인증서를 기반으로 하는 전자 현금 시스템

황 성 운†

요 약

본 논문은 인증 기관에서 발행한 인증서를 기반으로 한 효율적인 오프라인 전자 현금 시스템의 설계에 관한 것이다. 본 제안 시스템은 전자 현금 위조 불가, 익명성, 이중 사용 탐지, 누명 불가 등과 같은 전자 지불 시스템이 기본적으로 갖춰야 할 요구 조건들을 모두 만족하고 있다. 특히 제안 시스템은 (1) 인출 및 지불 단계에서 사용자(고객)가 계산해야 하는 지수 연산 횟수가 기존의 다른 프로토콜들에 비해 현저히 작으며 (2) 인출 단계에서 이루어지는 대부분의 계산이 인출 전에 미리 이루어 질 수 있다(사전 계산)는 점에서 계산적으로 매우 효율적이다. 따라서 본 제안 시스템은 메모리와 계산 측면에서 스마트카드로 구현되기에 적합하다.

Certificate-based Electronic Cash System

Seong-Oun Hwang†

ABSTRACT

We propose an efficient off-line electronic cash system based on the certificate issued by Certificate Authority. It satisfies all the basic requirements for electronic payment system such as cash unforgeability, cash anonymity, double spending detection, no framing, etc. Our proposed system is very computationally efficient in the sense that: (1) the number of exponentiation operation imposed on the user during withdrawal phase is much smaller than any existing off-line electronic cash schemes, (2) all the computation of user's during withdrawal phase can be performed by off-line pre-processing. So the proposed system is suitable to be implemented by smart cards in both memory and computation.

1. Introduction

With the onset of the Information Age, our nation is becoming increasingly dependent upon network communications. Computer-based technology is significantly impacting our ability to access, store and distribute information. Among the most important uses of this technology is *electronic commerce*: performing financial transactions via electronic information exchanged over telecommunications lines. A key requirement for electronic commerce is the development of secure and efficient electronic payment system.

Electronic payment systems come in many forms including digital checks, debit cards, credit cards and stored value cards. The type of electronic payment system focused on this paper is *electronic cash*. As the name implies, electronic cash is an attempt to construct an electronic payment system modeled after our paper cash system. Paper cash has such features as being: portable (easily carried), recognizable hence readily acceptable, transferable (without involvement of the financial network), untrace-

† 정 회 원 : 한국전자통신연구원 연구원
논문접수 : 1998년 5월 23일, 심사완료 : 1998년 8월 27일

able (no record of where money is spent), anonymous (no record of who spent the money) and has the ability to make "change". Among these, the designers of electronic cash have focused on preserving the features of payment untraceability and user anonymity.

Related Works

To provide payer anonymity during payment and payment untraceability so that the bank cannot find out whose money is used in a particular payment, it is necessary that the bank not be able to link a specific withdrawal with a specific deposit. This is achieved using a special kind of digital signature called a *blind signature*. Several blind signature schemes ([Cha82] [CFN88] [Bra93a] [Fer93a] [OO89] [AF96]) are introduced. Here we give only a high-level description of blind signature. In the withdrawal phase, a user makes the message to be signed by the bank and blinds it using a random quantity, which is called the blinding factor and is not known to the bank. The bank signs this random-looking text, and the user removes the *blinding factor*. In this way the user now has a legitimate electronic coin signed by the bank. The bank will see this coin when it is submitted for deposit, but will not know who withdrew it since the blinding factors are unknown to the bank.

Another issue of electronic cash is the double spending of the same coin. That is, as the electronic cash is a kind of digital information, it can be easily copied and then can be spent more than once by the user. Double spending can be prevented by the maintenance of database of electronic cash spent in an on-line payment system (Ecash[Cha89], CAFE [BCM94], NetCash[MN93]). But, in an off-line system where the bank does not intervene during the payment phase, there is no cryptographic method that prevents an off-line cash from being spent more than once beforehand. Instead, off-line double spending is detected when the cash is deposited in the bank and compared with a database of spent cash ([OO91][CFN88][Fer93a][Fer93b][Yac94][YLR93][LL93][CPS94]). Recently, by embedding a tamper-resistant device called an "observer" into the payment device of the account-holder, the method of achieving prior restraint of double spending for off-line electronic cash systems has been suggested ([Cha92][CP92][CP93][Bra93a][Bra94][Bra95][Fer93b]). An observer is embedded in such a way that a payment can only be successfully executed only if the observer cooperates.

In this paper, we propose a certificate-based off-line electronic cash system, which satisfies all the basic requirements of electronic cash system described below. To the best of my knowledge, the use of anonymous certificate appeared in [Yac94] [NMV97] and the use of anonymous account appeared in [Bra93b]. The basic idea of our system is as follows: The user generates his private/ public key pairs and registers the public key to the Certificate Authority. Only the Certificate Authority can link the public key to its owner. Then using the public key and its certificate, the user makes a monetary transaction with other parties such as bank and shops. In this way, payer anonymity during payment and payment untraceability are achieved.

The paper is organized as follows. In section 2, we describe some basic requirements of electronic cash system. Then we present our system which consists of several protocols in section 3. In section 4, we consider various security features of our system and in section 5, we evaluate its performance. Finally, we conclude this paper with remarks in section 6.

2. Requirements for Electronic Cash System

Some basic requirements for electronic cash system are as follows:

Off-line payments. The transaction between the user and the shop should be completed without the help of the bank or the third authority.

Detection of double spending. If a user repeatedly spent his cash, his identity should be found by the bank. In on-line electronic cash system, it would be detected before the fact. But in off-line one it would generally be found after the fact.

No framing. Every party participated in the electronic cash protocol should be protected from a collusion of all the other parties.

No forgery. It should be difficult for users or shops to create a valid-looking coin without making a withdrawal transaction with the bank.

Efficiency. The scheme should be efficient in storage, communication and computation. Convenience of making payments is highly desirable. Transaction cost should be low enough compared with transaction amount. And the computation amount imposed on the user during withdrawal/payment phase should also be small.

Privacy. The payment of a user should not be linkable to his withdrawal, even though all the parties except him could collude together.

3. Description of the Proposed System

3.0 Definitions

We define terms that will be used throughout this paper.

- ***U*: user or user's card**

The user is anyone who withdraws and spends electronic money. The user's card is a card constructed for and trusted by the user. It is the device with which he makes withdrawals, purchases, and reports transactions.

- ***B*: bank**

An institution which dispenses electronic cash for withdrawal and accepts it for deposit. The bank should not have the power to trace an honest user's spending.

- ***S*: shop**

A shop performs a deposit protocol with bank, to deposit the user's coin into his account. Shop usually can accumulate coins and deposit the aggregate value at the bank at suitable time when network traffic is low.

- ***CA*: Certificate Authority**

A Certificate Authority is a body that provides a trusted third party services in electronic commerce by issuing digital certificates. Formally, a certificate is a computer-based record which: (1) identifies the ***CA*** issuing it, (2) names, identifies, or describes an attribute of the subscriber, (3) contains the subscriber's public key, and (4) is digitally signed by the ***CA*** issuing it.

3.1 System Set-up

The RSA scheme [RSA78] is adopted by ***B*** and ***CA*** as follows: (e_B, n_B) / d_B, (e_{CA}, n_{CA}) / d_{CA} is respectively ***B***'s, ***CA***'s RSA public/private key pairs such that

$$e_B d_B = 1 \bmod \varphi(n_B),\ e_{CA} d_{CA} = 1 \bmod \varphi(n_{CA})$$

where φ is Euler totient function.

We assume the existence of a polynomial time collision-resistant one-way hash function h, h'. Public key parts are declared to everyone.

3.2 Certificate Issuing Protocol

U uses the Schnorr's scheme [Sch91] to generate his public/private key pair. All the system parameters p and q are primes such that $q \mid p-1$, $q \geq 2^{140}$ and $p \geq 2^{512}$. Denote by g a generator of the subgroup G_q of Z_p^*.

Then identifying himself to ***CA***, he gets a certificate on the public key from the ***CA*** that establishes a linkage between his identity and his public key. That is, the certificate means that the public key is registered at the CA. However, unlike in ordinary certificates, this linkage is hidden to everyone. That is, anyone except the CA cannot find out the owner's identity from the public key or the certificate. Before U opens an account at the bank, he performs the followings with CA:

(1) U generates his private key $s_U \in_R Z_q^*$. and computes the corresponding public key $p_U = g^{-s_U} \bmod p$. Identifying himself to CA, U sends his public key to CA to get the certificate on it and keeps his private key s_U secret.
(2) After verifying U's identity, CA issues the certificate $Cert_U = h(ID_{CA} \| p_U)^{d_{CA}} \bmod n_{CA}$ to U. Then CA stores the public key, certificate with the owner's identity. Here ID_{CA} is the CA's identity.
(3) On receiving this certificate, U checks that $[Cert_U]^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_U)$.

3.3 Opening an Account(performed for each user)

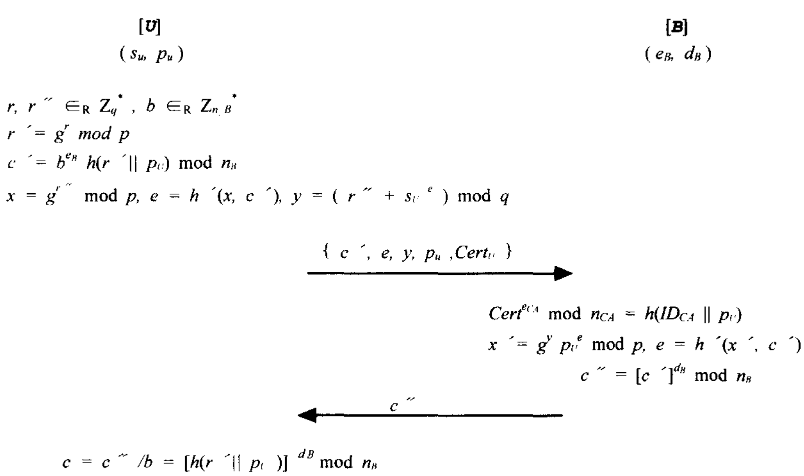
In this phase, a user gets an anonymous account which will be used to withdraw some money at the bank. That is, the following protocol takes place:

(1) U sends his public key p_U and its corresponding certificate $Cert_U$ to B without identifying himself.
(2) B verifies that the public key p_U is registered at the CA by checking: $[Cert_U]^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_U)$. If the verification holds, B opens an account for the public key p_U.

3.4 Withdrawal Protocol

When a user U wants to withdraw money from his account (corresponding to say p_U), he performs the following withdrawal protocol with B (Fig 1):

(1) U generates a random number $r \in_R Z_q^*$, computing: $r' = g^r \bmod p$. To get a B's blind signature to the message $h(r' \| p_U)$, U chooses a blinding factor $b \in_R Z_{n\_B}^*$ and computes $c' = b^{e_B} h(r' \| p_U) \bmod n_B$. U then generates a random number $r'' \in_R Z_q^*$, computing: $x = g^{r''} \bmod p$, $e = h'(x, c')$, $y = (r'' + s_U e) \bmod q$ and sends $\{c', e, y, p_U, Cert_U\}$ to B.
(2) B checks $Cert_U^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_U)$ and after computing $x' = g^y p_U^e \bmod p$, checks $e = h'(x', c')$. If the verification holds, B signs c' and returns the signature as $c'' = [c']^{d_B} \bmod n_B$.
(3) U then removes the blind factor b to obtain the B's signature $c = c''/b = [h(r' \| p_U)]^{d_B} \bmod n_B$. For each coin, U stores $\{c, r\}$.



(Fig.1) Withdrawal Protocol

3.5 Payment Protocol

When U wants to spend his coin at S, the following payment protocol is executed (Fig 2):

(1) U sends $\{c,\ p_U,\ Cert_U\}$ to S.

(2) S computes $d = h(A_S \| time \| c)$ and sends $\{A_S,\ time\}$ to U. This challenge value d should be unique for each transaction. Here time is the actual time and date the payment transaction occurred and A_S is the S's account number at B.

(3) U computes $d = h(A_S \| time \| c)$, $z = (r + s_U d)$ mod q and then sends z to S.

(4) S computes $w = g^z p_U{}^d$ mod p and verifies the following: $Cert_U{}^{e_{CA}}$ mod $n_{CA} = h(ID_{CA} \|, p_U)$, c^{e_B} mod $n_B = h(w \| p_U)$.

3.6 Deposit Protocol

At a suitable time, preferably when network traffic is low, S deposits all the received coins at B by sending $\{c,\ p_U,\ Cert_U,\ d,\ time,\ A_S,\ z\}$ for each coin. B goes through the same verification process as S did in the payment phase, i.e., computes $d = h(A_S \| time \| c)$, $w = g^z p_U{}^d$mod p and verifies the following: $Cert_U{}^{e_{CA}}$ mod $n_{CA} = h(ID_{CA} \| p_U)$, c^{e_B} mod $n_B = h(w \| p_U)$ and searches its deposit database to find out if it has stored the coin before. If all tests are successful, B credits S's account with an equivalent amount of money and stores the transaction history to its database.

4. Security Considerations

4.1 Double Spending

Double spending occurs when U double spends some coins in the hope that B cannot detect the identity. But, in the proposed system, double spending is detected as follows:

U spends c twice for two different challenges d and d'.

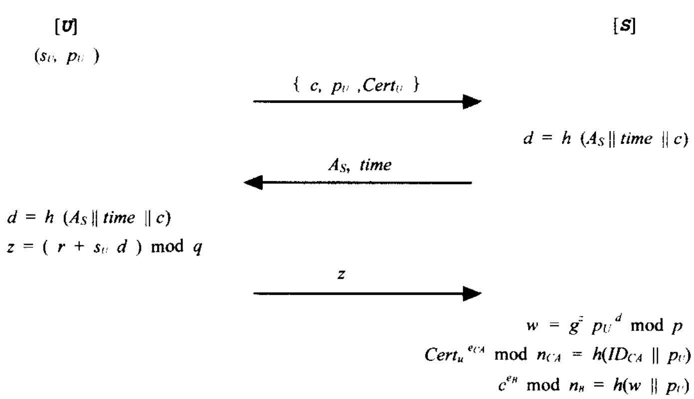
Then B has $z = (r + s_U d)$ mod q and $z' = (r + s_U d')$ mod q. B can easily find s_U by computing:

$$s_U = (z - z')/(d - d') \bmod q.$$

So the bank can present s_U to the CA as a proof of the double spending.

4.2 Anonymity and Privacy

The bank will not be able to link to user's identity. On the other hands, our coins are blindly signed by the bank so the bank cannot trace any particular coin to any particular user. But the payments made with the same certificate can be linked together, though the exact user cannot be traced.



(Fig. 2) Payment Protocol

4.3 Fairness (Conditional Tracibility)

But as we know well, unconditional privacy protection can be abused by criminals for black-mailing or money laundering, etc. To cope with this, it requires a user-tracing mechanism("fairness") ([BGK95][CMS96][FTY96][JY96][M'R96][SPC95]) when the condition holds, for instance, under the court's order. In our system, Certificate Authority can find out its owner's identity from any anonymous public key, so the bank can find out doubtful or illegal users with the help of Certificate Authority under the permission of the court. In particular, Certificate Authority can deal with these criminal problems in advance by using CRL (Certificate Revocation List) or blacklist.

4.4 Forgery

Forging our coins is equivalent to creating $(x, h(x)^{d_B} \bmod n_B)$, that is, equivalent to breaking the RSA scheme. This is conjectured to be infeasible unless the factorization of n_B is known. As the factorization of n_B is known to only $\boldsymbol{B}$, forging our electronic coins is infeasible for any other party.

4.5 Framing

To frame a particular user $\boldsymbol{U}$, $\boldsymbol{B}$ needs s_U, a proof of double spending. Assuming the Discrete Log assumption, if $\boldsymbol{U}$ follows the protocols and does not double spend, $\boldsymbol{B}$ cannot compute s_U. That is, $\boldsymbol{U}$ is computationally protected against a framing.

5. Performance Evaluations

When we consider efficiency features of the electronic cash system, the computational load imposed on the user is very important. It is because user capability is usually implemented in a smart card, which still has some limited memory and computing power. In particular, exponential operation is a critical factor which heavily affects the smart card's computation ability.

We compare the efficiency of our system with those of [Fer93a] and [Bra95]. When we assume in [Fer93a], $|n|$ = 512, $|v|$ = 128, and in [Bra95], $|p|$ = 512, $|q|$ = 140, $|H(\cdot)|$ = 72, and in our system $|e_B|$ = 16, $|n_B|$ = 512, $|n_{CA}|$ = 512, $|p|$ = 512, $|q|$ = 140, $|h(\cdot)|$ = 72, we get the following results on Table 1. For the convenience of the comparison, we assumed those values, but for greater security, one may want to increase those values. Examining Table 1 below, we see that the number of exponential operation imposed on the user is much smaller than any

<Table 1> Comparison of electronic cash protocols

		[Fer93a]	[Bra95]	Proposed Scheme
Primitive Problem		Factoring	Discrete Logarithm	Factoring
Signature Scheme (Blinding Scheme)		RSA (randomized blind signature)	Schnorr (restrictive blind signature)	RSA + Schnorr (RSA type blind signature)
Certificate		N/A	One-time certificate	Multi-spendable certificate
Fairness		No	No	Yes
Double Spending		Detect after the fact	Prevention / Detection	Detect after the fact
Storage per Coin value(bytes)		250	143	81.5
Communication Amount	Withdrawal	>> 480 bytes	96.5 bytes	282.5 bytes
	Payment	>> 224 bytes	148.5 bytes	218.5 bytes
# of Discrete Exponentiations	Withdrawal (user)	25	15	3
	Payment (user)	1	2	0
# of Multiplica-tions	Withdrawal (user)	>> 2881	1400 (online part: 210)	445 (online part:0)
	Payment (user)	108	321	1

existing off-line electronic cash schemes and all this computation can be performed by off-line pre-processing. So our proposed system is suitable to be implemented by smart cards.

But the communication amount of our system is a little large when compared with that of Brands system[Bra95]. This is mainly caused by the public key and certificate of users. To reduce the communication amount, it is necessary to adopt any efficient signature scheme with keys of shorter size than the current RSA scheme and a number of practical optimizations for embodiment.

- Withdrawal phase

81.5 bytes are required to store coin related data $\{c, r\}$. It is small enough to be stored on typical smart cards. To perform a withdrawal transaction, the user needs only three exponentiations. This is computationally efficient than all current off-line electronic cash schemes. The number of discrete exponentiations required in Ferguson's [Fer93a], Brands' [Bra95] protocols are 25 and 15 respectively. The number of multiplications modulo a 64 byte number required in Ferguson's protocol is greater than 2881. In Brands' protocol, the user must perform about 1400 multiplications modulo a 64 byte number: the on-line computations of this are about 210 multilpications modulo a 64 byte number. In our proposed system, the user must perform about 445 multiplicaitons modulo a 64 byte number: All this computation is done off-line. Note that the computational load imposed on the user is small enough for the proposed system to be implemented by smart cards, since only a few modular multiplications and/or modular reductions are required in all transactions except for off-line pre-processing stages.

- Payment phase

In our payment protocol, the user only has to compute a single response. This is far more efficient than all known off-line electronic cash schemes to-date, especially as the response message does not involve any discrete exponential computation. As we can see in the above Table 1, Ferguson's and Brands' protocol must perform about 108 and 321 multiplications modulo a 64 byte number, but our system needs only one multiplication.

6. Conclusion

We have proposed a simple, efficient off-line electronic cash system based on the certificate issued by Certificate Authority. It still satisfies all the basic requirements for electronic payment system such as cash unforgeability, cash anonymity, double spending detection, no framing, etc. It is believed that our proposed system is very computationally efficient and suitable to be implemented by smart cards. And our proposed system can cope with several problems such as blackmailing or money laundering, etc.

References

[1] M.Abe and E.Fujisaki, "How to date blind signatures," Advances in Cryptology-Asiacrypt '96, pp.244-251, 1996.

[2] J.P.Boly, A.Bosselaers, R.Cramer, R.Michelsen, S.Mjolsnes, F.Muller, T.Pedersen, B.Pfitzmann, P.de Rooij, B.Schoenmakers, M.Schunter and L.Vallee, "The ESPRIT project CAFE-High security digital payment systems," Computer Security-Esorics'94, LNCS 875, Springer-Verlag, pp.217-230, 1994.

[3] E.F.Brickell, P.Gemmell and D.Kravits, "Trustee based tracing extensions to anonymous cash and the making of anonymous change," Symposium on Distributed Algorithms (SODA'95), pp. 457-466, 1995.

[4] S.Brands, "Untraceable off-line cash in wallets with observers," Advances in Cryptology-Crypto'93, LNCS 773, Springer-Verlag, pp.302-318, 1994.

[5] S. Brands, "Electronic Cash Systems Based on the Representation Problem in Groups of Prime

Order," Preproceedings of Crypto'93.

[6] S.Brands, "Off-line cash transfer by smart cards," CWI Reports, CS-R9455, 1994.

[7] S.Brands, "Electronic cash on the Internet," Proc. Symp. on Network and Distributed System Security, IEEE Computer Society Press, pp.64-84, 1995.

[8] D.Chaum, A.Fiat and M.Naor, "Untraceable electronic cash," Advances in Cryptology-Crypto'88, LNCS 403, Springer-Verlag, pp.319-327, 1990.

[9] D.Chaum, "Blind signatures for untraceable payments," Advances in Cryptology-Crypto'82, pp.199-203, 1983.

[10] D.Chaum, "Online cash check," Advances in Cryptology-Eurocrypt'89, LNCS 434, Springer-Verlag, pp.288-293, 1989.

[11] D.Chaum, "Achieving electronic privacy," Scientific American, Aug., pp.96-101, 1992.

[12] J.Camenisch, U.Maurer and M.Stadler, "Digital payment systems with passive anonymity-revoking trustees," Esorics'96, 1996.

[13] D.Chaum and T.P.Pedersen, "Wallet databases with observers," Advances in Cryptology-Crypto '92, LNCS 740, Springer-Verlag, pp.89-105, 1993.

[14] R.J.F.Cramer and T.P.Pedersen, "Improved privacy in wallets with observers," Advances in Cryptology-Eurocrypt'93, LNCS 765, Springer-Verlag, pp.329-343, 1994.

[15] J.L.Camenisch and J.M.Piveteau and M.A. Stadler, "An Efficient Electronic Payment System Protecting Privacy," Computer Security-Esorics'94, pp.207-215, 1994.

[16] N.Ferguson, "Single term off-line coins," Advances in Cryptology - Eurocrypt'93, Springer-Verlag, pp.318-328, 1993.

[17] N.Ferguson, "Extensions of Single Term Off-Line Coins," Advances in Cryptology-Crypto'93, Springer-Verlag, pp.292-301, 1993.

[18] Y.Frankel, Y.Tsiounis and M.Yung, "Indirect discourse proofs : achieving fair off-line e-cash," Advances in Cryptology-Asiacrypt'96, LNCS 1163, pp.286-300, 1996.

[19] M.Jakobson and M.Yung, "Revokable and versatile e-money," Proceedings of the third annual ACM Symp. On Computer and Communication Security, March, 1996.

[20] C.H.Lim and P.J.Lee, "A Practical Electronic Cash System for Smart Cards," Proceedings of JW-ISC'93, Oct., 1993.

[21] G.Medvinsky and B.C.Neuman, "NetCash: A design for practical electronic currency on the Internet," Proc. 1st ACM Conf. On Computer and Communications Security, ACM Press, pp.102-106, 1993.

[22] D.M'Raihi, "Cost-effective payment schemes with privacy regulation," Advances in Cryptology-Asiacrypt'96, pp.266-275, 1996.

[23] K. Q. Nguyen, Y. Mu and V. Varadharajan, "One-Response Off-Line Digital Coins," Fourth Annual Workshop on Selected Areas in Cryptography (SAC)'97, August 11-12, 1997.

[24] T.Okamoto and K.Ohta, "Disposable zero-knowledge authentication and their applicaions to untraceable electronic cash," Advances in Cryptology-Eurocrypt'89, pp.481-496, 1990.

[25] T.Okamoto and K.Ohta, "Universal Electronic Cash," Advances in Cryptology-Crypto'91, pp.321-337, 1991.

[26] R.Rivest, A.Shamir and L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21(2), pp.120-126, 1978.

[27] C.P.Schnorr, "Efficient Signature Generation By Smart Cards," Journal of Cryptology, Vol.4, No.3, pp.161-174, 1991.

[28] M.Stadler, J.M.Piveteau and J.Camenisch, "Fair blind signatures," Advances in Cryptology-Eurocrypt'95, pp.209-219, 1995.

[29] Y. Yacobi, "Efficient electronic money," Advances in Cryptology-Asiacrypt'94, pp.153-163, 1994.

[30] H.Y.Youm, S.L.Lee and M.Y.Rhee, "Practical Protocols for Electronic Cash," Proceedings of JW-ISC'93, Oct., 1993.

황 성 운

sohwang@etri.re.kr
1993년 서울대학교 수학과 졸업(학사)
1998년 포항공과대학교 정보통신학과(공학석사)
1994년~1996년 LG-EDS Systems, Inc. 근무
1998년~현재 한국전자통신연구원 연구원
관심분야 : 암호학 이론 및 응용, 네트워크 보안, 전자현금 프로토콜