情報保護學會論文誌
第17卷 第5號, 2007. 10

위·변조에 안전한 RFID 지급결제시스템

김 인 석,[1†] 최 은 영,[2] 이 동 훈,[2] 임 종 인[2‡]
[1]금융감독원, [2]고려대학교

Secure RFID-based Payment System against Various Threats

In Seok Kim,[1†] Eun Young Choi,[2] Dong Hoon Lee,[2] Jong In Lim[2‡]
[1]Financial Supervisory Service, [2]Korea University

요 약

실생활에서 자동 인식 시스템은 바코드를 이용한 시스템이 대부분을 차지하며, 이러한 바코드 기반 자동 인식 시스템은 바코드의 인식거리에 대한 제한과 보안상의 문제점을 지적 받아왔다. 최근 바코드 기반 자동 인식 시스템보다 저장능력이 뛰어난 비접촉식 무선 주파수 인식(RFID: Radio Frequency Identification) 시스템이 주목을 받고 있으며 많은 연구가 이루어지고 있다. 특히 RFID 시스템은 물리적인 접촉없이 개체에 대한 정보를 인식한다는 점에서 화폐의 위·변조를 확인하는 매체로 사용가능하다. 본 논문에서는 RFID 시스템을 화폐에 적용하여 화폐의 위·변조 여부가 확인 가능한 지급결제시스템을 제안한다. 제안하는 지급결제시스템은 사용자의 프라이버시 침해의 문제를 해결하였으며, 추가적으로 위·변조 화폐의 사용자를 추적할 수 있는 기능을 제공한다.

ABSTRACT

Barcodes have been widely used to implement automatic identification systems but there are various problems such as security weakness or distance restriction in scanning barcode signals in a barcode-based automatic identifcation systems. Recently researchers are gradually interested in radio frequency identification (RFID) and RFID systems have been applied to various fields than before. Especially one of RFID application fields, a bank system uses RFID tagged bankontes to prevent illegal transactions such as counterfeiting banknotes and money laundering. In this paper, we propose a RFID system for protecting location provacy of a banknote holder. In addition, our paper describes that a trust party can trace a counterfeit banknote holder to provide against emergencies.

Keywords : *RFID, banknote*

Ⅰ. 서 론

최근 첨단 사무기기의 발달로 위·변조 화폐가 폭증하고 있으며 이에 대한 대책으로 위·변조 화폐를 구별할 수 있는 지급결제시스템이 제안되고 있으나 대부분 물리적인 접촉 하에서 사람의 육안으로 구별해야 하기 때문에 그 정확도가 낮다. 최근 주목받고 있는 자동 인식 시스템은 무선 주파수를 이용하여 물리적인 접촉 없이 개체에 대한 정보를 읽거나 기록하는 무선 주파수 인식(RFID: Radio Frequency Identification) 시스

접수일: 2007년 7월 10일; 채택일: 2007년 7월 31일
† 주저자, inskim@fss.or.kr
‡ 교신저자, jilim@korea.ac.kr

템이다.

최근 Juels는 유럽 중앙은행(European Central Bank)에서 사용할 위·변조 화폐 구별 지급결제시스템을 제안하였으며, 이 지급결제시스템은 위·변조 화폐 구별의 정확성을 높이기 위해 RFID를 화폐에 적용한 시스템이다 [1]. 이 지급결제시스템에서는 물리적인 접촉없이 인식이 가능하다는 RFID 시스템의 장점을 이용하여, 화폐에 RFID 태그를 내장함으로써 손쉽게 화폐의 위·변조를 확인 가능하게 시스템을 설계하였다. 그러나 RFID 시스템의 물리적인 접촉없이도 인식이 가능하다는 특징은 시스템의 안전성과 프라이버시 측면에서 여러가지 문제를 발생시킨다. Juels가 제안한 지급결제시스템은 태그와 리더의 통신에 제 삼자의 도청이 가능하며 도청한 정보를 사용하여 (1) 특정 화폐를 소지한 사용자의 위치 추적, (2) 화폐의 비밀 정보 노출이 가능하다. 이처럼 기존에 제안된 지급결제시스템들은 RFID 시스템을 적용하여 화폐의 위·변조를 확인할 수 있으나 화폐를 소지한 사용자의 프라이버시를 침해한다는 점에서 실제 생활에 적용하는 것이 부적절하다[2]. RFID 시스템에 대한 관심이 높아지면서 RFID 시스템의 프라이버시 침해문제를 해결하기 위해 영구적으로 태그를 무력화시키는 물리적인 기법과 암호학적 알고리즘 또는 단순한 연산자를 사용하는 다양한 기법들이 제안되었다[1-15].

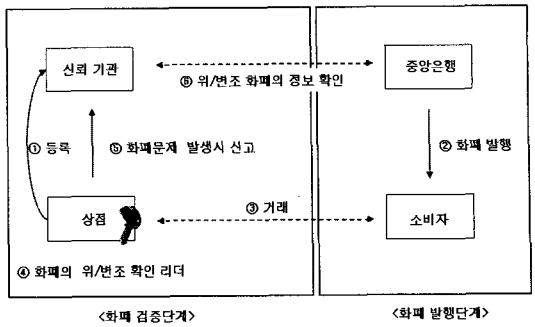
본 논문에서는 사용자의 프라이버시를 보호하고, 사용자에 대한 불법적인 추적이 불가능한 위·변조 화폐 확인 지급결제시스템을 제안한다. 제안하는 지급결제시스템은 현행 화폐가 만족해야만 하는 특성인 익명성, 양도성, 이동성과 즉시 결제성을 제공하고, 리더와 RFID 태그 모두 단순한 해쉬 함수 연산을 사용하여 효율적인 지급결제시스템을 구성할 수 있다.

Ⅱ. 위·변조에 안전한 RFID 지급결제시스템

제안하는 지급결제시스템에서 상점의 등록, 화폐 발행과 위·변조 검증 단계로 나누어 살펴보도록 하자[그림 1].

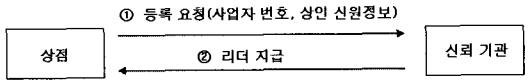
2.1. 등록단계

상인은 화폐의 위·변조 확인이 가능한 리더를 발급



〔그림 1〕 전체 시스템 구성도

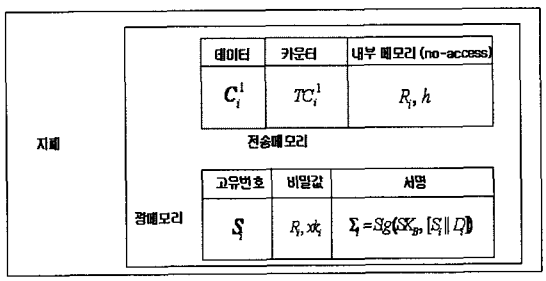
받기 위해서 신뢰기관에 상점의 사업자 번호를 등록하는 절차[그림 2]를 수행한다. 신뢰기관은 상점의 사업자 번호와 상점 주인의 정보가 올바른 경우에만 상점에 리더를 지급한다.



〔그림 2〕 등록단계

2.2. 화폐 발행 단계

1) 중앙은행은 화폐의 위·변조 방지를 위해 화폐마다 서명을 생성하여 RFID에 저장하며, 태그가 전송하는 값의 기밀성을 제공하기 위해서 암호화된 형태로 데이터를 저장한다[그림 3].



〔그림 3〕 태그 메모리 형태

(중앙은행의 서명키:(SK_B, PK_B), 화폐i의 고유번호:S_i, 화폐단위:D_i, Sig: 선택적 메시지 위·변조 공격에 안전한 서명 알고리즘, 해쉬 함수: h, 카운터:TC_i^1, 난수값: R_i, 태그 T_i의 비밀값 k_i, 신뢰기관의 (비밀키x, 공개키$y = g^x$))

2) 중앙은행은 화폐에 저장할 데이터의 기밀성을 보장하기 위해서 신뢰기관의 공개키를 사용하여 암

호문 C_i와 C_i^1를 생성한다.

$$C_i = [\alpha_i^0, \beta_i^0] = [(S_i \| \sum^i \| D_i) y^{k_i}, g^{k_i}],$$
$$C_i^1 = C_i \oplus h(TC_i^1 \oplus R_i)^{1)}$$

화폐의 태그에 저장된 정보는 태그의 세 개의 메모리 영역, 광메모리, 전송메모리와 내부 메모리 영역에 나뉘어 저장된다. 각각의 메모리의 형태는 다음과 같다.

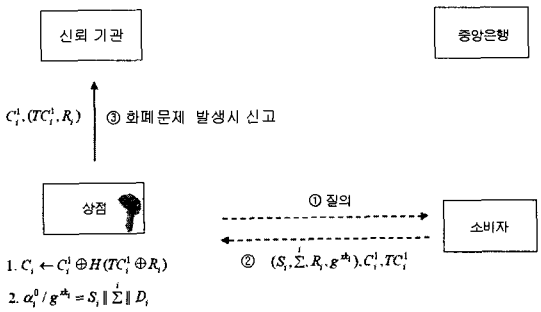
- 광메모리 : 광메모리 영역의 데이터의 형태는 현행 화폐에 적히는 숫자와 같은 형태이며 손쉽게 읽힐 수 있는 기계적 언어로 쓰인다. 이 영역에는 화폐의 고유번호 S_i, 서명 $\sum^i$, 비밀값 (R_i, xk_i)이 저장되어 있다. 이 영역에 저장된 비밀값은 제 삼자가 전송 메모리 영역의 정보 변경을 확인 가능하도록 한다. 광메모리 영역은 비접촉으로 읽히지만 제 삼자에 의해서 도청이 불가능하다.
- 전송메모리 : 일반적인 리더와 태그의 데이터 전송과정과 같은 영역이다. 리더의 질의에 응답하는 정보를 포함하고 있다. 이 영역에는 암호문 C_i^1와 카운터 TC_i^1을 저장하고 있다.
- 내부메모리 : 리더의 질의에 매번 다른 값을 전송하기 위해 필요한 부분이다. 이 영역에는 비밀값 R_i이 저장되어 있으며 해쉬 함수 h가 내장되어 있다. 이 부분은 외부의 접근이 불가능하다.

사용자는 이러한 화폐를 은행에 예치된 금액에 준하여 인출 가능하다. 인출한 화폐에 관련된 정보와 사용자의 정보를 은행의 데이터베이스에 저장한다. 화폐에 대한 문제가 발생하였을 경우 그 화폐와 관련된 사용자의 정보를 얻는다. 만약 이러한 과정이 은행의 CD(Cash Draw)나 ATM(Automatic Teller Machine)을 통해서 이루어질 경우에도 CD/ATM의 내부에 리더 기능을 추가함으로써, 인출하는 화폐와 사용자의 정보를 저장한다.

1) C_i^1는 i번째 태그와 리더 간 통신에서 첫 번째로 생성된 암호문을 의미한다. 일반적으로 C_i^j은 i번째 태그의 j 번째 통신에서 전송되는 암호문을 의미하며, 길이는 1024비트로 정한다.

2.3. 화폐의 위·변조 검증 단계

상점에서 사용자가 물건을 구매하고 돈을 지불한다. 상점의 상인은 계산대 주위에 리더를 통해서 화폐의 위·변조를 확인한다. 구체적인 과정은 다음과 같다.



[그림 4] 화폐의 위·변조 검증 단계

1) 화폐의 태그는 리더에 대한 응답으로 광메모리 영역의 고유번호 S_i, 서명 $\sum^i$, R_i, xk_i과 전송 메모리 영역의 암호문 C_i^1와 카운터 TC_i^1을 전송한다.
2) 상점의 리더는 전송받은 암호문 C_i^1를 이용하여 $C_i (= [\alpha_i^0, \beta_i^0] = [(S_i \| \sum^i \| D_i) y^{k_i}, g^{k_i}])$를 계산하고 광메모리 영역에서 얻은 xk_i값을 이용하여 $\alpha_i^0 / g^{xk_i} = S_i \| \sum^i \| D_i$ 인지를 확인한다. 만약 두 값이 동일하지 않은 경우 화폐의 정보에 대한 위·변조가 발생한 것이므로 상점에서 신뢰기관에 $C_i^1, (TC_i^1, R_i)$을 전송한다.

화폐의 위·변조에 검증하는 단계의 구체적인 흐름은 [그림 4]와 같으며, 화폐 i가 리더와 j번째에 통신을 하게 되면 화폐의 태그는 다음의 과정을 수행한다.

1) 화폐의 태그는 리더로부터 질의를 받을 때마다 카운터 TC_i^1를 증가시킨다. 현재 j번째 통신이므로 카운터 값은 TC_i^j이 된다.
2) 카운터 TC_i^j와 비밀값 R_i을 해쉬 함수 h의 입력값으로 하여 $h(TC_i^j \oplus R_i)$을 생성한다.
3) $h(TC_i^j \oplus R_i)$을 사용하여 j번째 응답으로

$C_i^j = C_i \oplus h(TC_i^j \oplus R_i)$을 생성하여 전송한다.

2.4. 추적 단계

신뢰기관은 전송받은 $C_i^1, (TC_i^1, R_i)$ 값을 통해서 위·변조된 화폐의 고유번호 S_i를 알아낸다. 그 과정은 다음과 같다.

1) 신뢰기관은 전송받은 값 $C_i^1, (TC_i^1, R_i)$을 이용하여 $C_i (= [\alpha_i^0, \beta_i^0] = [(S_i \| \sum^i \| D_i) y^{k_i}, g^{k_i}])$을 얻는다.

2) 신뢰기관은 화폐와의 직접적인 접촉 없이도 생성한 C_i에 자신의 비밀값 x를 이용하여 위·변조된 화폐의 고유번호와 서명을 얻는다.

$$\alpha_i^0 / (\beta_i^0)^x = S_i \| \sum^i \| D_i$$

이와같이 제안한 지급결제시스템은 네 단계로 구성되며 추가적으로 상점이 다음 과정을 수행한다면 위/변조 화폐 사용자의 신원까지도 확인할 수 있다.

1) 상점의 리더와 화폐의 태그가 통신할 때, 리더가 상점의 사업자 번호를 그 화폐의 태그에 쓴다.
2) 상점의 자체 데이터베이스에 화폐의 고유 번호와 사용자의 식별 정보를 저장한다. 상점의 데이터베이스는 고유번호와 사용자 정보에 대한 것을 하루 단위로 중앙은행에 전송한다.
3) 만약 그 화폐에 위/변조 사건이 발생하면, 상점에서 신뢰기간에 위/변조 발생 화폐에 대한 정보를 전송하고 신뢰 기간은 그 정보들을 데이터베이스에서 저장하고 관리한다.
4) 신뢰기관은 위/변조된 화폐의 고유 번호를 통해서 그 화폐를 사용한 사용자를 추적 가능하다.

이러한 추적의 기능은 일반적인 화폐에 적용하기 보다는 사용자의 신원을 확인하는 수표에 적용하는 것이 더 적합하다. 만약 제안한 지급결제시스템이 수표에 적용되고 그 수표에 위·변조 사건이 발생한다면, 중앙은행은 상점으로부터 신고를 받고 사용자의 신원확인이 가능하다.

Ⅲ. 안전성 및 효율성 분석

본 장에서는 사용자의 프라이버시 보호 가능한 화폐의 위·변조 방지 지급결제시스템의 안전성 및 효율성에 대해서 분석한다. 우선 제안한 지급결제시스템에서의 화폐 위·변조 가능성, 제안한 지급결제 시스템의 사용자의 프라이버시 보호 측면에서 안전성을 분석하고, 효율성에 대해서 분석한다.

3.1. 안전성

3.1.1. 화폐의 위·변조 불가능성

제안한 지급결제 시스템에서, 화폐의 고유 번호는 중앙은행의 비밀 서명키에 의해 서명된 값을 광메모리 영역에 저장하고 있다. 선택적 메시지 위·변조 공격에 안전한 서명 알고리즘을 사용하기 때문에 제 삼자가 주어진 서명을 획득함으로써 새로운 고유 번호에 대한 서명을 생성해 낼 수 없다. 그러므로 주어진 화폐는 새로운 고유번호에 대한 화폐 위·변조가 불가능하다. 더불어 화폐 위·변조의 어려움은 화폐 제작 기술의 비밀성에 있다.

제안한 지급결제시스템에서도 화폐의 광메모리 영역에 메시지를 저장하여 화폐를 생성해 낸다는 점에서 위·변조의 어려움을 뒷받침한다.

3.1.2. 사용자의 프라이버시 보호

1) 태그의 정보 유출 불가

화폐에 내장된 태그는 광메모리와 전송메모리 영역으로 나뉜다. 광메모리 영역은 제 삼자의 도청이 불가능하다는 메모리의 특성으로 인해서 일반적인 리더의 질의에 응답하는 영역은 전송메모리 영역이다. 전송메모리 영역에는 화폐의 고유번호 S_i를 신뢰기관의 공개키 y를 사용하여 암호화한 $C_i^j = C_i \oplus h(TC_i^j \oplus R_i)$ 값이 저장되어 있기 때문에 신뢰기관의 공개키에 대응하는 비밀값 x에 대한 정보를 모르는 제 삼자는 태그의 응답을 통해서 화폐의 고유번호에 대한 어떤 정보도 얻을 수 없다. 그러나 C_i^j와 TC_i^j가 공개되기 때문에 제 삼자가 특정 사용자의 화폐 소지 여부는 알 수 있다.

2) 화폐 소유자의 위치 정보 유출 불가

제안한 지급결제 시스템에서 화폐는 고유번호, 금액 단위와 서명으로 이루어진 고정된 값을 저장하고 있다. 그러나 제안한 지급결제 시스템에서 고정된 값을 저장하고 있으나 리더의 질의에 응답할 때는 카운터 값 TC_i^j과 난수값 R_i를 포함한 해쉬 값 $h(TC_i^j \oplus R_i)$을 이용하여 매번 다른 값 $C_i^j = C_i \oplus h(TC_i^j \oplus R_i)$을 생성한다. 그러므로 화폐에 내장된 태그는 리더의 질의에 매번 다른 값을 전송하기 때문에 특정 화폐 소유자의 위치 정보를 얻을 수 없다. 즉 사용자의 위치정보에 대한 프라이버시 침해가 불가능하다.

3.2. 효율성

저가의 RFID 시스템은 전력 소비, 연산 처리 시간, 저장, 게이트 (gate) 수 와 같은 부분에서 많은 제약을 갖는다. MIT의 Auto-ID 센터는 5센트의 저가의 태그 설계에 대해서 언급하였다[14]. 이러한 저가의 태그는 대략 500~5,000 게이트 정도로 구현될 수 있다. 그래서 이전에 제안된 기법들은 최저가의 RFID 시스템에 적용하기 어렵다. 기존에RFID 시스템을 적용한 기법들은 RFID 태그의 연산량을 줄이기 위해 외부장비를 통해서 태그의 정보를 변경하였다. 이러한 기법들은 외부장비를 항상 신뢰해야 한다는 문제점을 갖고 있다. 더구나 첨단 과학기술의 발달로 RFID 태그의 연산 처리에 대한 기능이 향상되고 있다. 최근, Feldhofer가 블록 암호 AES (Advanced Encryption Standard)를 5000개의 게이트만으로 설계하는 방법을 제안하였다 [4]. 본 논문의 제안한 지급결제 시스템에서 사용한 해쉬 함수는 AES 보다 더 단순한 구조이며, 하드웨어 기술의 발달로 인해 5000개의 게이트 이하에서 구현이 가능하게 될 것이다. 그러므로 제안한 지급결제시스템은 해쉬 함수(1번)와 단순한 XOR 비트 연산(2번)만을 요구하기 때문에 저가의 RFID 시스템에 적용 가능하다.

Ⅳ. 결론

최근, RFID 시스템은 원거리 통신으로 사물을 인식한다는 점에서 물류, 유통 등 다양한 분야에서 유용한 도구로써 인식되어 많은 연구가 이루어지고 있다. 또한, RFID 시스템의 이러한 특성은 화폐에 적용되어 화폐의 위·변조 여부를 확인하는 방법을 제시하였다. 그러나 RFID 시스템의 동작 원리의 특성상 사용자의 프라이버시 침해가 가능하다. 본 논문에서는 RFID 시스템에 기반한 사용자의 프라이버시를 보호 가능한 위·변조 화폐 확인 지급결제 시스템을 제안한다. 제안한 지급결제 시스템에서는 화폐의 태그 내에서 자체적으로 해쉬 함수를 적용하여 항상 새로운 응답을 전송하여 사용자의 프라이버시를 보호한다. 추가적으로 제안한 지급결제 시스템은 위·변조 화폐를 사용한 사용자의 신원 확인이 가능하며 이로 인해 부정한 행위를 한 사용자도 찾을 수 있다는 점에서 유용한 지급결제 시스템이다.

참고문헌

[1] A. Juels and R. Pappu. Squealing euros: Privacy protection in RFIDenabled banknotes. Financial Cryptography(FC'03), Springer - Verlag, LNCS 2742. pp. 103-121, 2003.

[2] G. Avoine. Privacy Issues in RFID Banknote Protection Schemes. Cardis'04, Kluwer, pp. 33-48, 2004

[3] G. Avoine and Ph. Ocehslin, A Scalable and Provably Secure Hash-Based RFID Protocol. PerSec 2005, IEEE Computer Society Press, Kauai Island, Hawaii, USA, 2005.

[4] M. Feldhofer, S. Dominikus, and J. Wolker storfer. Strong Authentication for RFID Systems using the AES Algorithm. CHES04 , LNCS 3156, pp. 357 - 370, Springer-Verlag, 2004

[5] D. Henrici and P. Muller. Hash-based Enhance ment of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. PerSec'04 at IEEE PerCom. pp. 149-153, 2004.

[6] A. Juels. Minimalist cryptography for Low-Cost RFID Tags. In The Fourth International Conferecne on Security in Communication Networks-SCN 2004, vol. 3352 LNCS, pp.

149-164, Springer-Verlag. 2004.

[7] A. Juels, R. L. Rivest and M. Szudlo. The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy. In the 8th ACM Conference on Computer and Communications Security, pp. 103-111, ACM Press. 2003.

[8] S. Junichiro, R. Jae-Cheol and S. Kouichi. Enhancing privacy of Universal Re-encryption scheme for RFID Tags. EUC 2004, Vol. 3207 LNCS, pp. 879-890, Springer-Verlag, 2004.

[9] R. Keunwoo, K. Jin, K. Seungjoo and W. Dongho. Challenge-Response based secure RFID Authentication Protocol for Distributed Database Environment. SPC2005, Vol. 3450 LNCS, pp. 70-84, Springer-Verlag, 2005.

[10] M. Ohkubo, K. Suxuki and S. Kinoshita. "Efficient Hash-Chain Based RFID Privacy Protection Scheme", Ubcomp2004 workshop.

[11] L. Su Mi, H. Young Ju, L. Dong Hoon and L. Jong In. Efficient authentication for Low-Cost RFID systems. ICCSA05, vol. 3480 LNCS, pp. 619~629, 2005.

[12] 유성호, 김기현, 황용호, 이필중. 상태 기반 RFID 인증 기법 프로토콜. 정보보호학회논문지, 제 4권, 6호, 2004

[13] S. A. Weis, S. E. Sarma, S. A. Weis and D. W. Engels. Security and privacy Aspects of Low-Cost Radio Frequency Identification Systems. First International Conference on Security in Pervasive Computing, 2003. http://theory.lcs.mit.edu/sweis/spc-rfid.pdf.

[14] X. Zhang and B. King. Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeiting. Information Security Conference, 2005

[15] Auto-ID Center, 860Mhz-960MHz Class I Radio Frequency Identification Tag Radio Frequency and Logical communication Interface Specification Proposed Re-commendation Version 1.0.0. Technical Report MIT-AUTOID-TR-007. AutoID Center, MIT, 2002.