전자화폐 설계시 안정성이 최고 고려 사항

물리적 화폐의 단점 보완, 화폐의 미래

본고는 한국정보보호진흥원에서 제공받은 자료로 디지털콘텐츠 산업에 있어서 가장 핵심적인 요소 중의 하나인 과금 체계에 대해 설명하고 있다. 온라인 과금 체계는 여러 가지가 있지만 본고에서는 전자화폐의 기술적인 부분과 시스템 구성도, 구성원(요인) 등에 대해 설명하고 있다. 특히 전자화폐는 물리적 화폐와 달리 복제와 이중 사용 등이 가능해 안전성이 무엇보다 요구된다고 할 수 있다.

-편집자 주-

〈출처: 한국정보보호진흥원〉

전자화폐 시스템 (Electronic Cash System)

1. 전자화폐 시스템의 기본적인 모델

전자화폐 시스템은 일반적으로 그것의 기본적인 요구사항과 가정이 무엇이냐에 따라서 구성 모델이 서로 상이할 수 있다. 본고에서는 오프라인 전자화폐 시스템의 가장 기본적인 요구사항과 가정에 기반을 두어 모델을 설명하고자 한다.

전자화폐 시스템의 구성원

전자화폐 시스템은 시스템 구성에 참여하는 구성원들과 그 구성원들 사이에서 일어나는 프로토콜로 이루어진다. 프로토콜에 참여하는 구성원들은 일반적으로 다음과 같이 이루어진다.

- 사용자(user)

전자화폐를 발행기관으로부터 발급 받아 그것을 각 상점에서 사용하는 주체.

- 상 점(shop)

사용자로부터 전자화폐를 구매대금으로 받는 공급자.

- 은 행(bank)

사용자에게는 전자화폐를 발급해 주는 발행기관이며, 상점에게는 전자화폐를 결제해 주는 결제기관.

상기에 설명된 구성원은 전자화폐 시스템에서의 최소 구성원이며, 확장된 요구사항과 가정에 따라 그것의 구성원이 증가할 수도 있다. 예를 들어, 익명성이 취소 가능한 전자화폐 시스템을 구성하기 위해서는 사용자 익명성 취소의 역할을 수행해 줄 수 있는 신뢰기관이 참여 구성원으로서 존재해야 한다.

전자화폐 시스템의 기본적인 프로토콜

전자화폐 시스템은 시스템 구성원들 사이에서 수행되는 프로토콜에 그 기반을 둔다. 즉, 전자화폐 시스템을 설계하기 위해서는 시스템 구성원들 사이의 각 프로토콜을 설계하면 되는 것이다.

일반적으로 상기에서 설명된 구성원들의 경우와 마찬가지로 설계하고자 하는 전자화폐 시스템의 요구사항과 가정이 무엇이냐에 따라 프로토콜은 달라질 수 있다. 본 절에서는 전자화폐 시스템의 가장 기본적인 프로토콜을 소개할 것이며, 그 내용은 아래와 같다.

- 인출 프로토콜 (withdrawal protocol)

사용자와 은행 사이에서 수행되는 프로토콜로서 은행이 사용자에게 전자화폐를 발급해 주는 절차를 명 세한 것으로서 전자화폐 시스템 설계 시 가장 중요한 부분이 된다.

- 지불 프로토콜 (payment protocol)

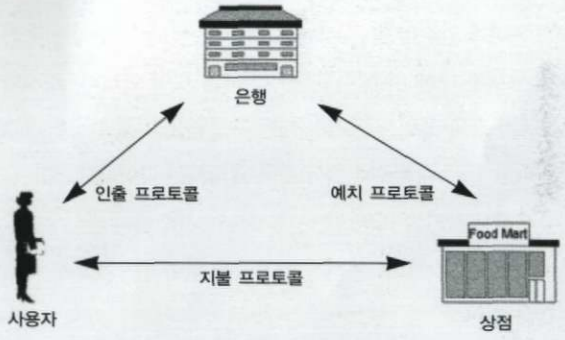
사용자와 상점 사이에서 수행되는 프로토콜로서 사용자가 구매대금으로 자신의 전자화폐를 상점에 지불하는 과정을 명세한 프로토콜이다.

- 예치 프로토콜 (deposit protocol)

상점과 은행 사이에서 수행되는 프로토콜로서 상점이 사용자로부터 받은 전자화폐를 은행이 결제해 주는 프로토콜이다.

상기에서 살펴본 바와 같이 전자화폐 시스템의 프로토콜은 시스템을 구성하는 구성원의 수와 시스템이 요구하는 기능에 따라 그 구성이 달라질 수 있다.

즉, 구성원이 증가하게 되면 당연히 프로토콜의 수도 증가하게 되며, 전자화폐 시스템에 어떤 기능을 추가하는 경우 그것을 위한 별도의 프로토콜이 반드시 필요하게 되는 것이다. [그림1]은 지금까지 살펴본 구성원과 프로토콜을 묘사한 것이다.



[그림 1] 전자화폐 프로토콜 구성도

2. 전자화폐 시스템의 기본적인 요구사항

전자화폐는 일반적으로 물리적 화폐와 비슷한 기능을 가지도록 설계하는 것이 기본 원칙이다. 그러나, 완벽하게 물리적 화폐와 같은 기능을 갖는 전자화폐 시스템을 구축하기는 상당히 어려운 일이다.

그것은 물리적 화폐의 다양한 기능성을 전자화폐가 수학적 방식으로 포용하기 어렵기 때문이다. 그럼에도 불구하고, 전자화폐가 필요한 이유는 물리적 화폐가 다음과 같은 문제점들을 가지고 있기 때문이다.

- 물리적 화폐의 제작, 유통, 관리 및 폐기에 수많은 인력과

자금이 소요.

- 컬러 복사기 및 프린터의 발달로 위조 화폐의 제작이 용이.
- 급속한 컴퓨터 네트워크의 발달에 따른 전자상거래 시대에 온라인 결제 수단으로서 사용하기 어려움 등.

결국, 상기 이유로 인해 전자화폐가 완벽하게 물리적 화폐의 특성을 갖지 않음에도 불구하고 개발되고 있는 것이다. 전자화폐 시스템에서 요구사항이라고 일컫는 것은 이러한 전자화폐의 기본적인 특징을 정의한 것이다. 전자화폐 시스템의 기본적인 요구사항은 일반적으로 다음과 같다.

- 안전성(security)

안전성의 정의는 여러 학자들에 의해 크게 두 가지로 대별되며, 본 논문에서는 다음과 같은 두 가지 관점으로 분류한다.

① 물리적 안전성 (physical security) : 물리적 안전성이란 전자화폐 자체에 대한 위조의 어려움을 의미하는 것으로서, 전자화폐가 쉽게 위조될 수 없어야 한다는 것을 의미한다.

일반적으로 전자화폐는 스마트 카드라는 물리적 보안장치에 저장되는 것을 원칙으로 하기 때문에, 결국 물리적 안전성이라는 것은 스마트 카드의 안전성으로 귀결된다.

② 논리적 안전성 (logical security) : 논리적 안전성이란 전자화폐 자체에 대한 위조 여부를 의미하는 것이 아니라, 전자화폐 시스템의 각 구성원은 나머지 다른 구성원들의 공모 공격(collusion attack)에 대해 안전해야 함을 의미하는 것이다.

상기에서 살펴본 바와 같이, 전자화폐 시스템의 안전성이라고 하는 것은 일반적으로 논리적 안전성을 의미하는 것으로 해석할 수 있을 것이다.

왜냐하면, 물리적 안전성이라고 하는 것은 전자화폐의 안전성이라고 하기보다는 스마트 카드 자체의 안전성을 의미하기 때문이다. 그러므로, 본 논문에서는 전자화폐 시스템의 안전성 요구사항을 논리적 안전성으로 해석할 것이다.

- 이중사용(double-spending)의 방지

전자화폐는 그 자체가 하나의 가치 있는 디지털 정보이다. 디지털 정보는 종이 문서와는 달리 복사본의 생성이 쉬우며, 더불어 그것의 원본 및 사본의 구별이 불가능하게 된다.

결국, 이중사용의 의미는 악의(惡意)의 사용자가 전자화폐를 불법 복제하여 무단으로 반복적으로 사용하는 것을 의미하는 것이며, 이것은 전자화폐 시스템 설계시 가장 중요하게 고려해야 될 부분인 것이다. 이중사용 문제에 대한 해결방법으로는 다음과 같은 두 가지 방법이 존재한다.

① 사후검출(after the fact) : CFN 시스템은 최초의 오프라인 전자화폐 시스템이다. 여기서 Chuam 등은 사후검출이라는 방식으로 이중사용의 문제를 해결하였다. 사후검출이란 은행이 사용자가 전자화폐를 발급 받을 때 전자화폐 내에 사용자의 ID 정보를 입력한 후, 사용자가 전자화폐를 이중 사용하는 경우 사후, 은행은 이것을 감지하여 전자화폐 내에 삽입되어 있는 사용자의 ID를 추출하여 이중사용자를 추적하는 방법을 의미한다.

물론, 은행은 정당한 사용자(전자화폐를 단지 한 번만 사용한 자)의 전자화폐로부터는 사용자 ID를 추출할 수 없게 된다.

사후검출 방식은 많은 오버헤드를 가지게 된다. 이중 사용자를 사후에 검출해야 하기 때문에 기존에 사용된 전자화폐들에 대한 데이터베이스를 유지시켜야 하며, 또한 범죄가 발생 이 후에만 해결 가능한 방식이 되기 때문에 이중사용 행위를 사전에 막을 수 없다는 문제가 발생하게 된다.

② 사전검출(before the fact) : CFN 시스템 이후 많은 전자화폐 시스템들이 소개되었으나 모두가 사후검출 방식에 의해 이중사용을 방지하는 방법을 취하였다.

그러나, Chaum 등은 처음으로 [8]에서 사전 검출 방법을 제안하였다. 기본적인 개념은 스마트 카드와 같은 TRM 을 이용하여 사용자가 전자화폐를 이중 사용하는 경우, 같은 정보가 반복적으로 이용되는 것을 감지함과 동시에 작동을 중지시키는 방법을 취하는 것이다.

이것은 사후검출 방식의 문제점을 해결함과 동시에 전자화폐 시스템의 실질적인 구현에 커다란 발판을 마련하는 계기가 되었다.

참 고

온라인 방식의 전자화폐 시스템은 기본적으로 사전검출이 된다. 즉, 예치 단계에서 은행이 개입하게 되므로, 상점이 전자화폐를 은행에 예치하는 경우 은행은 기존에 사용된 전자화폐의 저장 정보와의 동일 여 부를 비교하여 이중사용을 사전에 검출할 수 있는 것이다. 그러므로, 온라인 전자화폐 시스템은 전자화폐의 이중사용 문제가 쉽게 해결될 수 있다.

- 프라이버시 (privacy)

전자화폐 시스템이 지불 브로커 시스템과 가장 차별화 되는 점이 바로 사용자 프라이버시의 보장이다. 즉, 전자화폐는 실제 현금과 같이 사용자의 거래 내역이 추적되지 않는다.

이러한 사용자 거래의 불추적성을 일반적으로 사용자의 프라

이버시라고 일컫는다. 사용자 프라이버시의 보장은 전자화폐 시스템의 가장 큰 장점이 되며, 프라이버시 보장 강도에 따라 다음과 같이 두 가지로 나뉜다.[10][11]

① 불추적성(untraceability) : 은행과 상점이 어떠한 공모를 행하더라도 전자화폐를 지불한 사용자의 지불정보와 인출정보는 서로 연결될 수 없는 것을 의미한다. 즉, 은행은 상점과 공모하더라도 사용자의 지불 내역을 추적할 수 없게 된다(물론, 사용자가 단골고객인 경우 상점의 설명으로 은행이 지불자의 정보를 알 수는 있지만, 후에 이것을 증명할 수는 없기 때문에 거래 내역에 대한 정보로서 사용할 수가 없게 된다).

② 불연계성(unlinkability) : 은행과 상점이 공모하는 경우 은행은 비록 사용자의 거래내역을 추적할 수는 없지만, 두 가지의 지불이 같은 사용자에 의한 것임을 알 수 있는 경우가 있는데(이것은 전자화폐 시스템의 설계 스킴에 따라 존재하게 되는데, 대표적인 예로서는 전자면허를 사용하는 전자화폐 시스템[5]이 이러한 불연관성 조건을 만족하지 못하게 된다), 이러한 경우 연계성(linkability)이 있다고 일컬어진다.

이러한 연계성이 전자화폐 시스템이 존재할 경우 궁극적으로는 사용자의 불추적성이 보장되지 않을 수도 있게 된다. 그러므로, 전자화폐 시스템이 완벽하게 사용자의 프라이버시를 보장하기 위해서는 불연계성이 보장되어야만 한다.

	온라인(on-line) 방식	오프라인(off-line) 방식
방 식	전자화폐의 지불단계와 결제단계가 동시에 수행(지불 프로토콜과 예치 프로토콜이 실시간으로 수행)	수신된 전자화폐를 일괄 처리하여 은행에 결제를 요구하는 방식(지불 프로토콜이후 예치 프로토콜 수행)
장 점	지불단계와 결재단계가 거의 동시에 이루어지므로 이중사용을 지불단계 전에서 사전방지 가능(사전검출)	통신량 분산과 더불어 네트워크 인프라가 구축되지 않아도 사용 가능
단 점	통신량 집중화 현상과 통신량 증가에 따른 오버헤드 증가	이중사용이 이루어지고 난 이후 은행에서 이중사용자에 대한 신분 검출이 가능하므로 이중사용의 범죄 발생 가능
적용분야	고액거래로 높은 안전성을 요구하면서 운용비에 대한 부담이 크게 작용하지 않는 현금시장에 적합	많은 양의 소액거래가 이루어지는 곳으로 이중사용으로 인한 부정 가능 금액이 소규모인 거래에 적합
발달국가	미국 (통신망의 발달)	유럽 (스마트 카드의 발달)

[표1] 온라인 방식과 오프라인 방식의 비교

상기에서 살펴본 바와 같이 프라이버시는 그 강도에 따라 두 가지로 나뉘어지는데 일반적으로 ②의 조건을 만족하게 되면, ①의 조건은 당연히 만족되어지며, 보통 전자화폐 시스템의 프라이버시라고 언급되는 것은 대부분이 ②의 불연계성을 의미하는 것이다.

● 오프라인 (off-line)

전자화폐 시스템은 온라인 방식과 오프라인 방식으로 대별될 수 있다. 온라인 전자화폐 시스템은 사용자와 상점의 거래시 은행의 개입이 필요한 시스템으로서, 바꾸어 말하자면, 사용자가 상점에 전자화폐를 지불하는 경우 네트워크 상으로 은행의 개입이 있어야 한다는 것이다.

반대로 오프라인 전자화폐 시스템은 사용자와 상점의 거래시 은행의 개입이 필요치 않은 것이다. 일반적으로 전자화폐 시스템은 오프라인 방식을 채택하고 있는데, 이것은 물리적 화폐의 기본 성질에 따른 것이며, 더불어 컴퓨터 네트워크를 통해서 뿐만 아니라 일반 상점의 오프라인 단말기를 통해서도 거래가 가능토록 해주는 장점을 주기 때문이다. 다음 [표1]은 온라인 방식과 오프라인 방식을 비교 설명한 것이다.

3. 전자화폐 시스템의 부가적인 요구사항

전자화폐 시스템의 요구사항을 명확히 정의하는 것은 학자들마다 다를 수 있다. 본 논문에서는 2.2절에서 살펴본 바와 같이 전자화폐의 요구사항을 기본적인 것과 부가적인 것으로 나누고 있다.

일반적으로 안전성, 이중사용의 방지, 프라이버시는 전자화폐 시스템이 갖추어야 기본적인 요구사항이 되며, 이러한 전자화폐 시스템은 온라인 방식이 될 수도 있으며, 오프라인 방식으로 될 수도 있다. 그러나, 근래에는 일반적으로 오프라인 방식을 기본으로 취하고 있는 추세이다.

전자화폐는 글자 그대로 실제 화폐와 비슷한 성질을 갖는 가치있는 디지털 정보이다. 그러므로, 상기에서 언급한 기본 요구사항만을 가지고서는 전자화폐를 일반 화폐처럼 사용하기가 어렵다. 예를 들어 다음과 같은 경우를 생각해 보자.

사용자가 실제로 전자화폐를 발급받아 그것을 상점에서 사용한다고 가정하자. 이 경우 만약 상품구입 금액이 지불하는 전자화폐의 금액보다 작게 된다면, 사용자는 상점으로부터 잔액을 거슬

러 받아야 된다.

그러나, 이러한 사소한 사실 한 가지가 실제로는 여러 가지 문제점들을 불러 일으킬 수 있는 요소가 된다.

첫째로 이 거래가 원격지 간의 전자상거래라면, 사용자는 상점으로부터 실제 화폐로는 잔액을 받을 수 없게 된다. 그러므로, 상점은 잔액에 해당하는 만큼의 소액 규모의 전자화폐를 미리 가지고 있어야 하며, 이것은 시스템 저장 공간의 오버헤드가 된다.

둘째로 상점이 그러한 소액 규모의 전자화폐를 가지고 있다고 하더라도, 만약 이것을 사용자에게 잔액으로 지불하게 된다면, 사용자는 받은 잔액을 다른 상점에서 사용할 수 없게 된다.

즉, 사용자가 이것을 다른 상점에 쓰게 되면, 이중사용 문제가 발생했을 경우 이것이 상점에 의한 것인지 또는 사용자에 의한 것인지를 구별할 수 없게 되므로 사용자는 상점으로부터 받은 전자화폐를 반드시 은행에 예치해야만 한다는 것이다. 결국, 사소한 잔액의 문제는 전자화폐를 사용하기 불편하게 만드는 주원인이 된다.

상기에서 살펴본 바와 같이 전자화폐를 실제 화폐와 같이 사용하기 위해서는 기본적인 요구사항 이외에도 다음과 같은 몇 가지 부가적인 요구사항이 있어야 한다.

● 전자수표(electronic check)

최초의 오프라인 전자화폐 시스템인 CFN시스템[4]은 상기에서 언급한 잔액의 문제점을 해결코자 전자수표라는 방식을 제안하였다. 이것은 사용자가 전자화폐를 발급 받는 경우, 금액이 큰 전자화폐를 발급 받은 후 사용할 때에는 자신이 지불할 금액만큼만을 지불할 수 있는 형태이다.

이것은 잔액 처리의 문제를 해결해 줄 수 있으며, 더불어 상점에서 잔액을 위한 전자화폐를 별도로 마련치 않아도 된다는 장점이 있다. 그러나, 이것은 인출 · 지불 · 예치 프로토콜 외에 또 다른 프로토콜을 필요로 하게 된다는 단점이 있다.

즉, 사용자는 발급 받은 전자수표를 사용한 후 발급 금액에서 지불 금액을 뺀 나머지 금액을 은행으로부터 상환 받기 위해서 상환 프로토콜(refund protocol)을 수행해야만 한다.

● 분할성(divisibility)

분할성은 전자수표와 비슷한 개념으로서, 사용자가 전자화폐를 발급 받는 경우 발급 받은 전자화폐를 사용자 마음대로 나누어 사용할 수 있는 성질이다.

즉, 인출 받을 당시의 금액을 기준으로 사용한 총액이 지정된 금액을 넘지 않을 때까지 사용자가 나누어 사용할 수 있음을 말하는 것이다. 이것은 전자수표와는 달리 한 번 발급 받은 전자화폐를 여러 번 나누어 사용할 수 있으며, 또한 전자수표가 가지고 있던 상환 프로토콜(refund protocol)이 필요 없다는 장점을 갖는다.

그러나, 이것은 완벽한 프라이버시 보장이 안된다는 단점을 가지게 된다. 즉, 불추적성은 만족하나, 불연계성은 만족되지 않는다는 것이며, 결국 분할성은 완벽한 프라이버시가 보장되지 않는다는 문제점을 가지고 있다.

● n회 사용가능성(n-spendability)

이것은 분할성의 개념과 비슷하지만본질적으로는 큰 차이가 있다. 분할성은 사용자가 발행받은 전자화폐 금액내에서 사용자가 지불하기 원하는 금액만큼 사용금액에 맞추어 지불할 수 있는 기능이다.

반면에 n회 사용가능성은 금액을 나누어 사용한다는 개념보다는 지하철 정기권과 같이 동일한 금액을 횟수 기준으로 n번 까지 사용한다는 개념이다.

즉, n회 사용가능성은 어느 일정한 금액을 일정 횟수만큼만 사용가능케 하는 것이다. 그러나, 이 기능도 분할성과 같이 불연계성을 만족시키지 못한다는 문제점이 생긴다.

● 양도성(transferability)

실제 화폐의 성질들 중 가장 특기할 만한 것은 쉽게 양도 가능하다는 것이다. 즉, 발행기관으로부터 만들어진 화폐는 그것의 수명이 다할 때까지 계속해서 사회에 유통된다.

그러나, 기본적인 요구 사항만을 만족하는 전자화폐는 그러한 양도 기능이 없으며, 이것은 전자화폐가 실제 화폐를 대치하지 못하고 있는 이유중의 하나가 된다. 이러한 문제점을 해결하고자, T. Okamoto 등은 [19]에서 양도성 기능을 갖는 전자화폐 시스템을 제안하였다. 그러나, 양도성 성질에는 두 가지 문제점이 존재하게 된다.

첫 번째는 사용자의 프라이버시가 보장되기 어렵다는 것이다. 즉, 양도 가능한 전자화폐가 이중 사용되었다고 가정할 경우, 은행은 이중사용자를 추적하기 위해서는 반드시 중간 양도자들에 대한 조사를 해야만 한다. 이 과정에서 부득이하게 이중사용된 양도 가능한 전자화폐의 사용자들은 그들의 신분을 노출시킬 수 밖에 없는 것이다.

두 번째 문제는 양도 가능한 전자화폐는 양도횟수가 증가할 수록 그것의 크기가 증가한다는 것이며, 이것은 [6]에서 증명되었다.

4. 전자화폐 시스템의 기반기술

은닉서명 프로토콜

전자화폐는 은행이 가치를 보증해주는 일종의 가치 있는 디지털 정보이다. 이러한 전자화폐의 가치를 증명해주기 위해서 은행이 이용할 수 있는 방법은 디지털 서명을 사용하는 것이다. 그러나, 일반적인 디지털 서명을 사용하게 되면 사용자 프라이버시가 보장되지 않는다는 문제점이 발생하게 된다.

즉, 은행은 사용자가 서명 받기 원하는 메시지와 그에 대한 서명문을 알게 되기 때문에, 전자화폐 발급 후 은행은 그것들을 서로 연결시킬 수 있게 되는 것이다.

그러므로, 전자화폐를 발급하기 위해서는 일반적인 디지털 서명이 아닌 새로운 종류의 특수한 디지털 서명이 필요하게 되며, 이것은 전자화폐 시스템을 구성하는 프로토콜 중 인출 프로토콜을 설계하는데 기반이 된다.

D. Chuam은 1982년 [3]에서 상기의 요구사항을 만족하는 특수한 디지털 서명 프로토콜인 은닉서명(blind signature) 프로토콜을 제안하였다. 은닉서명 프로토콜은 서명자(signer)가 제공자(provider)의 메시지를 볼 수 없는 상태에서 그것에 대한 서명을 해주며, 제공자에게는 자신이 원하는 메시지에 서명을 받을 수 있게 해주는 역할을 수행한다.

구체적인 은닉서명 프로토콜의 내용은 [그림2]와 같으며, 여기서 사용되는 함수 및 프로토콜 절차는 아래와 같다.

● 함수(function)

- s'는 서명자만이 알고있는 서명함수이며, 그것에 대한 역함수인 s는 s(s'(x))=x와 같이 검증함수로 사용되는 공개되어 있는 정보이다. 그러나, s는 s'에 대한 어떠한 정보도 제공하지 않는다.

- 가환함수 c와 그것의 역인 c'는 제공자에만 알려져 있는 함수이며, c'(s'(c(x)))=s'(x)와 같은 역할을 수행하며, 여기서 c(x)와 s'는 x에 대한 어떠한 정보도 제공하지 않는다.

- r은 유효한 서명들을 찾는 것이 불가능하게 하도록 충분한 리던던시(redundancy)를 확인해 주는 리던던시 확인 함수(predicate)이다.

● 프로토콜(protocol)

- 1단계. 제공자는 랜덤하게 r(x)인 x를 선택한 후, c(x)를 생성하고나서 이것을 서명자에게 전송한다.

- 2단계. 서명자는 s'를 이용하여 c(x)에 서명을 행한 후, 그 결과 s'(c(x))를 제공자에게 전송한다.

- 3단계.) 제공자는 c' 함수를 이용하여 c'(s'(c(x)))=s'(x)와 같이 s'(c(x))에서 s'(x)만을 추출한다.

- 4단계. 제3자는 서명자의 검증함수 s를 이용하여 r(s(s'(x)))을 확인함으로서 s'(x)가 서명자에 의해 서명된 것임을 확인할 수 있다.

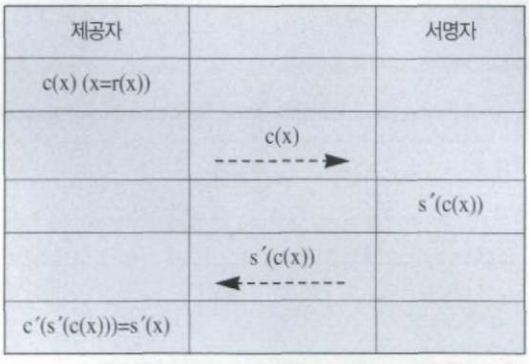
상기에서 살펴본 은닉서명 프로토콜은 다음 세 가지의 안전성 성질들을 갖는다.

① 디지털 서명 : 누구나가 추출된 서명 s'(x)는 서명자의 비밀키 s'를 사용한 것이라는 사실을 확인할 수 있다.

② 은닉 서명 : 서명자는 s'(xi)와 같은 추출된 서명들의 집합과 s'(c(xi)) 와 같이 추출되기 전의 서명들의 집합 사이에서 서로 대응되는 쌍들을 찾을 수 없다.

③ 서명들의 보호 : 제공자는 서명자에 의해 서명된 각각의 것들에 대해 기껏해야 하나의 서명만을 추출할 수 있다(즉, 제공자가 s'(c(x1)),... ,s'(c(xi))와 같이 추출된 서명들의 집합과 이에 대한 c,c',x를 가지고 있다 하더라도, r(y)를 만족하며 y=xi가 아닌 새로운 수 y에 대한 서명 s'(y)를 구하는 것은 불가능하다).

D.Chuam은 [3]에서 상기에서 설명한 은닉서명 프로토콜의 개념을 처음 제안하였지만, 그것의 구체적 구현은 보이지 못하였다. 그러나, [3]에서 발표된 은닉서명 프로토콜의 개념은 전자화폐 시스템의 인출 프로토콜에서 사용자의 프라이버시를 보장해주는 프리미티브(primitive)로 작용하는 중요한 역할을 담당하게 되었다.



[그림2] 은닉서명 프로토콜

cut-and-choose 기술과 challenge-and -response 기술

D.Chuam에 의해 은닉서명 프로토콜이 제안된 이후 사용자의 프라이버시를 만족하는 최초의 오프라인 전자화폐 시스템이 D.Chuam, A.Fiat, M.Naor에 의해 1988년 CRYPTO에 발표되

었다 [4].

불추적성을 만족하는 오프라인 전자화폐 시스템을 설계하는 경우 가장 어려운 것은 이중사용을 검출할 수 있는 정보를 전자화폐에 넣는 방법이다.

만약 이러한 정보를 은행측에서 넣도록 한다면, 은행이 부정행위를 하는 경우 그 정보를 이용하여 사용자의 프라이버시를 침해할 수 있으며, 반대로 그 정보를 사용자측에서 넣도록 한다면, 은행측에서는 은닉서명의 특성상 사용자의 메시지를 볼 수 없기 때문에 사용자의 부정행위를 막을 수 없게 된다.

이러한 문제를 Chuam등은 [4]에서 cut-and-choose 기술로 해결하였다. Cut-and-choose 기술이란 전송된 정보의 정확성을 확인하기 위해 같은 방법을 사용한 여러 정보들 중 일부의 내용 구성을 확인한 후, 그것의 확률로서 나머지 정보에 대한 정확성을 규정하고 그 정보들을 처리 대상으로 사용하는 것이다.

즉, [4]의 인출 프로토콜에서는 사용자가 랜덤정보와 자신의 식별자를 넣은 전자화폐를 K개 생성한 후, 그것들을 은행에 전송하게 되며, 은행측에서는 그것들 중 K/2개를 선택하여 사용자의 도움을 받아 선택된 정보들의 정확성을 검증한다.

그리고 나서, 선택되지 않은 나머지 K/2개의 정보들은 하나의 전자화폐로서 사용된다. 이 때, 생성된 전자화폐의 정확성은 1-(1/(2(K/2)))이 된다.

그러나, 상기와 같은 cut-and-choose 기술을 사용하는 전자화폐 시스템은 많은 오버헤드를 가지게 된다. 즉, 그러한 전자화폐 시스템은 인출 프로토콜이나 지불 프로토콜을 수행하는 경우 많은 통신량을 요하게 되며, 더욱이 각각의 전자화폐가 차지하는 메모리 용량은 상당히 크다는 문제점을 가지게 된다.

결국, 이러한 문제점들은 전자화폐 시스템을 실제로 구현하는 경우 아주 큰 장애요소로 작용하게 되었다.

1993년, S.Brands와 N.Ferguson은 각기 [10]과 [11]에서 challenge-and -response 기술을 사용한 전자화폐 시스템을 제안하였다. challenge-and -response 기술은 cut-and-choose 기술의 문제점을 완전히 해결한 기반 기술로서, 두 시스템 모두 Shamir가 [12]에서 제안한 비밀 공유 직선(secret sharing line)의 개념을 이용하였다.

전자화폐 시스템의 인출 프로토콜에서 cut-and-choose 기술이 사용된 이유는 이중 사용자의 식별자 검출을 위한 사용자의 식별자 정보를 사용자 자신이 메시지 내에 삽입하는 데에서 기인하는 것이다.

즉, 이러한 사용자의 메시지 구성을 은행측에서는 믿을 수 없기 때문에 그것의 정확성을 확인할 수 있는 방법으로서 오버헤드가 큰 cut-and-choose 기술을 사용한 것이다.

그러나, [10],[11]에서는 사용자의 식별자 정보를 은행측에서 넣는 방식을 취하는 새로운 은닉서명 프로토콜을 사용함으로써 challenge-and-response 기술을 사용가능케 하였다. Challenge-and-response 기술은 일반적으로 개인식별에서 많이 사용되는 형태로서 사용자측은 먼저 commitment를 보내고, 이후 은행측은 challenge를 전송하며, 마지막으로 사용자측이 기존에 보냈던 commit- ment와 challenge에 일관성을 갖는 response를 보내는 방식이다.

chall- enge-and-response 기술을 cut-and-choose 기술과 비교해보면 많은 차이가 있음을 쉽게 알 수 있다. 우선, 검증할 메시지를 M이라고 가정하였을 경우 전송되는 통신량을 비교해보면, challenge-and-response 기술은 [commitment의 크기+challenge의 크기+response의 크기] 만큼의 통신량이 필요한 반면, cut-and-choose 기술은 (1-1/(2K/2))의 정확성을 갖기 위해서 기본적으로 [(K*M)+((K/2)* M)+((K/2)*M)] 만큼의 통신량을 요하게 된다.

또한, cut-and-choose 방법에서의 안전성 파라메터는 K이기 때문에 보다 높은 안전성을 보장하기 위해서는 K에 비례하여 통신량이 증가하게 되는 반면, challenge-and-response 기술에서는 일반적으로 chall- enge가 안전성 파라메터 역할을 수행하기 때문에 전체적인 통신량의 증가 없이 단지 challenge의 길이만 증가시킴으로써 안전성을 높일 수 있다.

상기에서 살펴본 바와 같이 1993년 이후에는 전자화폐 시스템 설계 시 challenge-and-response 기술을 사용하게 되었으며, 이것은 전자화폐 시스템의 효율성을 개선시키는 기폭제가 되었다.

■ 참고문헌

[1] W. Diffie and M. Hellman, "New Directions in cryptography", IEEE Transaction on Information Theory, Vol.22, No.6. pp.644-654, November 1976

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", Communications of the Association for Computing Machinery, Vol.21, No.2, pp.120-126, 1978.

[3] D. Chaum, "Blind Signatures for Untraceable Payments", Proc. of CRYPTO'82, Plenum Press, pp.199-203, 1983.

[4] D. Chuam, A. Fiat and M. Naor, "Untraceable Electronic Cash", Advances in Cryptology, Proc. of CRYPTO'88, pp.319-327, 1988.

[5] T. Okamoto and K. Ohta, "Universal Electronic Cash", Advanc- es in Cryptology, Proc. of CRYPTO'91, pp.324-337, 1991.

[6] D. Chuam and T.P. Pedersen, "Transferred Cash Grows in Size", Advances in Cryptology, Proc. of EUROCRYPT'92, pp.390-407, 1992.

[7] T. Eng and T. Okamoto, "Single-Term Divisible Electronic Coins", Advances in Cryptology, Proc. of CRYPTO'94, pp.108- 117, 1994.

[8] D. Chuam and T.P. Pedersen, "Wallet Databases with Observers", Advances in Cryptology, Proc. of CRYPTO'92, pp. 89-105, 1992.

[9] R.J.F Cramer and T.P. Pedersen, "Improved Privacy in Wallets with Observers", Advances in Cryptology, Proc. of EUROCRYPT' 93, pp.329-343, 1993.

[10] S. Brands, "Untraceable Off-line Cash in Wallet with Observ- ers", Advances in Cryptology, Proc. of CRYPTO'93, pp.302- 317, 1993.

[11] N. Ferguson, "Single Term Off-line Coins", Advances in Crypto- logy, Proc. of EUROCRYPT'93, pp.318-328, 1993.

[12] A. Shamir, "How to Share a Secret", Communications of the As- sociation for Computing Machinery, Vol.22, No.11, pp.612-613, 1979.

[13] S. Brands, "Restrictive Binding of Secret-Key Certificates", Advances in Cryptology, Proc. of EUROCRYPT'95, pp.231 - 247, 1995.

[14] S.von Soloms and D. Naccache, "On Blind Signatures and Pe- rfect Crimes", Computer & Security, Vol.11, pp.581-583, 1992.

[15] E. Brickell, P. Gemmell, and D. Kravitz, "Trustee-based Tracing Extensions to anonymous Cash and the Making of Anonymous change", Proc. 6th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), pp.457-466, 1995.

[16] David Pointcheval and Jacques Stern, "Provably Secure Blind Signature Schemes", Advances in Cryptology, Proc. of ASIA- CRYPT'96, pp.253-265, 1996.

[17] David M'Raihi, "Cost-Effective Payment Schemes with Privacy Regulation", Advances in Cryptology, Proc. of ASIACRYPT'96, pp.266-275, 1996.

[18] Masayuki Abe and Eiichiro Fujisaki, "How to Date Blind Signatures", Advances in Cryptology, Proc. of ASIACRYPT'96, pp.243-251, 1996.

[19] T. Okamoto and K. Ohta, "Disposable Zero-Knowledge Authenti- cations and Their Applications to Untraceable Electronic Cash", Advances in Cryptology, Proc. of CRYPTO' 89, pp.449-460, 1993.

[20] N. Ferguson, "Extensions of Single term coins", Advances in Cr- yptology, Proc. of CRYPTO'93, pp.292-301, 1993.