제26회 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호 (2006. 11)

복구가능성과 불추적성을 제공하는 전자화폐의 효율성 향상을 위한 연구※

장승희*, 이창섭*, 송진욱*,
이정필*, 장우석*,
원동호*, 김승주*†
*성균관대학교 정보통신공학부 정보보호연구소
e-mail:icarus@ece.skku.ac.kr

A Study on Recoverable and Untraceable E-cash for Improving Efficiency

Seungheui Jang*, Changseop Lee*, Jinwook Song*,
Jungpil Lee*, Woosuk Chang*,
Dongho Won*, Seungjoo Kim*†
*Information Security Group, School of Information and Communication Engineering, Sungkyunkwan University

요 약

전자화폐가 안전하게 널리 사용되기 위해서는 여러 가지 특성을 만족해야 한다. 그러한 특성 중에서 데이터의 손실이나 분실에 따른 피해를 막기 위한 복구가능성과 사용자의 전자화폐 사용 내역과 같은 정보를 보호하기 위한 불추적성은 서로 충돌하는 특성으로 동시에 달성하는 것이 매우 어렵다. 기존에 제안된 전자화폐 시스템에서는 이 문제를 해결하는 과정에서 해쉬함수를 사용하였으나, 해쉬함수의 충돌회피성 때문에 실제로 구현하여 사용하는데 문제가 있다. 본 논문에서는 이에 대한 해결 방안을 제시하여 좀 더 효율적으로 구현 가능한 전자화폐 시스템을 제안한다.

1. 서론

디지털 기술이 발전함에 따라 물리적인 수단들이 점차 디지털화되어 가고 있다. 이러한 흐름 중의 하나로 물리적 가치단위인 화폐가 디지털화되어가고 있지만, 물리적 화폐의 특성인 익명성, 불추적성, 교환가능성 등을 동시에 보장하지 못하고 있으며, 물리적 화폐가 디지털화되었을 때 발생할 수 있는 문제들 때문에 전자화폐의 도입에 어려움을 겪고 있다.

특히, 전자화폐에 대한 데이터의 손실, 분실 또는 도난에 의하여 전자화폐를 사용하지 못할 경우, 그에 따른 모든 피해는 사용자가 받게 된다. 발급된 전자화폐에 대한 정보를 보관하고, 나중에 문제가 생길 경우 사용하지 못한 전자화폐를 재발급 받을 수 있도록 한다면 사용자의 피해를 최소화 할 수 있을 것이다.

본 논문에서는 기존에 제안되었던 복구 가능성과 불추적성을 보장하는 전자화폐 시스템[4]의 문제점을 분석하고 이를 해결할 수 있는 방법을 제안한다. 2장에서는 본 논문에서 사용될 용어들을 정의하고 설명한다. 3장에서는 기존 시스템[4]의 특징과 문제점을 분석하고, 4장에서는 이 문제점을 해결할 수 있는 방법을 제안하여 개선된 전자화폐 시스템을 제시한다. 5장에서는 기존 시스템[4]과 본 논문에서 제안한 방법을 사용하는 시스템을 간략히 비교 분석하고, 6장에서는 제안한 방법을 사용할 경우, 이를 확장하여 응용할 수 있는 몇 가지 내용들에 대해 다룬다. 마지막으로 7장에서는 앞으로 더 연구해야 할 부분에 대해서 언급하고 결론을 내도록 한다.

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음
† 교신저자 : skim@security.re.kr

2. 용어 정의 및 설명

본 논문에서 사용되는 용어들은 다음과 같다.

Bank : 은행
TTP : 제 3의 신뢰기관
*Sign** : * 의 전자서명
A : 동전의 일련번호
B : 동전과 유효성과 관련된 정보
C : $\{A,B,Sign_{Bank}(A,B)\}$, 은행에서 발급한 동전
H() : 해쉬함수
mod : 나머지 연산
m : *TTP*에서 하루에 발급 가능한 *y*의 최대 개수, 상점과 은행에 공개.
D : 년/월/일로 표현되는 복구데이터 발급일자
N : 한 번의 전자화폐 데이터 복구 요청 시 발급받을 수 있는 동전의 최대 개수
n : 사용자가 전자화폐 데이터 복구를 요청한 동전의 개수 ($n \le N$)
r : $0 \sim m-1$ 사이의 난수값
k : $0 \sim N$ 사이의 난수값
x_i : 해쉬함수 입력 값, 복구 시 사용되는 데이터
x_i' : $r + mk_i$
y : $H(x_i)$
y' : $x_i' \bmod m$
S_c : $Sign_{TTP}\{C, x_i\}$
S_c' : $Sign_{TTP}\{C, D, x_i'\}$
S_b : $Sign_{TTP}\{y, n\}$
S_b' : $Sign_{TTP}\{D, y', n\}$
R : $\{S_b, y, n\}$, 기존 시스템의 복구데이터
R' : $\{S_b', D, y', n\}$, 제안한 시스템의 복구데이터

3. Joseph 등이 제안한 전자화폐 시스템 분석

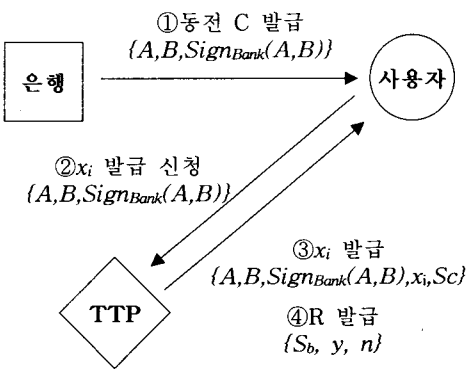
사용자의 거래내역을 모두 저장하는 데이터베이스를 구축하고, 후에 사용자의 거래내역을 모두 조사해보면 사용자가 발급받은 전자화폐에서 사용된 금액을 알 수 있다. 하지만 불추적성을 보장하기 위해 사용자의 거래내역을 저장할 수 없기 때문에 새로운 기법을 필요로 한다. Joseph 등이 제안한 기존 시스템[4]에서는 이 문제를 해결하기 위해 제 3의 신뢰기관(*TTP*)을 도입하였다. *TTP*에 은행에서 발급받은 동전 *C*의 일련번호 *A*를 모두 등록하고, 상점이 *TTP*에 거래 내역을 통보하면 사용된 동전과 사용되지 않은 동전의 정보를 알 수 있다. 그러나 상점에서 거래내역을 *TTP*에 전송해야 하는 부담이 추가로 발생하고, 사용량이 증가하면 데이터베이스의 크기가 증가하여 사용된 일련번호 검색의 효율성이 떨어진다. 이 문제는 해쉬함수를 이용하여 해결하였다. 아래와 같이 동일한 해쉬값 *y*를 갖는 입력값 x_i를 발행하는 화폐의 개수만큼 미리 찾아놓고, 이 x_i를 각각의 화폐에 함께 부여한다. 사용자가 *y*와 x_i를 발급받은 동전의 총 개수 n을 가지고 있으면 *TTP*에 거래내역을 저장하지 않아도 이 정보를 통해 은행에서 복구가 가능하게 된다. 자세한 복구 과정은 아래의 과정을 통해 설명할 것이다. 이 때 x_i는 사용자의 신원과 무관한 데이터 값 이므로 불추적성과 복구가능성을 동시에 만족한다.

$$H(x_1) = H(x_2) = H(x_3) = \ldots = H(x_n) = y$$

이 시스템에서 사용하는 전자화폐의 금액 단위는 동전이라는 하나의 단위만 존재한다. 그리고 기존의 시스템[4]과 본 논문에서 제시하는 개선된 시스템은 다음과 같은 과정으로 구성된다.

(1) 전자화폐의 발급과정

사용자는 은행에서 동전 *C*를 발급받은 후 *TTP*를 통해서 복구를 원하는 동전의 x_i와 복구정보 *R*을 부여받는다.



(그림 1) 전자화폐 발급과정

(2) 전자화폐의 사용과정

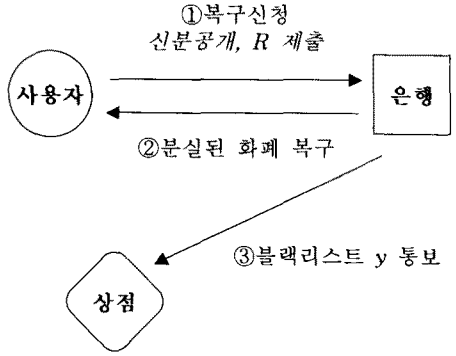
상점은 사용자로부터 넘겨받은 동전의 x_i를 해쉬함수를 이용하여 블랙리스트에 있는지 검사 후 없으면 거래를 수행한다.

(3) 전자화폐 예치과정

상점은 하루의 마지막에 은행에 C와 x_i를 전송한다. 은행에서는 상점과 마찬가지로 받은 동전에 대해 블랙리스트 검사 후, 이상이 없으면 동전의 정보를 데이터베이스에 저장하고, 상점의 계좌에 해당 금액을 예치하게 된다.

(4) 전자화폐 복구과정

사용자가 동전을 분실한 경우, 은행에 자신의 신분을 공개하고 R을 제출한다. 은행은 R의 서명이 유효한지 검증한다. 이상이 없는 경우, 데이터베이스에 저장되어 있는 x_i를 해쉬함수를 이용하여 결과값이 y인 동전의 개수를 찾는다. 은행이 발급해준 동전의 개수 n에서 검색된 y의 개수를 제외하면 사용자가 잃어버린 동전의 개수를 알 수 있어 복구가 가능하다. 또 사용자가 실제로 분실하지 않았으나 분실한 것처럼 은행을 속이고 동전을 복구 받아 부정 사용하는 것을 방지하기 위해서, 복구와 동시에 상점에 y를 블랙리스트로 통보한다.



(그림 2) 전자화폐 복구과정

기존 시스템[4]은 TTP에서 사용자의 익명성 보장을 위해 해쉬함수를 사용, 사용자의 신원 정보와 무관한 x_i를 구한다. 하지만 이 방법은 해쉬함수의 기본특성인 충돌회피성 때문에 서로 다른 입력 값 x_i에 대해 동일한 해쉬값 y를 갖는 x_i의 집합들을 찾아내는데 매우 많은 시간이 필요할 뿐만 아니라 이를 저장하기 위한 방대한 데이터베이스가 요구된다. 또한 해쉬함수의 해쉬값의 크기가 한정되어 있으므로, 일정 시간이 지나면 y의 값이 모두 사용된다는 문제점이 있다.

4. 제안하는 전자화폐 시스템

(1) 해쉬함수의 대체

기존 시스템[4]에서는 x_i를 생성하기 위해서 해쉬함수를 사용하지만 충돌회피성을 위반하는 문제점이 있다. 이를 해결하기 위해 해쉬함수를 대체할 수 있는 다음과 같은 수학적 연산을 제안한다.

$$r + mk_i = x_i'$$
$$x_i' \bmod m \equiv y'$$

x_i', y'는 기존 시스템의 x_i, y를 대체한다. r은 난수값으로, y'을 결정하기 때문에 복구데이터 발급 신청 시 중복되지 않아야 한다. 또한 y'는 유일한 값이기 때문에 r은 0과 $(m-1)$사이의 값이 되어야 한다.

이 연산은 합동식의 특성을 이용하여, m을 법으로 하는 합동인 x_i'의 집합을 쉽게 찾을 수 있다는 점에 착안하였다. 이로 인해 해쉬함수에 비해 쉽게 계산이 가능하다는 장점이 있다. 그러므로 기존 시스템[4]처럼 해쉬 입력 값과 해쉬값으로 구성된 방대한 데이터베이스를 미리 계산하여 구축할 필요가 없다. 그리고 x_i' 역시 x_i와 같이 사용자의 신원과 관련된 어떠한 정보도 포함하고 있지 않기 때문에 불추적성을 여전히 만족한다.

기존 시스템[4]은 해쉬함수의 특성인 일방향성 때문에 제 3자에 의한 x_i의 유추가 매우 어렵다. 반면에 본 논문에서 제안한 방법은 합동식의 특성으로 인해 x_i'을 쉽게 유추할 수 있다는 문제가 있다. 하지만 x_i'이 유출되더라도 위조를 위해서는 TTP의 전자서명이 필요하기 때문에 TTP의 개인키가 유출되지 않는 한 악용될 소지는 없다.

(2) 복구 데이터 발급 날짜의 추가

앞서 설명했듯이 기존 시스템[4]에서는 해쉬함수의 해쉬값의 크기가 한정되어 있으므로, 일정 시간이 지나면 y의 값이 모두 사용된다는 단점이 있다. 이 문제는 동전 C에 x_i이외에 복구데이터 발급 날짜인 D를 추가하여 간단히 해결할 수 있다.

D를 추가할 경우 y'의 값이 각각의 D에 대해서만 유일하면 되기 때문에, 서로 다른 D에 대해서 동일한 y'를 사용할 수 있게 된다. 이외에도 상점과 은행에서 블랙리스트를 검색할 때, D를 기준으로 검색할 경우 검색 범위가 크게 줄어들어 효율성이 증가한다.

5. Joseph 등이 제안한 기존 시스템과의 비교 분석

Joseph 등이 제안한 기존 시스템	제안하는 시스템
동일한 해쉬 값 y를 갖는 x_i의 집합을 찾기가 어려움 (충돌회피성 위반)	합동식의 특성을 이용하여, m을 법으로 하는 합동 x_i의 집합을 쉽게 구함
(x_i,y)의 쌍을 사전에 미리 계산하여 DB에 저장 필요	복구 데이터 발급신청 즉시 빠르게 계산 가능하므로 DB 불필요
블랙리스트 검색 시 모든 y를 검색	D를 기준으로 검색하므로 효율적
제 3자에 의한 x_i의 추측이 어려움	제 3자에 의한 x_i의 추측이 쉬움

6. 제안한 시스템의 응용

*TTP*에서 하루에 발급 가능한 R'의 최대 개수는 m개이다. 하루에 m개를 초과하는 발급 신청이 요청될 경우 다음과 같은 방법을 사용하면 이를 해결할 수 있다.

(1) 미사용 D의 활용

사용하지 않는 D를 활용하여 m의 개수를 늘릴 수 있다. 예를 들면, 2006년 9월 21일에 총 발급 신청의 건수가 m을 초과할 경우 시스템 도입 이전 연도의 D인 1006년 9월 21일을 같은 날짜로 처리하는 것이다. 또는 존재하지 않는 13월을 1월로 14월을 2월로 같다고 가정하고 그 D를 사용하는 방법도 가능하다.

(2) 복수 신뢰기관

*TTP*를 복수로 확장시키는 방법을 통해 m의 개수를 늘릴 수 있다. 이 방법은 R'이 어느 *TTP*에서 발급되었는지에 대한 정보가 추가로 필요하지만 m의 개수를 늘리는 것 외에도 하나의 *TTP*에 집중되는 부하를 분산시킬 수 있다는 장점이 있다.

7. 결론

복구가능성은 전자화폐 시스템의 절대적인 특성은 아니지만, 사용자의 피해를 막고 전자화폐가 널리 쓰이도록 하기 위해서 요구되는 특성이다.

본 논문에서 제안한 방법을 통해 불추적성과 복구가능성을 제공하고, 기존 시스템[4]에서 사용된 해쉬함수로 인한 문제점을 해결하였다. 또한 간단한 수학적 연산을 사용했기 때문에 효율성이 향상되었으며 구현 가능성이 높아졌으므로 이를 통해 전자화폐 도입에 긍정적인 역할을 할 수 있을 것을 기대해 본다.

그러나 본 논문에서 제안한 방법은 좀 더 효율적인 복구가능성과 불추적성을 제공하지만 전자화폐의 중요 특성인 분할가능성과 교환가능성은 아직 제공하지 못한다는 문제가 있다. 전자화폐의 활성화를 위해서는 이 문제점을 해결해야 하므로 추후 더 많은 연구가 필요할 것이다.

참고문헌

[1] Niels Ferguson. "Single Term Off-Line Coins", Proceedings of Eurocrypt 93, 1994.

[2] Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. In J. Feigenbaum, editor, Advances in Cryptology - CRYPTO '91, Lecture Notes in Computer Science, Springer-Verlag. 1992.

[3] S. Brands. Untraceable off-line cash in wallet with observers. In Advances in Cryptology - CRYPTO '93, Lecture Notes in Computer Science, Springer-Verlag, 1993.

[4] Joseph K. Liu and Victor K. Wei and Sandy H. Wong, Recoverable and Untraceable E-cash. Proceedings of International Conferences on Trends on Communications, EUROCON'2001,Vol.1, Bratislava, Slovak Republic, July 2001