분할 가능한 화폐를 위한 새로운 환불 방식

최 형섭*, 김 상진*, 오 희국*

*한양대학교, 컴퓨터공학과

A New Refund Mechanism for Divisible Cash

Hyungsup Choi*, Sangjin Kim*, Heekuck Oh*

*Department of Computer Science and Engineering, Hanyang Univ.

요 약

선불방식의 화폐시스템에서 고객은 인출한 화폐를 은행으로부터 환불받을 수 있어야 한다. 그러나 분할된 화폐가 서로 연관될 수 있는 분할 가능한 화폐시스템에서는 고객이 사용한 화폐의 익명성을 유지하면서 남은 금액을 환불해주기가 어렵다. 이 논문에서 이런 문제를 해결한 새로운 방식의 환불 메커니즘을 제공한다. 제안된 새 방식에서 고객은 은행에 익명으로 접근하여 환불티켓을 인출하고, 나중에 인출된 티켓을 이용하여 기존 지불의 익명성을 유지하면서 환불을 받게 된다. 환불티켓을 사용하면 환불과정을 인출이나 지불과정과 독립적으로 제공할 수 있어 환불이 필요없는 경우에는 아무런 추가비용이 소요되지 않는 장점이 있다. 또한 같은 이유에서 여러 시스템에 쉽게 응용이 가능한 유연한 방식이다. 끝으로 환불액을 계속해서 하나의 티켓에 축적하는 방법을 사용하면 지불액과 환불액간에 직접적인 차액관계가 없어지므로 고객의 익명성이 증진되며, 은행에 접촉해야 하는 횟수를 줄여주는 효과가 있다.

I. 서론

전자화폐는 보통 선불방식(debit-based)이지만 후불방식(credit-based)[1]을 사용하는 경우도 있다. 후불방식은 사용한 금액만큼 나중에 청구하는 방식이므로 고객의 익명성을 보장할 수 없으나 환불(refund)이 필요 없는 방식이다. 반면에 선불방식은 익명성을 제공할 수 있지만 화폐를 인출할 때 화폐의 금액만큼 미리 지급하고 사용하므로 남은 화폐가 있다면 이것을 은행에 전달하여 환불을 받을 수 있어야 한다. 일반적인 동전방식의 오프라인 화폐[2]에서는 고객이 상점 대신 은행과 지불 프로토콜을 수행하여 아무런 문제없이 환불받을 수 있다. 그러나 하나의 화폐를 여러 개의 화폐로 나누어 사용할 수 있는 분할 가능한 화폐[3]에서는 환불받는 것이 간단하지 않다.

일반적으로 분할 가능한 화폐에서 각 분할된 화폐는 서로 연관이 된다[3,4]. 예를 들어, A라는 익명화폐가 a_1, a_2, a_3로 분할되어 사용될 수 있다고 하자. 고객이 a_1, a_2를 지불에 사용하고 a_3는 환불받고 싶다. a_1, a_2, a_3는 서로 연관되므로 a_3를 은행에 전달하여 환불을 요청하면 a_1, a_2의 익명성이 깨진다. 하지만 기존 분할 가능한 화폐를 제안한 논문에서는 환불에 대한 언급이 없다[3,4].

분할 가능한 화폐뿐만 아니라 동전들이 서로 연결되어 있는 시스템에도 같은 문제가 있다. Nguyen 등[5]은 오프라인 동전방식에서 여러 개의 동전을 이용하여 지불하면 지불의 효율성이 떨어지는 문제점을 해쉬체인(hash chain)[1]을 이용하여 극복하고자 하였다. 이를 위해 익명동전들을 해쉬체인을 이용하여 연결하여 사용하고 있다. 따라서 이 시스템에서도 사용하고 남은 동전을 반납하게 되면 기존에 사용된 동전과 체인으로 연결되므로 익명성에 문제가 생긴다. 하지만 이 시스템도 환불에 대한 언급이 없다.

이처럼 분할 가능한 화폐시스템이나 Nguyen 등과 같은 시스템의 환불 메커니즘은 다음과 같은 요구사항을 만족하여야 한다.

- **요구사항 1.** 원래 받아야 하는 금액만큼만 환불받을 수 있어야 한다.

- **요구사항 2.** 환불받을 화폐의 인출자만 환불받을 수 있어야 한다.
- **요구사항 3.** 이미 지불한 부분의 익명성이 유지되어야 한다.

수표방식의 시스템에서는 이미 환불 메커니즘을 제공하고 있다[6,7]. 수표방식에서 고객은 보통 하나의 수표를 지불하고 수표의 액면가와 지불대금의 차액에 해당하는 거스름을 받게된다. 온라인 수표시스템[6]에서는 은행이 거스름을 생성한다. 따라서 거스름 자체를 새로운 수표로 만들 수 있으며, 이것을 다시 지불에 사용할 수도 있고, 동전방식에서처럼 지불 프로토콜을 이용하여 쉽게 환불받을 수도 있다. 오프라인 수표시스템[7]에서는 지불과정에서 은행이 거스름을 만들어 줄 수 없으므로 수표를 인출할 때부터 두 부분으로 구성한다. 두 부분 중 하나는 지불에 사용하고 다른 하나는 환불에 사용한다. 이 두 부분은 서로 연관시킬 수 없으므로 환불을 받더라도 익명성은 계속 유지된다. 그러나 수표의 액면가가 고정되어 있으므로 고객이 환불을 받게되면 지불액과 환불액간에 차액을 통해 그 고객이 사용한 수표를 추측할 가능성이 있다. 이 문제는 분할 가능한 화폐에서도 있는 문제이지만 이런 화폐에서는 인출할 수 있는 화폐의 액면가가 고정되어 있지 않으므로 그 가능성이 수표방식보다는 적다.

오프라인 수표시스템에서 사용한 환불방법을 분할 가능한 화폐에 적용할 수 있지만 지불과정에서 환불받을 때 부정을 못하도록 하기 위한 추가적인 연산과 정보 교환이 필요하다. 온라인 수표시스템에서 거스름을 받는 방식을 응용하여 은행으로부터 환불받을 때 사용할 새로운 값을 받아 환불받을 수 있다. 이렇게 하면 환불이 필요 없는 경우에는 아무런 추가비용이 소요되지 않으며, 기존 인출이나 지불과정과 무관하게 환불을 제공할 수 있다. 또한 이런 문제가 있는 모든 시스템에 쉽게 적용이 가능하다. 하지만 은행에 환불티켓을 받은 후 다시 또 접촉해야 하는 불편함은 있다.

이 논문에서는 온라인 수표시스템의 환불방식을 응용한 새로운 환불 메커니즘을 제안한다. 이 메커니즘에서 고객은 익명으로 환불받을 부분의 정당성을 은행에 입증하고 은행으로부터 환불액에 해당하는 익명의 환불티켓을 인출받게 된다. 고객은 나중에 이 티켓을 은행에 전달함으로써 기존 지불의 익명성을 유지하며 환불을 받을 수 있다. 또한 지불액과 환불액간에 차액을 통해 이미 사용된 부분을 추측할 수 없도록 환불액을 하나의 티켓에 계속 축적할 수 있는 방법도 제시한다. 제시된 방법은 특정 시스템에만 적용할 수 있는 것은 아니고, 이런 문제가 있는 모든 시스템에 인출이나 지불과정에 영향을 주지 않고 쉽게 적용할 수 있다. 이 논문의 구성은 다음과 같다. 2장에서는 제안하는 새로운 환불방식을 설명하고, 그것의 장단점을 분석한다. 끝으로 3장에서는 결론과 향후 연구방향에 대해 서술한다.

II. 새로운 환불방식

1. 환불티켓 인출 프로토콜

고객은 사용하고 남은 금액을 은행에 지불하는 형식을 취하여 익명으로 환불티켓을 요청한다. 이 결과 고객은 익명의 티켓을 얻게 되며, 나중에 이 티켓을 이용하여 실제로 환불을 받게 된다. 환불티켓은 서론에서 나열한 요구사항을 만족하여야 한다. 특히 공격자가 전달되는 은닉된 티켓을 바꾸어 이득을 얻을 수 없어야 한다. 이것을 보장하는 두 가지 방법을 생각할 수 있다.

- **방법 1.** 전달되는 은닉된 티켓 자체를 변경할 수 없도록 만든다.
- **방법 2.** 은행이 은닉된 티켓에 대한 어떤 검증과정을 걸쳐 전달된 화폐의 인출자만이 사용할 수 있는 티켓인지 확인한다.

환불티켓에는 고객 식별자, 환불금액, 그리고 티켓을 독특하게 만들기 위한 요소가 포함되어야 한다. 고객 식별자는 티켓을 통해 환불받을 수 있는 고객을 한정하기 위해 필요하다. 환불티켓은 고객이 스스로 만들어 전달하므로 위에서 나열한 방법 1을 사용하면 은행이 올바른 고객 식별자가 포함되어 있는지 확인할 필요는 없다. 방법 2을 사용하면 화폐에 포함된 식별자와 티켓에 포함된 식별자가 같은지 영지식(zero knowledge) 방법으로 확인할 수 있다. 환불금액은 고객이 명시할 수도 있고 은행이 명시할 수도 있다. 고객이 명시할 경우에는 부정할 수 없도록 은행은 티켓을 발급하기 전에 금액을 확인하여야 한다. 반면에 은행이 서명키 등을 이용하여 금액을 명시하면 부정할 가능성이 없어지므로 편리하다. 하나의 환불티켓을 여러 번 사용할 수 없도록 하기 위해서는 티켓을 독특하게 만들고, 은행은 환불된 티켓을 보관하여 환불요청이 있을 때마다 이전에 사용된 티켓이 아닌지 확인하여야 한다. 환불티켓은 요구사항을 만족하는 어떤 형태로도 구성할 수 있다. 다음에는 환불티켓의 한 예를 제시한다.

그림 1은 RSA 기반 부분은닉서명[8]을 이용한 환불티켓 인출 프로토콜이다. 부분은닉서명에서 수신자는 은닉되는 m과 공개되는 c에 서명을 받

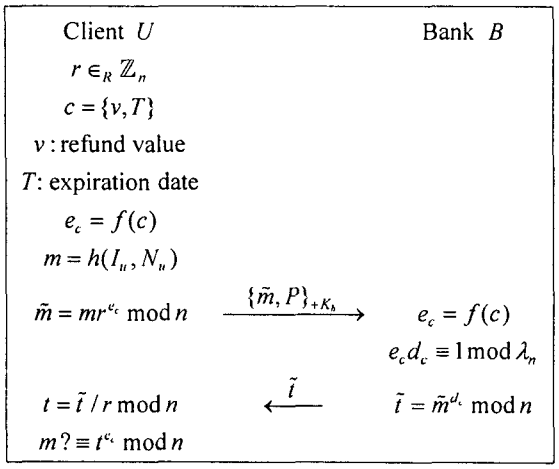

그림 1: 부분은닉서명을 이용한 환불티켓

게되지만 서명자는 결과 서명 $\mathrm{Sig}(m, c)$와 m에 대한 어떤 정보도 얻을 수 없다. 일반 은닉서명에서 서명자는 서명내용을 전혀 볼 수 없지만 부분은닉서명을 사용하면 서명자는 c정보가 서명에 반드시 포함됨을 확신할 수 있다. 그림 1에서는 부분은닉서명의 공개정보를 이용하여 환불액과 환불티켓의 유효기간을 명시한다.

그림 1에는 환불받을 화폐를 전달하고 확인하는 과정이 생략되어 있다. 이것은 환불 기능을 적용한 화폐시스템의 지불과정을 그대로 사용하면 되기 때문이다. 다만 은닉되어 전달되는 티켓을 공격자가 공격할 수 없도록 하여야 한다. 그림 1에서는 앞서 설명한 방법 1을 사용한다. 즉, 은닉된 티켓 $\tilde{m}$과 P를 같이 은행의 공개키 $+K_b$로 암호화함으로써 이 기능을 제공한다. 여기서 P는 환불받을 화폐의 인출자만이 알고 있는 정보라고 가정한다. 따라서 은행은 이 값을 확인함으로써 요청한 고객이 화폐의 인출자임을 확인할 수 있다. 다른 누구도 P를 알 수 없으므로 이 암호문은 오직 화폐의 인출자만이 만들 수 있다.

그림 1의 기술된 프로토콜을 보충 설명하면 다음과 같다. 고객은 환불액 v와 유효기간 T를 이용하여 c를 구성하고, 공개지수 생성함수 f를 이용하여 e_c를 생성한다. 고객은 환불티켓의 일련번호가 될 난스(nonce) N_u를 생성하고, 자신의 식별자 I_u와 함께 해쉬함수 h에 적용하여 m을 구성한다. 이 m은 나중에 환불티켓이 된다. 고객은 은닉요소 r을 선택하여 m을 은닉하고, 은닉된 $\tilde{m}$과 P를 은행의 공개키로 암호화하여 전달한다.

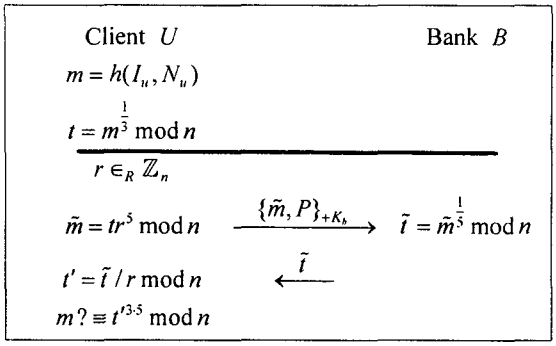

그림 2: 축적이 가능한 환불티켓

은행은 P를 이용하여 화폐를 확인하고 이상이 없으면 환불금액만큼만 환불받을 수 있도록 $\tilde{m}$에 서명하여 돌려준다. 실제 환불을 받기 위해 고객은 I_u, N_u, t, c를 은행에 전달한다. 은행은 t를 확인하고 이전에 사용된 티켓이 아니면 티켓의 일련번호 역할을 하는 N_u를 데이터베이스에 I_u와 연관시켜 저장해 놓는다. 환불요청이 들어오면 이 데이터베이스를 검색하여 이중요청이 아닌지 검사한 뒤 고객의 계좌에 환불액을 입금시킨다.

환불티켓을 사용하더라도 특정 화폐에 대한 환불액을 은행이 알고 있기 때문에 환불 요청이 있을 때 환불액에 해당하는 화폐를 데이터베이스에서 검색해 볼 수 있다. 어떤 고객이 600원을 환불받아갔는데 데이터베이스에 검색하여 보니 환불액이 600원에 해당하는 화폐가 오직 하나밖에 없는 경우가 있을 수 있다. 이처럼 은행은 환불액 정보를 이용하여 화폐의 인출자를 추측할 수 있는 가능성이 있다. 이 문제를 해결하기 위해 환불액을 하나의 티켓에 계속 축적하는 방법을 생각해 볼 수 있다. 만약 각각의 금액이 명시되지 않고 축적된 금액만 나타낼 수 있는 누적기를 환불티켓에 적용하면 은행의 추측가능성은 줄어든다. 이것은 축적된 환불액이 어떤 특정 화폐의 환불액과 직접적인 관계가 없어지기 때문이다.

환불액을 축적하기 위해 Chaum의 온라인수표에서 사용된 쿠키통(cookie-jar)를 이용할 수 있다[6]. 그림 2는 쿠키통을 환불티켓으로 이용한 환불티켓 인출 프로토콜이다. Chaum은 환불액을 나타내기 위해 여러 개의 RSA의 공개지수를 사용하였다. 이 논문에서도 공개지수 3, 5, 7, 11을 이용하며, 각각 100원, 200원, 400원, 800원을 나타낸다. 만약 어떤 공개지수에 대응되는 비밀지수로 티켓이 서명되어 있다면 해당 금액이 축적되어 있는 것을 나타낸다. 그림 2에서 고객은 이미 100원이 축적되어있는 환불티켓 $t = m^{1/3} \bmod n$을 가지고 있

다. 고객은 이 티켓에 200원을 더 축적한 새로운 티켓 $t' = m^{1/(3\cdot5)} \bmod n$ 을 얻게된다.

2. 안전성 분석

위조가능성: 그림 1과 2의 프로토콜에서 사용된 RSA modulus n의 인수분해를 모르면 직접적으로 환불티켓을 위조할 수 없다.

익명성: 그림 1과 2의 프로토콜에서 고객은 완전 익명성을 제공하는 은닉서명 프로토콜을 사용하여 티켓을 인출한다. 따라서 티켓과 환불받은 화폐를 연관시킬 수 있는 정보는 금액 정보뿐이다. 만약 금액 정보를 통해 티켓과 화폐를 연관시킬 수 없으면 기존 화폐의 익명성은 유지된다.

금액 정보를 통한 추측가능성: 각각의 환불액은 알 수 없고 최종 축적된 환불액만을 알 수 있는 이상적인 누적기가 있고, 100원단위로 축적한다고 하자. 이 때 환불티켓에 400원이 축적될 경우의 수는 100원을 4번, 200원을 1번하고 100원을 3번, 200원을 2번, 300원을 1번하고 100원을 1번, 400원을 1번한 경우로 총 5가지이다. 그러나 쿠키통을 누적기로 사용하면 각 공개지수가 몇 번씩 사용되었는지를 알려주어야 확인이 가능하다. 또한 하나의 환불액에 대해서 같은 공개지수를 여러번 적용하여 축적하지 않기 때문에 이상적인 누적기보다 경우의 수는 줄어든다. 예를 들어 $1/(3\cdot3\cdot5)$로 서명된 400원의 환불티켓이 있다면 100원 2번하고 200원을 1번한 경우와 100원을 1번하고 300원을 1번한 경우로 총 2가지 경우밖에 없다. 그러나 유통되는 화폐와 환불받는 고객이 많고, 하나의 티켓에 많은 금액을 축적하면 금액정보를 이용하여 고객을 추측할 가능성은 희박해진다.

이중사용: 은행은 환불된 환불티켓의 일련번호를 해당 고객과 연관시켜 데이터베이스에 기록해 두기 때문에 하나의 티켓을 이용한 이중요청은 쉽게 검출할 수 있다. 환불티켓의 인출은 은행에 화폐를 지불하여 티켓을 사는 형태를 취한다. 따라서 환불과 무관하게 지불시스템이 이중사용을 정확히 검출한다면 고객은 남은 금액 이상의 가치를 지닌 티켓을 인출할 수 없을 뿐만 아니라 이중으로 티켓을 인출할 수도 없다.

공격가능성: 환불받고자 하는 화폐에는 인출자만이 알고 있는 정보 P가 있다고 가정한다. 고객은 이 정보와 티켓을 은행의 공개키로 암호화하여 전달하므로 공격자는 이 부분을 변경할 수 없다.

III. 결론

이 논문에서는 기존 분할 가능한 화폐에서 화폐의 익명성을 유지하면서 사용하고 남은 금액을 환불받을 수 있는 새로운 환불 메커니즘을 제안하였다. 이 메커니즘은 기존 인출이나 지불과정과 독립적으로 제공할 수 있어, 환불이 필요 없는 경우에는 아무런 추가비용이 들지 않는다는 장점이 있다. 또한 같은 이유에서 이런 문제가 있는 여러 지불시스템에 쉽게 적용이 가능한 유연한 방식이다. 하지만 환불티켓을 인출한 다음에 다시 은행 또 접촉해야 하는 불편함이 있다.

또한 환불액을 하나의 티켓에 계속 축적할 수 있는 방법도 제시하였다. 이 방법을 사용하면 환불액을 통해 이미 지불에 사용한 화폐의 인출자를 추측할 수 있는 문제점을 극복할 수 있으며, 은행에 접촉하여야 하는 횟수도 줄일 수 있다. 그러나 이 논문에서 환불액을 축적하기 위해 사용한 쿠키통 방식은 많은 공개키 연산이 필요하며, 축적된 금액을 확인하기 위해 각 공개지수가 몇 번 사용되었는지 밝혀야 하는 문제점이 있다. 이에 보다 효율적이고, 이상적인 누적기의 연구가 필요하다.

참고문헌

[1] R. Rivest and A. Shamir, "Payword and Micromint: Two simple micropayment schemes," *Proc. of 1996 Int. Workshop on Security Protocols*, LNCS 1189, pp. 69-87, 1996.

[2] S. Brands, "Untraceable off-line cash in wallets with observers," *Crypto'93*, LNCS 773, pp. 302-318, 1993.

[3] T. Okamoto and K. Ohta, "Universal electronic cash," *Crypto'91*, LNCS 576, pp. 324-337, 1991.

[4] A. Chan, Y. Frankel, and Y. Tsiounis, "Easy come - easy go divisible cash," *Eurocrypt'98*, LNCS 1403, pp. 561-575, 1998.

[5] K. Nguyen, Y. Mu, and V. Varadharajan, "Secure and efficient digital coins," *Proc. of the 13th IEEE Computer Security Applications Conf.*, pp. 9-15, 1997.

[6] D. Chaum, "Online cash check," *Eurocrypt'89*, LNCS 435, pp. 288-293, 1989.

[7] A. Solages and J. Traore, "An efficient fair off-line electronic cash system with extension to checks and wallets with observers," *Financial Cryptography'98*, LNCS 1465, pp. 275-295, 1998.

[8] M. Abe and J. Camenisch, "Partially blind signature Schemes," *Proc. of the 1997 Symp. on Cryptography and Information Security*, SCIS97-33D, 1997.