한국항행학회 논문지 제14권 제5호 2010년 10월

효율적인 영지식 부인봉쇄 프로토콜 연구

Study of Undeniable Signatures Schemes based on Zero-Knowledge Proof

계이기*, 최황규**

Yi-Qi Gui* , Hwang-Kyu Choi**

요 약

본 논문은 부인봉쇄에서 영지식 검증을 위해 일방향 함수와 부분선택 방법을 사용하는 새로운 기법을 제안한다. 제안된 기법의 핵심은 서명자의 협조 없이 전달되는 문서에 대하여 서명자를 보호하는 것이다. 또한 본 논문은 확인과 부인 프로토콜 수행 과정에서 메시지 교환을 위한 통신비용을 최소화할 수 있음을 보이며, 이는 모바일 환경에 매우 유용하다. 한편 제안된 기법은 서명자가 원래 메시지와 서명을 모르는 상황에서 검증자의 비밀을 보호하면서 서명이 유효한지를 검사할 수 있는 검증자를 허용한다.

Abstract

The main idea is to protect the signer of a document against the document being digitally distributed without the cooperation of signer. This paper proposes a new scheme of undeniable signature, which is so effective and improved D. Chaum's scheme. And our scheme which is zero-knowledge proved by using one-way function and partition-selection method, shows that its communication(challenge-response) only needs much fewer times during the confirmation protocol and disavowal protocol respectively, being very useful for wireless network environment. In the meantime, our scheme allows the verifier to verify that the signature is valid, while t he signer doesn't know the original message and the signature, to preserve the privacy of the verifier.

Keywords: zero knowledge(영지식), undeniable signature(부인봉쇄), one-way function(일방향 함수)

Ⅰ. Introduction

In order for a computer network to offer services (ex: multi-user electronic commerce, MSN chatting group and so on) related to be security and privacy, various solutions were proposed for this issue, for example, encryption technique, digital signature technique (including general signature scheme, blind signature scheme, undeniable signature scheme, group signature scheme, etc), and other cryptographic techniques[1].

Undeniable signatures are one of the techniques, which can achieve their zero knowledge. Undeniable signatures, first devised by David Chaum and Hans van Antwerpen[2], where signatures can only be verified with the consent of the signer. Zero-knowledge undeniable signatures, devised by D. Chaum[3], have

* 강원대학교 컴퓨터정보통신공학과(Dept. of Computer Science & EngKangwon National Univ.)
** 강원대학교 컴퓨터학부(Dept. of Computer Eng. Kangwon National)
· 제1저자 (First Author) : 계이기 · 교신저자: 최황규
· 투고일자 : 2010년 9월 15일
· 심사(수정)일자 : 2010년 9월 15일 (수정일자 : 2010년 10월 26일)
· 게재일자 : 2010년 10월 30일

two distinctive features:

1. The verification process is interactive, so the signer can limit who can verify their signature.

2. A disavowal protocol, that is a cryptographic protocol which will allow them to prove that a given signature is a forgery.

In D. Chaum's scheme, four times communications (challenge-response) are needed between the verifier and the signer in each of two(confirmation/disavowal) protocols. In Bi-proof[4], there is only one protocol for verification process and disavow process, while it needs much more communication times than D. Chaum[3] between the verifier and the signer.

In this paper, we present a novel zero-knowledge undeniable signature scheme. In the confirmation protocol, the one-way function is used to hide the private key value and achieve the zero-knowledge proof; in the disavowal protocol, we proof our protocol is zero-knowledge by partition-selection method. Our scheme communicates message exchange only twice while D. Chaum's scheme needs 4 communications so that it is more efficient. Moreover our scheme is suitable for the zero-knowledge proof of blind signatures. In a blind signature scheme, the signers neither learn the messages they sign, nor the signatures the recipients obtain for their messages. In offline electronic cash this is used to encode a customer's identity into the messages that are signed by the bank such that the messages obtained by the customer all have his identity encoded correctly. In the D. Chaum scheme, however, the signer knows the message and the signatures in advance, which is the proving condition of the zero-knowledge, and the signer selects responding protocol determined by the validity of the signature.

Hence the D. Chaum scheme needs four times communications in the confirmation or disavowal protocol. In Bi-proof scheme, the signer can reconstruct the response only if the signer knew the original message and the signature before. Otherwise, the protocol can not keep going. While in our scheme, the signer can finish the verification process even though he/she does not know it's message and signature, and we preserve the privacy of the verifier at one time. The organization of the rest of this paper is as follows. The related researches are introduced in section2. In section3, we first provide the definition of our undeniable signature scheme and detail our zero-knowledge undeniable signature scheme is proposed. And the analysis and proofs are provided, mainly including zero-knowledge and undeniability for our scheme. Conclusions appear in section 4.

Ⅱ. Related work

Digital Signatures[5] are one of the most important concepts of cryptography, and are easily verified as authentic by anyone using corresponding public key. A epitome of signature schemes, undeniable signatures are different from those of digital signatures. Although an undeniable signature is similar to a digital signature in that it is a number issued by a signer that is related to the signer's public key and his/her message, the difference is that an undeniable signature cannot be verified without the cooperation of the signer. The validty or invalidity of an undeniable signature can be ascertained by accompanying a protocol with the signer, assuming the signer participates. In undeniable signature schemes[2,3,6] consist of two parts, a confirmation protocol and a disavowal protocol. if a confirmation protocol is used, a verifier can verify the validity of a signature by interacting with the validity of an invalid signature, and there is no opportunity that the signer can uncorrectly represent the validty of an invalid signature. If the validity test fails, the verifier can make a decision wether the signature is invalid or the signer is false by the disavowal protocol.

However, Bi-proof assures signature confirmation and disavowal with the same protocol. In other words, executing the scheme one time is equivalent to executing

both confirmation and disavowal protocols at the same time. Hence, without regard to signer's demand, the verifier can always determine whether a signature is valid or invalid, through executing the scheme once. In interactive proof systems[7], a prover has infinite power while the verifier is restricted to probabilistic polynomial time bounded. However, it does not ensure that the verifier can distinguish between the invalid signature and the falseness of the signer. To construct an undeniable signature scheme the interactive bi-proof system was defined in Bi-proof[3]. And Bi-proof scheme used a minimum knowledge proof for a common witness problem which based on the random self-reducible problem[8] in it's interactive bi-proof system. Here, the minimum knowledge[9] is a variant of zero-knowledge. The great drawback of Bi-proof scheme is that it needs much more communications (challenge-response) for the validty or invalidity of one undeniable signature being ascertained. Therefore, we proposed our novel scheme which can reduce message exchange communication improving the poor wireless verification network environment. The details of our scheme are in section 3.

Ⅲ. Our Proposed Signature Scheme

3-1 Definition of the scheme

Let a big prime $p=2q+1$ such that q is also a prime. Let G denote the multiplicative subgroup of Z_p^* of order q where G consists of the quadratic residues modulo p. We define the public data p and g which are for some signers. We then let $x \epsilon Z_p^*$ $(1 \le x \le q-1)$ be an element of order q and let $y=g^x \bmod p$. Finally we let the set of possible messages be equal to the set of the possible signatures be equal to G.

In this section we will define our undeniable signature scheme. This scheme is based on the discrete log problem and uses a challenge and response protocol to verify signatures.

Now we define the public key $pk=y$ and the private key $ak=x$. The signature of a message $m \epsilon G$ is then defined this way: $s=sig_{ak}(m)=m^x \bmod p$. Computing the private key from the public key, assume only random messages are signed, is the discrete log problem; forging signatures on random messages is at least as hard as breaking Diffie-Hellman key exchange. Different from other digital signatures, our digital signature scheme cannot verify and disavow the signature without cooperation of the signer on the confirmation protocol and disavowal protocol respectively.

3-2 Confirmation Protocol

we now introduce the challenge-and-response protocol for verifying a signature. A verifier V would like to verify a signature s on message m made by a signer S, where $m, s \epsilon G$. The confirmation protocol is as follows:

1. V choose at random a, $b \epsilon Z_q$.
2. V then computes $C=m^a g^b \bmod p$ and send it to S.
3. S chooses at random k then computes $D=C^x \bmod p$, $E=hash(D\|k)$ and then send E, k to V.
4. V computes $D'=s^a y^b \bmod p$, $E'=hash(D'\|k)$ and V accepts s as a valid signature on m only if $E=E' \bmod p$.

Now we will proof the 4th step in the protocol, namely how V accepts s as a valid signature on m only if $E=E' \bmod p$. From the definition we directly get

$$D \equiv C^x \equiv (m^x)^a (g^x)^b \equiv s^a y^b \equiv D' \bmod p$$

$$E \equiv hash(D\|k) \equiv hash(D'\|k) \equiv E' \bmod p$$

If the signature s is valid, and these two expressions are formed properly, we see that the verifier will accept a valid signature.

3-2-1 Security of the Confirmation Protocol

Two essential points can be proved as follows:

Theorem 1: Even with infinite computing power s cannot with probability exceeding p^{-1} provide a valid response for an invalid signature.

Proof: If the signature is invalid, we can get $s \neq m^x \bmod p$. Suppose $s = m^{x'} \bmod p$, with $x \neq x'$. Assuming the signer can find another pair $(a1, b1)$ corresponding to a challenge value to reconstruct the message1, we can get

$$m^a g^b \equiv m^{a1} g^{b1} \Rightarrow m^{(a-a1)} \equiv g^{(b-b1)} \bmod p$$

$$(m^{x'})^a (g^x)^b \equiv (m^{x'})^{a1} (g^x)^{b1} \Rightarrow (m^{(a-a1)})^{x'} \equiv (g^{(b1-b)})^x$$

.

By these two expressions , the same response is accepted only if

$$m^{(a-a1)} \equiv g^{(b-b1)} \equiv 1 \bmod p \Rightarrow$$
$$a = a1, b = b1 .$$

Due to the probability of $a = a1, b = b1$ being $q-1$, the probability that the signer will accept a forged signature is $q-1$.

Theorem 2: The protocol is zero-knowledge.

Proof: If V sends a message 2 that should result in a message 3 being sent, V can get any information of the valid signature determined by solving a log problem because of S hiding the information perfectly in message 3. Any V can simulate the message 2, 3 to cheat any third-party by choosing a, b, k as a random group element, but any third-party does not believe V.

3-3 Disavowal Protocol

As we have seen, the Confirmation Protocol allows V to verify that the signature is valid, but how can V check that a signature is invalid? This is where the disavowal protocol comes in. A formal and detailed description follows.

1. V chooses at random $a_1, a_2, \ldots\ldots, a_n, \; a_i \epsilon Z_q \;, \; i \epsilon [1,n]$
2. V then computes $C_i = g^{a_i} \bmod p$, $D_i = y^{a_i} \bmod p$.
3. V now chooses at random b, $b \epsilon Z_q$ and then computes $U = m g^b \bmod p$, $V = s y^b \bmod p$.
4. V randomly range the array[n+1] with data among $((C_i, D_i), (U, V))$ and send them to S, where $i \epsilon [1, n]$
5. S checks the n+1 times of equations as following:
$$D_i = C_i^x \bmod p \quad \text{and} \quad V = U^x \bmod p.$$
Any equation (U', V') which is not formed properly will be sent to V. If the number of the incorrect equation is more than 1, we can think V may be cheating and then stop the protocol.
6. V now concludes that the signature s is indeed a forgery if $(U', V') = (U, V)$.

For proof of why this will actually detect forgeries, we can get

$$D_i \equiv y^{a_i} \equiv (g^{a_i})^x \equiv C_i^{\,x} \bmod p$$

$$V \equiv s y^b \neq m^x (g^x)^b \equiv (m g^b)^x \equiv U^x \bmod p.$$

If the signature s is invalid ($s \neq m^x \bmod p$), and these two expressions are formed properly, we see that S finds the incorrect equation(U', V') and sends it to V to prove that the signature s is invalid.

As more interesting thought is, what if Signer tries to disavow a valid signature and as a result does not

follow the protocol truthfully? Actually the signer can cheat with probability 1/(n+1) in the above disavowal protocol, where n is a mutually agreed constant and order k operations must be performed by the signer. In practice n might be 1024, for instance, and the protocol could be conducted 3 times for a chance of cheating that is 2^{-30} or 10 times give a chance of only 2^{-100}. The more robust our protocol can be, the bigger n or k is increasing.

3-3-1 Security of the Disavowal Protocol

Again two things are proved as follows:

Theorem 3: Even with infinite computing power S cannot with probability exceeding 1/(n+1) provide a valid response for a valid signature.

Proof: if $s = m^x$, the challenge value (C_i, D_i) hide the (U, V) perfectly in the first message. Since the value(U, V) can not be selected by the signer, S only can to guess (U, V).

Theorem 4: The protocol is zero-knowledge.

Proof: In the disavowal protocol, the verity V sends the array[n+1] with data among $((C_i, D_i), (U, V))$, the signer S only does find (U, V) which V can always recognize and then send it to V. So the protocol is zero-knowledge. when V wants to cheat to get more information and as a result does not follow the disavowal protocol, S can find out V has been cheating in the 4th step. In the same way, the verifier can let the third party believe the copy of the protocol, which can be made by V, since the protocol is zero-knowledge.

Ⅳ. Conclusion

In this paper, we present a novel zero-knowledge undeniable signatures scheme, which improved D. Chaum's zero-knowledge undeniable signatures scheme. This scheme is a zero-knowledge undeniable signature proved by one-way function and partition-selection method in the confirmation protocol and disavowal protocol respectively. Compared with the existing schemes, our scheme is more effective and needs less communications(challenge-response) during the protocol. Futhermore our protocol can be used for proofing blind signatures which is zero-knowledge.

Acknowledgment

This study is supported by Kangwon National University.

References

[1] W. Mao, “Modern cryptography: theory and practice,” *Prentice-Hall, PTR, USA, ISBN 0-13-066943-1,* 2004.

[2] D. Chaum, and Hans van Antwerpen, “Undeniable signatures,” *CRYPTO 1989, LNCS 435, Springer, pp. 212-216,* 1990.

[3] D. Chaum, “Zero-knowledge undeniable signatures,” *EUROCRYPT 1990, LNCS 473, Springer, pp. 458-464,* 1991.

[4] A. Fujioka, T. Okamoto, and K. Ohta, "Interactive Bi-Proof Systems and Undeniable Signature Schemes", *Spring-Verlay,* 1998.

[5] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theroy, Vol.IFT-22, No.6, pp644-654,* 1976.

[6] Y. Q. Gui, M. B. Kim, H. K. Choi, "A New Undeniable Signatures Scheme Based on Zero-Knowledge Proof", *20th fall Proceedings of Korean Society for Internet Information, pp.233-236*, 2009.

[7] S. Goldwasser, S. Micali, and C. Rackoff, "The Konwledge Complexity of Interactive Proof-Systems, " Proceedings, 17th annual ACM Symposium on

Theroy of Computing, pp.291-304, 1985.

[8] M. Tompa and H. Woll, "Random Self-Reducibility and Zero Knowledge Interactive Proofs of Possession of Information," *28th annual Symposium on Foundations of Computer Science, IEEE, pp.472-482,* 1987.

[9] Z. Galil, S. Haber and C. Yung, "Minimum-Knowledge Interactive Proofs for Decision Problems," *SIAM Journal on Computering, Vol.18, No.4, pp.711-739,* 1989.

계 이 기 (桂易琪)

2007년 2월 : 강원대학교 컴퓨터정보통신공학과 (공학 석사)
2007년 3월~현재 : 강원대학교 컴퓨터정보통신공학과 박사과정
관심분야 :인터넷통신프로토콜, 인터넷 보안, 멀티미디어시스템.

최 황 규 (崔晃奎)

1984년 : 경북대학교 전자공학과 (공학사)
1986년 : KAIST 전기및전자공학과 (공학석사)
1988 : KAIST 전기및전자공학과 (공학박사)
1994년 7월 ~ 1995년 7월 Univ. of Florida 방문교수
1999년 3월 ~ 2001년 2월 강원대학교 전자계산소 소장
2002년 7월 ~ 2003년 7월 Univ. of Minnesota 방문교수
2009년 1월 ~ 2010년 1월 Univ. of Rhode Island 방문교수
1990년 3월 ~ 현재 강원대학교 컴퓨터학부 교수
관심분야 : 멀티미디어시스템, 데이터베이스시스템, P2P시스템