Scalable, Tax Evasion-free Anonymous Investing

Shouhuai Xu[1] Moti Yung[2] Gendu Zhang[1]

[1]Dept. of Computer Science, Fudan Uni., P. R. China
{shxu, gdzhang}@fudan.edu.cn

[2]CertCo, NY, NY, USA. moti@cs.columbia.edu

revised, Jan. 14, 2000

Abstract

Motivated by the open problems of [MS99], we proposed a *scalable* (i.e., one signature is enough to certify a trading/election transaction independent of the number of involved shares), *tax evasion-free*, anonymous investing scheme via the new notion introduced in this paper, namely *anonymous account*. While our trading model is *fair* to both the sellers and the buyers, a mechanism for the law enforcers to *actively* detect abuses (i.e., brute force, inflation, insider trading, and money laundering) is also provided. We also discuss some useful extension to realize various preferred trade-offs.

1 Introduction

"Anonymous investing" was introduced by MacKenzie and Sorensen in [MS99] to enable anonymous trading and secret investment, thereof realizing better protection for the privacy of the investors. In the same paper, they also proposed a solution based on the new concept called *eshare*, whereas the underlying components are borrowed from e-cash schemes. Nevertheless, their solution, as noticed by the authors themselves in [MS99], is neither *scalable* nor *tax evasion-free*. In this paper, we propose a new notion called *anonymous account*, via which we construct a practical "anonymous investing" scheme. While our solution is of scalability and tax evasion-freeness, further objectives are also implemented.

1.1 Background

Privacy is increasingly concerned in the digital economy of the virtual Internet world. Though *customer anonymity* has already been somehow well-studied in the context of electronic payments (refer to, [C82, BGK95, CMS97, CFN88, FTY96, FTY98, JY96, M96]), privacy of the investors in capital markets is only recently paid attention in [MS99]. The key difference between the two applications lies in the fact that there are no concepts of *anonymous dividending* and *anonymous voting* we have to realize in e-cash context. It should also be noted that *anonymous voting* in "anonymous investing" is different from the *secure voting* in a general election scheme, because we not only need to hide the votes of the individual participants, but we wish further not to reveal their identities. On the other hand, "anonymous investing" has also the potential to be abused (say, insider trading and money laundering), which suggests us the effort in e-cash [vSN92].

Let's briefly review the solution proposed in [MS99]. In their model, the certificate authority (CA) maintains an anonymous e-cash scheme with trustee-revocable anonymity, from whom the investors withdraw *zero-value* "coins" that can only be *paid* to "purchase" certified public keys. Therefore, the anonymity of a certificate can be revoked by the trustees indirectly from the corresponding *zero-value* coin.[1] With such certificates, the investors can anonymously trade and vote according to the shares of some companies they hold. Actually, a share/eshare is denoted via a doubly-signed certificate, i.e., certified by the company on the investor's certificate issued by the CA. The companies who sell eshares need to maintain public databases for their own eshares.

To see the drawbacks of the solution, we need to get a little into techniques. Assume investor Bob firstly withdraws a *zero-value* coin c (i.e., obtained from c', the view of the CA, via the technique simi-

[1] While it seems more modular to have a separate CA certifying identities [MS99], the investors' identities can be illegally revoked by some participant, other than the intended CA, from the e-coins used to buy shares. Fortunately, such an illegally revocation is impossible in our solution.

lar to blind signature [C82, FTY98]) from the CA, and then pays c back to the CA who will certify Bob's public key p_{Bob}. We denote such a certificate $cert_{Bob} \stackrel{def}{=} SIG_{CA}(p_{Bob})$, and its anonymity can be revoked from the *zero-value* coin c, as in e-cash. This is the very reason to assume the existence of a conditionally anonymous e-cash system. Specifically, an eshare of IBM held by Bob is denoted as $SIG_{IBM}(cert_{Bob})$, i.e., $SIG_{IBM}(SIG_{CA}(p_{Bob}))$, in the database maintained by IBM. If IBM has 10^8 eshares, its database has exactly 10^8 records. When Bob intends to sell this eshare, the ownership can be easily proved/checked as he knows the secret key corresponding to the public key p_{Bob}. Unfortunately, in the model of [MS99], if Bob wants to sell his 1000 IBM eshare, 1000 signatures have to be signed (by Bob) and verified (by IBM) against (possibly) 1000 certificates. In this case, Bob may have to setup 1000 balance accounts at the bank to which he redeems the e-checks (signed by the company after successful selling), if not in physical cash. This can be further worsen as it is impossible (even Bob himself) to foretell how many eshares (therefore, the corresponding certificates) to be bought. On the other hand, the fact that Bob has many certificates will make it technically impossible to generate accurate capital gains report for him, without which there may be potential tax evasion. This is further complicated by the normal yet frequent buying-and-selling processes (e.g., firstly buying 1000 eshares at the price of \$10, then selling 500 eshares at the price of \$20). Therefore, to realize *scalable* and *tax evasion-free* anonymous investing system is the open problem proposed in [MS99].

Additionally, the trading model in [MS99] is disqualified due to the *unfairness* in the transactions. More specifically, after Bob broadcasting an offer for his eshare $SIG_{IBM}(SIG_{CA}(p_{Bob}))$ at price d, Alice needs to broadcast her bidding at price d' with respect to exactly Bob's offer, what is the worst is that whether this transaction will take effect or not depends *only* on Bob's mind, and nothing else (i.e., even Alice). This is contrast to the function of financial markets to bring buyers and sellers together and to provide a price discovery mechanism for the assets being traded [FSW99].

1.2 Our Result

We introduce a new notion, namely "anonymous account" (AA) with which a money balance and a share balance are associated at the (say, New York) stock exchange. To setup such an account, investor Bob needs only to apply a "conditionally anonymous certificate" (CAC) from the certificate authority who needs only to transparently maintain its own proactively signing infrastructure with the techniques in [HJJKY95, JY97] for a case study. Our solution succeeds in addressing the two open problems proposed in [MS99]: *scalability,* only *one* signature is enough to perform a trading/voting transaction[2] independent of the number of share involved, and *tax evasion-freeness.* While our trading model is also fair to both the seller and the buyer, thereof a real market in the sense of [FSW99], a new mechanism introduced in this paper will entitle the law enforcers to *actively* detect abuses (e.g., money laundering). As we will see, our solution can also be extended to realize various preferred trade-offs.

Remarks: 1. The "Certified Anonymous Public Key" (CAPK) used in [MS99], is similar to the "conditionally anonymous certificate" (CAC) adopted in the current paper. However, the anonymity of a CAPK in [MS99] is indirectly implemented through some anonymous e-cash system, whereas it is directly realized by the certificate authority in ours. Moreover, it is technically possible in our solution for any participant other than the intended certificate authority to revoke *illegally* the anonymity of any investor, therefore the bank in our solution will not bear the potential legal risk (refer to [Ba98]).

2. The *active* detection mechanism of this paper may be independently interesting in other context. For example, jewellers always dare not to publish their real name and address for the prevention of robbery, whereas the government may hope to know the advertisements by whom they are posed (say, to ensure that the jewels are not "dirty").

1.3 Outline.

In next section we will describe our model of anonymous investing, which is somewhat different from the one in [MS99]. We present the basic scheme of our solution in section 3, and its properties in section 4. Extension to the basic scheme, and a comparison between it with the [MS99] solution is unfolded in section 5. We conclude with open problem in section 6.

2 The Model

We model *anonymous investing* market a stock exchange (**SE**, as in [FSW99]), which dynamically

[2]The voting scheme may be independently useful in any other anonymous, authentic, yet universally verifiable elections.

maintains an Anonymous Bulletin Board (ABB, where the validated bids/offers of the investors are posted)[3]. That is, we assume the existence of anonymous communication channel between the investors and the **SE**, similar to [MS99, S96]. Every investor **I** setups an *anonymous account* (AA, with which his money balance and share balance are associated) via his "conditionally anonymous certificate" (CAC) issued by the **CA** using some proactive cryptography (for the sake of a case study, we adopt the methods in [HJJKY97, JY97] whereas many other techniques can be used instead) of quorum-revocation anonymity.

Functionally, the stock exchange consists of four components: **SEC** (Stock Exchange Center, the core one responsible for completing and cancelling trading requests posted on the ABB according to certain rules), **SEE** (Stock Exchange Election, the one responsible for handling voting and dividending according to the regulations), **SET** (Stock Exchange Taxation, the one keeping all the transaction transcripts for the sake of taxation and abuse detection), and **SEV** (Stock Exchange Verification, the one responsible for verifying the validity of certain bids/offers, and posting those valid requests on the ABB).

We assume that all investors trust that there never be a quorum servers in the **CA** infrastructure illegally conspiring to reveal their anonymity, and **SE** (thereof, all its components) honestly does everything according to certain rules/regulations independent of the current paper. Technically we assume that neither DLOG (i.e., DSS [NIST91] and Schnorr [S91]) nor RSA [RSA78] signature is existentially forgeable under adaptive chosen message attack [GMR88].

We use $SIG_Y(\cdot)$ to denote the signing function (possibly thresheld and proactivized) of entity Y whereas $ENC_X(\cdot)$ the secure encryption function under the public key of participant X.

2.1 The Goals

We extend the objectives of an anonymous investing system proposed in [MS99] to include *tax evasion-freeness*, and *active detection* (i.e., against brute force, inflation, insider trading, and money laundering). Therefore, we realize:

Unforgeability: The "conditionally anonymous certificate" (CAC) is existentially unforgeable.

Over-trading prevention: Any over-selling or over-buying can be prevented.[4]

Over-trading framing-freeness: No participants (including the **SE** and the **CA**) can successful frame an investor for any over-trading transaction.

Traceability: The *anonymous investing* scheme supports three kinds of passive traceabilities: (1) From an *anonymous account* (AA) to the corresponding investor ID; (2) From investor ID to the corresponding *anonymous account* (AA); (3) Whether an *anonymous account* (AA) is corresponding to certain investor ID.

Revocability: Any traced *anonymous account* (AA) can be blacklisted or frozen.

Anonymity: The probability for any coalition of participants not including a quorum **CA** servers to determine the identity of the owner of a AA/CAC is negligible.

Anonymous voting: Each anonymous investor should be able to vote exactly once per share (i.e., authentic), and the votes should be universally verifiable.

Tax evasion-freeness: Tax evasion is impossible for any investor.

Active detection: The system itself provides the law enforcers an *active* detection mechanisms against abuses including brute force, inflation, insider trading, and money laundering.

3 The Basic Scheme

3.1 The Idea

Each investor **I** applies a "conditionally anonymous certificate" (CAC) from the **CA**, via which he setups a *anonymous account* (AA) at the stock exchange **SE**. With such a AA, the investor can deposit his money via either physical money or unconditionally anonymous e-cash. Every time **I** wants to trade some shares at certain price, he signs such a request verifiable against his CAC and sends it to **SEV** who will validate or invalidate this *request* according to the status of his money and share balance. For example, if the investor is bidding for some shares without enough money balance or offering shares more than his share balance afford to, it is invalidated. A *request* is validated if it is not invalidated, and a validated request will be posted on the ABB. **SEC** will

[3] Refer to [MS99] for further description of the properties of an ABB. We also do not rely on any strict timing of posts (as in [MS99, S96]) to guarantee security because an adversary seeing a user's post may insert a new post before anyone else seeing that post.

[4] Double-trading is a special type of over-trading.

be responsible for performing all the transactions indicated by the validated requests posted on the ABB (e.g., if there is a match in price for a pair of selling and buying requests), therefore transferring money for such a successful transaction. **SET** generates the capital gains reports for all anonymous investors via their *anonymous accounts* respectively, and **SEE** is in power for all voting processes (e.g., assuring one vote per share).

3.2 Investor's Setting Up

The following two protocols are necessary for every investor, but only once.

Protocol 1: Investor **I** obtains a "conditionally anonymous certificate" (CAC) from the **CA** who transparently maintains a proactive cryptography based signing infrastructure [HJJKY97, JY97].

1. **I** shows his normal certificate (alternatively, any valid ID) to the **CA**.
2. After checking the validity of that certificate (or ID), **I** and **CA** engage in a protocol to obtain a CAC (key, r, s) on his public key (say, Schnorr public key $key \stackrel{def}{=} g^x$ in certain mathematical group [S91]).

Protocol 2. The investor opens an *anonymous account* (AA) at the stock exchange, **SE**.

1. **I** shows his CAC (key, r, s) to **SE**.
2. **SE** checks the validity and ownership of this anonymous certificate (e.g., via a signature on a fresh challenge).
3. **SE** associates that CAC to that AA randomly chosen by **I** (or **SE**). Every time now on, if any one claims that he is the owner of some AA, authentication is requested.

3.3 Depositing at the Anonymous Account

Protocol 3. The investor deposits physical money or e-money obtained from certain unconditionally anonymous payment system independent of the current paper at his *anonymous account*, AA.

1. **I** deposits directly some physical money (alternatively, unconditionally anonymous e-money) at his AA.

3.4 Buying Shares

Protocol 4. An investor **I** signs a buying request $SIG_I(buying, AA, name, price, quantity)$ with intention to buy *quantity* (say, 100) shares of *name* (say, IBM) at the *price* (say, \$10 per share) at the payment of the *anonymous account* AA.

1. **I** sends a request, $SIG_I(buying, AA, name, price, quantity)$, to **SEV**.
2. **SEV** checks the semantics of the signature (i.e., if it is valid against the "conditionally anonymous certificate" (CAC) associated with the claimed AA, and if $price * quantity \leq mbalance_{AA}$, where $mbalance_{AA}$ is money balance at AA. If ok, **SEV** posts it on the ABB.
3. **SEC** will decide honestly whether this buying request being done or not. If there is a successful trading, it will perform all the corresponding work (i.e., debiting the buyer's money balance and crediting the his share balance), whereas **SET** will record the transaction transcripts.

3.5 Selling Shares

Protocol 5. **I** signs a selling request $SIG_I(selling, AA, name, price, quantity)$ with intention to sell *quantity* (say, 100) shares of *name* (say, IBM) at the *price* (\$10 per share) at the *anonymous account* AA.

1. **I** sends his request, $SIG_I(selling, AA, name, price, quantity)$, to the **SE**.
2. **SEV** checks the semantics of the signature (i.e., if it is valid against the CAC associated with the claimed AA, and if $quantity \leq sbalance_{AA}$, where $sbalance_{AA}$ is the share balance at AA. If ok, **SEV** posts it on the ABB.
3. **SEC** will decide honestly whether this selling request being done or not. If there is a successful trading, it will perform all the corresponding work (i.e., crediting the seller's money balance and debiting his share balance), whereas **SET** will record the transaction transcripts.

3.6 Dividending

Protocol 6. Dividending can be realized by **SEE** who will retrieve all the shareholders of the intended shares of certain company (say, IBM).

1. **SEE** lists all the shareholders with the corresponding quantities from the account database (maintained by the **SE** rather than by the company, IBM, in [MS99]) and dividends according to the given process (say, \$0.5 per share, therefore crediting the money balance of all the corresponding *anonymous accounts*).

3.7 Voting

As mentioned in the introduction, the voting scheme should be anonymous, authentic, and universally verifiable.

Protocol 7: Investor **I** posts a signed ballot to **SEE** who will check and validate/invalidate it. We assume there are m candidates.

1. **I** posts the signed vote $SIG_I(voting, AA, candidate_1, quantity_1, \cdots, candidate_m, quantity_m)$, to the **SEE** implying that he intends to support $candidate_i$ with $quantity_i$, where $i = 1, \cdots, m$.

2. **SEE** checks the semantics of this signed voting paper, i.e., the freshness, the validity of the signature against the "conditionally anonymous certificate" (CAC) associated with the claimed *anonymous account* AA, and $\sum_{i=1}^{m} quantity_i \leq sbalance_{AA}$, where $sbalance_{AA}$ is the share balance at AA. If ok, it is a valid ballot, and is posted on the anonymous bulletin board (ABB) or broadcasted.

3.8 Taxing

The basic process for taxation, though different from here to there, may be that the tax agency will go to the stock exchange (alternatively, the investors themselves declare their incomes) to impose duties. The specific tax law is independent of the current paper, and we only focus on the calculation of precise dutiable income.

Protocol 8: The stock exchange taxation (**SET**) prepares all the precise reports for the dutiable incomes based on the transaction transcripts for the taxation agency (**TA**).

1. **SET** prepares the dutiable incomes for all anonymous investors for **TA**.

2. **TA** imposes duties according to the law.

3.9 The Active Detection Mechanism

This technique is introduced to entitle the law enforcers to *actively* detect certain abuses (i.e., brute force, inflation, insider trading, and money laundering), therefore implementing fail-stop [P96] at the system level.

3.9.1 Detection Brute Force

As the stock exchange (**SE**) maintains a central database for the investors, we assume there are satisfactory mechanisms to protect the integrity of the database. If the signing key of the **CA** is brute forced (i.e., via either brute force attack or social engineering, even it is protected through the proactive cryptography mechanism), it may be abused to launder money by opening many anonymous accounts that are traced to nobody. Let $\sum_{CAC}$ denote the number of anonymous certificates having been issued, $\sum_{CAC}^{revocation}$ the number of the certificates having been revoked, and $\sum_{AA}$ the number of anonymous accounts. If $\sum_{CAC} - \sum_{CAC}^{revocation} < \sum_{AA}$, there must be some counterfeiting of certificates.

3.9.2 Detection Inflation

There are two types of inflation attacks, namely issuing extra "conditionally anonymous certificates" (i.e., the **CA** may illegally issue CACs to criminal organizations to launder money) and issuing extra "credit" (e.g., some investor can buy shares more than his money balance afford to pay). It is rather simple to *actively* block such two serious attacks in our model.

Let $\sum_{application}$ be the total number of applications (including re-application after cancelling a compromised certificate), $\sum_{CAC}$ the number of "conditionally anonymous certificates" having ever been issued (including also the certificates having been revoked). If $\sum_{CAC} > \sum_{application}$, then there exists a certificate inflation attack.

If the investor is allowed by the **SE** to buy shares more than his money balance afford to pay, or to sell shares more than his share balance, this will result sever problems in the economy. A natural approach to address this is to audit periodically the transaction records against the involved money/shares balances.

3.9.3 Detection Inside Trading and Money Laundering

All the monitoring and audit techniques adopted in the physical world can be seamlessly integrated into our scheme, though anonymously. For example, if one (anonymous) investor always gains a high profit

margin (say, 1000%), there may be some inside trading. On the other hand, the records of the transactions transcripts can be used to assure the income of any investor from the stock market. Such transcripts is useful for the law enforcers to detect laundering [MW98].

4 The Claims

We claim the properties of the basic scheme in the following theorems, and the sketched proof of **Theorem 1** is presented in **Appendix A**, whereas **Theorem 2** can be directly deduced from the discussion in section 3.8.

Theorem 1 *The basic anonymous investing scheme achieves unforgeability, over-trading prevention, over-trading framing-freeness, traceability, revocability, anonymity, anonymous voting, and tax evasion-freeness.*

Theorem 2 *The basic anonymous investing scheme entitles the law enforcers to actively detect abuses including brute force, inflation, insider trading, and money laundering.*

5 Extension and Discussion

In our basic scheme, we assume everyone is allowed to hold just one anonymous certificate/account, based on which we show the available control, efficiency, and scalability. However, as all the anonymous transactions completed by the same investor are *linkable*, this may (arguably) compromise the anonymity of (some) investors. Though such concerns are mentioned in the literature, to the best of our knowledge, no researches in this direction have been published (say, to lead the identities of the customers via data mining). Fortunately, the basic scheme can be easily adapted to provide better (i.e., unlinkable) anonymity, while most (i.e., possibly losing something) of the properties realized in the basic scheme are preserved.

The obvious extension is to allow one to hold $m > 1$ anonymous certificates/accounts. Therefore, while all the transactions associated with the same account are linkable, the transactions associated with different accounts are unlinkable, and the *active* detection mechanism (i.e., against brute force, inflation, insider trading, and money laundering) are still preserved, whereas the only potential (i.e., depending on the concrete laws) lost is the property of *tax evasion*. This occurs only when the duty on Bob who makes \$1000 (say, from selling 1000 shares) is different the duties on him when he earns \$1000 by selling 500 shares twice. In this case, such a lost is inevitably due to the *unlinkability* among the transactions performed by the same person.

5.1 Related Work: A Closer Look

Now, it is interesting to compare our solution with the one in [MS99]. The obvious *cursor* is the *scale*, i.e., how many certificates/accounts one is allowed to hold.

Our basic scheme can be viewed as an instance at the one extreme end of the ruler because every one is allowed to hold exactly one certificate/account. While we realize the best control, efficiency, and scalability, the transactions are linkable. If such linkability is the principal concern, our extension can be adopted instead while almost nothing is lost.

The totally unlinkable anonymity of [MS99] is located at the other extreme end as each share is associated with a different certificate. As mentioned in the introduction, such a solution is bound to be non-scalable. Though this solution can still be extended to let one hold $m > 1$ certificates[5], with similar to our extension at first glance, such an extension is still disadvantageous over ours in the following senses.

- This extension is still non-scalable as each share corresponds to a certificate, therefore, a signature can only serve a trading of one share, whereas in our extension one signature is enough in each transaction independent of the number of involved shares.
- Their trading model is unfair to the buyers, whereas our solution is a really fair market in the sense of [FSW99].
- A new detection (i.e., after-the-fact) mechanism entitling the law enforcers to actively block abuses (e.g., brute force) is introduced in our solution, whereas it is totally unclear how to realize such a mechanism.
- Their certificate authority has to maintain an additional e-cash scheme, whereas it only needs to proactivize its own signing function in ours. To some extent, our solution is piggybacked!

6 Conclusion and Future Work

By introducing the new concept of *anonymous account* with which the money and share balances of

[5] Thus, shares attached to the same certificate are linkable.

an investor are associated, we have proposed a *scalable* (e.g., one signature is enough to certify a trading/election transaction independent of the number of involved shares), *tax evasion-free*, *fair* (to both the sellers and the buyers) anonymous investing scheme with a mechanism for the law enforcers to *actively* detect abuses (i.e., brute force, inflation, insider trading, and money laundering).

An interesting challenge for future work is to investigate how much the affection is the *anonymous linkability* on privacy? Hopefully, data mining may play an important role in this direction.

References

[Ba98] Basle Committee on Banking Supervision, Risk Management for Electronic Banking and Electronic Money Activities, http://www.bis.org, 1998

[BGK95] E. F. Brickell, P. Gemmell, and D. Kravitz, Trustee-Based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change, SODA'95

[C82] D. Chaum, Blind Signatures for Untraceable Payments, Crypto'82

[CFN88] D. Chaum, A. Fiat, and M. Naor, Untraceable Electronic Cash (Extended Abstract), Crypto'88

[CMS97] J. Camenisch, U. Maurer, and M. Stadler, Digital Payment Systems with Passive Anonymity-Revoking Trustees, Journal of Computer Security, 5(1), 69-89, 1997

[FSW99] M. Fan, J. Stallaert, and A. B. Whinston, A Web-Based Financial Trading System, IEEE Computer, April 1999, 64-70

[FTY96] Y. Frankel, Y. Tsiounis, and M. Yung, Indirect Discourse Proofs: Achieving Efficient Off-Line E-Cash, Asiacrypt'96

[FTY98] Y. Frankel, Y. Tsiounis, and M. Yung, Fair Off-Line E-Cash Made Easy, Asiacrypt'98

[GMR88] S. Goldwasser, S. Micali, and R. L. Rivest, A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks, SIAM J. Computing, 17(2):281-308, 1988

[HJJKY97] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczky, and M. Yung, Proactive Public Key and Signature Systems, ACM CCS'97

[JY96] M. Jakobsson and M. Yung, Revokable and Versatile Electronic Money, ACM CCS'96

[JY97] M. Jakobsson and M. Yung, Distributed "Magic Ink" Signature, Eurocrypt'97

[M96] D. M'Raihi, Cost-Effective Payment Schemes with Privacy Regulations, Asiacrypt'96

[MW98] D. A. Mussington and P. Wilson, Cyberpayments and Money Laundering, http://www.rand.org, 1998

[MS99] P. MacKenzie and J. Sorensen, Anonymous Investing: Hiding the Identities of the Stockholder, Financial Cryptography, 1999

[NIST91] National Institute for Standards and Technology, Digital Signature Standards, 1991

[OECD96] Organization for Economic Co-operation and Development, OECD Workshops on the Economics of the Information Society, 1997

[P96] B. Pfitzmann, Digital Signature Scheme-General Framework and Fail-Stop Signatures, LNCS 1100, 1996

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystem, CACM, Vol. 21, No. 2, 1978

[S91] C. P. Schnorr, Efficient Signature Generation by Smart Cards, J. Cryptology, 4(3), 1991, 161-174

[S96] D. Simon, Anonymous Communication and Anonymous Cash, Crypto'96

[vSN92] B. von Solms and D. Naccache, On Blind Signatures and Perfect Crimes, Computer & Security, 11(6), 1992, 581-583

A Proof for Theorem 1

Theorem 1. Our system achieves unforgeability (**Lemma 1.1**), over-trading prevention (**Lemma 1.2**), over-trading framing-freeness (**Lemma 1.3**), traceability (**Lemma 1.4**), revocability (**Lemma 1.5**), anonymity (**Lemma 1.6**), anonymous voting (**Lemma 1.7**), and tax evasion-freeness (**Lemma 1.8**).

Lemma 1.1. The "conditionally anonymous certificate" is existentially unforgeable.

proof: *(sketch)* This can be directly concluded from the assumption of the *existential unforgeability* of the underlying (threshold) magic-ink signature scheme in [JY97] and the security of the underlying proactivization scheme in [HJJKY97]. □

Lemma 1.2. Any over-trading can be prevented.

proof: *(sketch)* On one hand, as the stock exchange verification (**SEV**) will check the validity of the buying and selling requests against the database maintained by the stock exchange, and then decide whether such a claim is valid (thereby posting on the anonymous bulletin board, ABB) or not (i.e., omitting it), either over-buying or over-selling can prevented unless the **SEV** is dishonest. □

Lemma 1.3. No participants can falsely frame an investor participating in over-trading.

proof: *(sketch)* According to the buying and selling protocols, a successful trading must be witnessed by the investor's signed request which can be verified by the stock exchange verification (**SEV**) against the corresponding "conditionally anonymous certificates" (CAC). Therefore, no parties (including even **SEV**) are able to frame the investor in any trading or over-trading process as the underlying signature scheme is assumed existentially unforgeable. □

Lemma 1.4. The anonymous investing scheme supports three kinds of passive traceability: (1) From *anonymous account* (AA) to investor's ID; (2) From an investor ID to the corresponding AA; (3) Whether an AA is corresponding to certain investor ID.

proof: *(sketch)* (1) This is in nature to trace from a "conditionally anonymous certificate" (CAC) to the corresponding investor's ID. It can be done via the same way as in [JY97], i.e., via the underlying magic-ink signature primitive.

(2) This can done by firstly tracing from an investor's ID to the corresponding "conditionally anonymous certificate" (CAC) according the techniques depicted in [JY97], and then from CAC to the corresponding AA, thereof the money/share balance attached to it.

(3) This is equal to decide whether certain CAC is issued in certain signing session, which can be done via the technique in [JY97]. □

Lemma 1.5. Any traced share/money can be blacklisted or frozen implying revocability.

proof: *(sketch)* As any "anonymous account" (AA) can be traced, thus the stock exchange can blacklist or freeze the share/money attached to the AA. □

Lemma 1.6. The probability for any coalition of participants not including a quorum servers of the certificate authority to determine the identity of the owner of a AA is negligible.

proof: *(sketch)* If there exists such as adversary succeeding in doing this with probability non-negligible, it can be used as an oracle to reveal the identity of the investor holding the corresponding "conditionally anonymous certificate" (CAC), which is contrast to the conclusion proved in [JY97]. □

Lemma 1.7. Our scheme implementing anonymous voting.

proof: *(sketch)* (1) No participants can impersonate an investor in voting as a signature is necessary to certify it. (2) It is impossible for an investor to vote more than his share balance afford to as the stock exchange election (**SEE**) knows the quantity of the shares he holds. (3) The election scheme is universally verifiable whereas anonymity for the voter is preserved. □

Corollary 1.8. Our scheme is tax evasion-free.

proof: *(sketch)* As all capital gains are precisely recorded, the tax agency can calculate the taxes (anonymously) with similar to the process in the physical world (non-anonymously). The taxes can be paid directly from the AAs of the investors. □