer. Benaloh (1986, 1987) later observed that Shamir's threshold scheme have (+, +)-homomorphic property—any linear combination of secret-shares is itself a share of the linear combination of secrets. So, if t secrets S are decomposed into shares s,

$$S_1 \rightarrow s_{1,1}, \ldots, s_{1,\eta}$$

$$\ldots$$

$$S_t \rightarrow s_{t,1}, \ldots, s_{t,\eta}$$

$$\text{then } \sum_{i=1}^{t} S_i \leftarrow \sum_{i=1}^{t} s_{i,1}, \cdots, \sum_{i=1}^{t} s_{i,1} .$$

This facilitates a simpler mechanism for VSS as computation can be performed on secret-shares without the need to construct the secret.

The basic idea for VSS is to have the potentially untrustworthy dealer commits to the SS polynomial—where the free term defines the secret S—by committing the coefficients using a function that is probabilistic and homomorphic, which can be any of the schemes discussed in

section 2.2. Due to the homomorphic properties, the verification function will convince the shareholders that their shares lie on a polynomial of degree $t-1$, thus identify a unique secret.

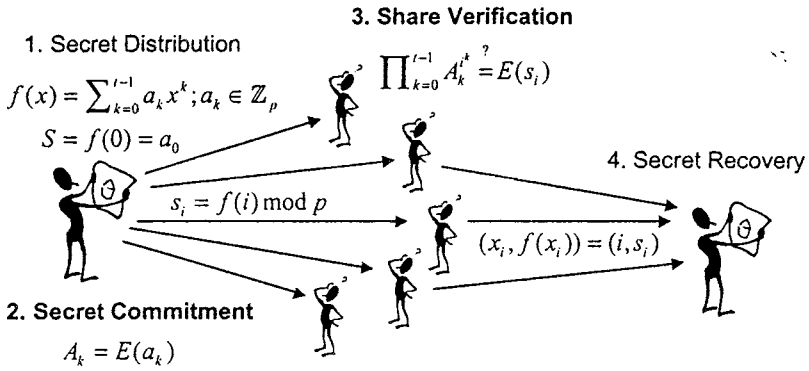

Figure 2.2: Verifiable secret sharing scheme

We are interested in *non-interactive* VSS schemes for its communication efficiency. We outline two different flavours of non-interactive VSS techniques: Feldman (1987), which is based on the hardness of computing DL over $\mathbb{Z}_p$ and Benaloh (1994) which relies on the intractability of r^{th} residuosity problem (or the factorisation of an RSA (Rivest *et al.*, 1978) modulus).

Feldman-VSS

The solution assumes SS polynomial $f(x)=\sum_{k=0}^{t-1} a_k x^k$ over $\mathbb{Z}_q$ with the secret distribution phase similar to Shamir's SS scheme (cf. subsection 2.2.3). To check for a consistent dealing, the commitment and verification procedures employ the use of DL-based probabilistic homomorphic encryption scheme, such as ElGamal (cf. subsection 2.2.3):

- *Secret Commitment*: The dealer broadcast public values $A_k = g^{a_k} \bmod p$ for $k = 0, \ldots, t-1$.
- *Share Verification*: Shareholder computes $g^{f(x_i)} \stackrel{?}{=} \prod_{k=0}^{t-1} A_k^{x_i^k}$, exploiting the homomorphic properties of the exponentiation function, $g^{\alpha} g^{\beta} = g^{\alpha\beta}$.

Note that the value $g^{a_0} \bmod p$ is revealed. Thus, the semantic security can only be stated on the computational assumption of g^{a_0} (the intractability of DL problem). Pedersen (1991b) presented