네트워크 상에서의 안전한 전자복권 시스템 구현

이덕규, 박희운, 이임영
순천향대학교 정보기술공학부*

A Application of Secure Electronic Lottery Ticket System on Network

Duk-Kyu Lee, Hee-Un Park, Im-Yeong Lee
Division of Information Technology Engineering, SoonChunHyang University*

요 약

정보화 사회가 발전되고 전자 상거래가 새로운 상거래 시스템으로 부각되면서 전자 상거래에 전자 복권에 대한 수요의 증가와 함께 연구가 활발히 진행되고 있다. 이 중 전자 복권 시스템은 인터넷과 같이 개방된 네트워크 환경 하에서 사용하기 위한 목표로 기존의 복권을 대신하여 사용될 것이다. 복권번호 중복문제, 사용자· 사업자간의 결탁문제 등 여러 가지의 문제점이 지적되고 있다. 본 고에서는 기존의 전자복권 시스템에 대한 고찰과 그에 상응하는 요구사항을 살펴본 뒤 실제로 제안된 기법을 검토하여 안전한 프로토콜에 대해 설명한다.

1. 서론

정보 통신 기술의 발달은 기업의 경영 환경과 개인의 생활에 큰 변화를 가져왔으며, 이제는 기업은 물론 개인에게도 필수적인 생활 도구가 되었다. 이와 같은 정보통신기술의 발달은 온라인 컴퓨터 통신 서비스와 인터넷이라는 개방형 네트워크의 발달, 그리고 월드와이드웹(WWW : World Wide Web)이라는 그래픽을 이용한 쉽고 편리한 인터넷 사용자 인터페이스의 탄생으로 전자상거래 참여자들의 급증이라는 결과를 낳았고 이와 함께 전자상거래는 현실로 다가오고 있다.[9][10]

이와 같이 인터넷과 전자상거래의 발전은 우리들의 삶에 많은 이로움과 편리함을 가져온 반면 많은 문제점을 수반하고 있다. 해킹, 바이러스, 위조, 변조, 부인봉쇄 등이 그 좋은 예라 할 수 있다. 그러나 이러한 문제점은 암호학의 발전으로 인하여 해결할 수 있는 방안들을 모색할 수 있게 되었으며 본 논문 또한 으용분야 중의 하나인 복권 사이트를 그 예로 하여 이러한 네트워크상의 문제점과 보안문제를 해결할 수 있는 방안을 제시하고자 한다.

본 논문에서는 복권의 기본적인 개요 및 요구사항과 기존의 전자복권 시스템에 대한 고찰, 네트워크 상에서의 안전한 새로운 방식을 설명하고 있다. 또한 기존의 전자복권 시스템과 새로운 방식을 비교 분석하여 서로 어떠한 장단점을 가지고 있는지를 분석하였다.

2. 복권의 기본적 개념

복권에 대한 정보는 시대를 걸쳐 다양하게 정의되게 되는데, 그 중 대표적인 것으로 "제비를 뽑아서 맞는 표에 대해 많은 배당을 주는 표찰"이 있으며, 모든 불법적인 요소를 배제시키고 국가적 사업으로 시행되는 현대의 복권은 적은 비용으로 당첨에 대한 기대와 재미를 함께 보장하는 생활속의 건전한 국민오락이다. 현재 100여 개국에서 복권을 발행하고 있으며, 복권발행의 수익금은 국가의 중대한 사업 전개, 필요기간산업 지원, 의료, 복지, 교육, 지방재정 지원 등 국가가 국민들의 궁극적인 생활 향상을 위한 사업을 수행하는데 쓰여지고 있다.

현재는 사이버 상에서 판매되는 복권이 늘어가고 있으며 이 중에서 많은 수가 무료로 복권을 제공하고 있다. 일부는 온라인 결제를 이용한 실물 복권 구입과 컨텐츠 사업의 일부로서 무료로 복권을 제공하고 그 수익은 컨텐츠 이용에 두고 있다.

일반적인 복권 사이트들을 탐색하고 살펴보면 다양한 형태의 운영방식들이 있다. 복권의 종류에는 크게 네가지로 나누어 볼 수 있다. 추첨식 복권(Draw Game), 즉석 복권(Instant Game), 로토(Lotto) 및 숫자 게임(Numbers Game)이 그것이다.

추첨식 복권은 판매 종료일 이후 추첨하여 추첨된 번호와 구입한 복권 번호가 일치되면 지급하는 것이고, 즉석 복권은 스크래치(Scratch-Off) 복권이라고도 하는데 즉석에서 긁음으로써 알 수 있기 때문이다. 로토는 5개 또는 6개 조합을 맞추는 게임으로 온라인 복권이며, 숫자게임은 3 또는 4개 자리 번호를 선택하여 맞추는 게임으로 숫자 배열 순서까지 일치해야 되는 순열(straight)과 순서에 관계없는 조합(Box)의 두 종류의 게임 방법이다.[11]

본 연구는 실물 복권과 같은 방식을 채택하여 당첨 번호를 마지막에 산출하는 방식을 채택하고 있다. 본 연구의 장점은 일반적으로 발생할 수 있는 문제점을 사전에 방지하고자 하였다. 그리하여 사고자하는 복권의 네트워크 상에서의 안전한 방법으로 복권을 구입하는 방법을 추구하였다.

3. 기존의 전자 복권 시스템에 대한 고찰

이 장에서는 기존의 시스템에서의 구성요소를 살펴보며

그에 따른 결탁의 문제에 대해 고찰한다.

3.1 기존 시스템의 분석[4]

3.1.1 구성 요소

· 사업자

사업자는 사용자의 디지털 서명을 확인하는 것으로 발매 및 당첨을 확정지으며, 해쉬를 통해 복권 번호를 비교한다. 고찰하고자 하는 이전 버전에서의 서버는 사업자와 같다는 개념을 사용하고 있는데 고찰방식에서의 서버는 단지 사업자가 해쉬되기 전의 값을 만들면 그 값을 이용하여 해쉬 값을 산출한다.

· 사용자

사용자는 서명을 통하여 간단한 신상명세서를 작성하여 사업자에게 보내고 사업자가 보낸 해쉬값을 보고 사업자의 서명을 확인한다. 당첨번호 4자리를 선택하고 서명을 수행한 뒤 사업자에게 보낸다.

· 사용하고 있는 암호화 방식

RSA 공개키 암호화 방식을 사용하고 있다.

- 서로 발송하는 것에 대한 확인이며, 이것은 부인봉쇄를 한다.
- HASH FUNCTION(해쉬 함수)은 당첨번호를 위하여 전송

3.1.2 운영방식의 구조

· 시스템 계수

Rn : 20자리의 숫자로 구성된 해쉬되기 전의 값
EKR : 사업자의 비밀키로 암호화수행
ANS : 사용자가 작성한 4자리의 일련번호
ID : 사용자가 초기에 사업자에게 등록해 놓은 값

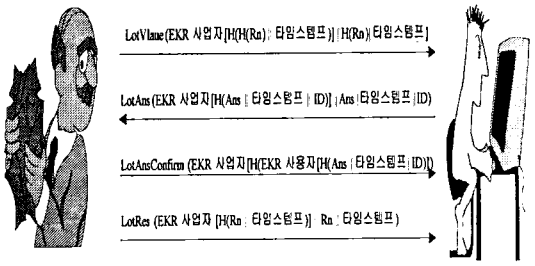

그림 1. 기존방식의 프로토콜

· 중복성의 문제(복권구입문제)

이 논문에서는 해쉬되기 전의 값을 당첨번호로 사용을 하고 있다. 즉, 20자리의 십진수 숫자 중 4자리가 당첨번호가 되는데 이는 104개의 복권을 의미한다. 이것은 고객이 같은 번호를 보내어 중복되는 복권이 많아진다는 것을 의미한다

· 서버와 사용자의 결탁문제

미리 번호를 공개하여 사용자와 서버가 결탁을 결탁하여 사용자을 당첨자로 만들 경우를 말하는 것이다.

· 서버와 사업자간의 결탁문제

서버와 사업자가 결탁을 하여 당첨금이나 다른 특정한 목적으로 가지고 당첨자를 일부러 안 만드는 경우를 말한다.

· 서버, 사업자 그리고 사용자의 결탁문제

서버, 사업자 그리고 사용자가 결탁을 하여 특정한 사용자를 당첨자로 뽑아 당첨금을 탈수 있게 하는 경우를 말한다.

4. 새로운 방식 제안

본 방식에서는 전자 복권에 대한 발매에 대한 언급을 하고 있으며 은행에 관한 내용은 제외하였다.

4.1 네트워크 상에서의 안전한 구현을 위한 조건

4.1.1 구성 요소

· CA(인증기관)

사업자로부터의 복권 번호 일부와 CA 자신의 복권 번호 일부를 Random하게 생성하여 올리는 일을 맡고 있다.

· 사업자

단지 복권 발행을 목적으로 운영되는 기관을 말한다. 고객이 접속하여 회원 가입 시 ID와 비밀번호를 발급한다. 사용자가 복권을 구입하면 사용자에게 어떤 복권을 구입 확인서를 보내주고, 사용자가 복권을 LIST를 만들어 보관한다. 보관하는 값에는 ID, Time Stamp, (사용자의 공개키로)암호화된 복권번호, 사용자의 공개키를 보관한다.

사업자는 후에 공개보드에 CA와 만들어낸 1/2의 복권번호를 동시에 올리고 사용자들에게 알린다.

· 사용자

다른 사용자가 먼저 구입한 복권은 구입할 수 없으며 미판매된 복권은 여러 장을 구입할 수 있다.

사용자는 자신의 복권번호 구입시 생성되는 공개키를 이용하여 복권번호를 암호화하여 전송한다. 사업자는 올바른 정보를 받았다는 응답을 한다. 사용자는 이 응답을 받아 사업자의 서명을 확인한 후 자신의 저장공간에 저장한다.

당첨확인은 공개보드를 통하여 볼 수 있으며 당첨자일 경우 사용자가 보내는 당첨자 확인서에 의해서 확인할 수 있으며 불확실한 경우 자신의 개인키로 암호화된 자신의 복권번호를 복호화 함으로써 자신의 당첨여부를 알 수 있다.

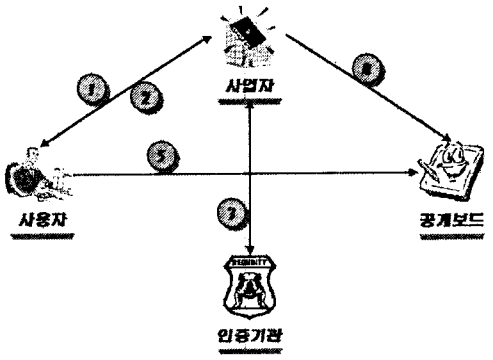

그림2. 새로운 제안방식 전체 흐름도

4.1.2 시스템 계수

다음의 계수는 복권의 구매 혹은 당첨 프로토콜에서 사용되는 계수들이다.

Uid : 사용자의 ID
B_N : 복권 번호
TS : Time Stamp
EKR : 사용자 혹은 사업자의 비밀키로 암호화 수행
H : 해쉬함수

4.1.3 사전 준비 단계

본 고에서는 은행의 구현은 현재 배제하였다. 은행의 기능은 지금까지 구현된 전자 은행을 근거로 한다.

Step 1. 사업자는 ID 발급을 위해 신상명세서를 사용자에게 보낸다.

Step 2. 사용자는 사업자가 발급한 신상 명세서를 사용자에게 보낸다.

Step 3. 사업자는 ID와 같이 사용자에게 확인서를 보낸다.(회원 가입 확인서)

Step 4. 사용자는 복권구입을 위하여 은행에 사업자와 연결된 계좌를 만들며 원하는 만큼의 화폐를 구입한다.(단 계좌는 자동으로 사업자, 은행, 사용자의 거래가 은행에 의하여 이루어진다.)

Step 5. 은행은 사용자에게 화폐를 구입하였음을 증명하는 증명서를 발급한다.

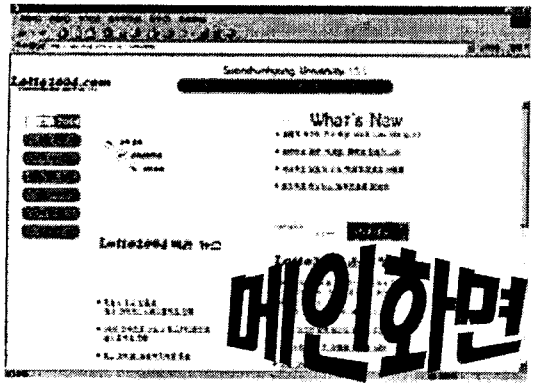

그림 3. 복권 사이트 메인화면

4.1.4 구입 단계

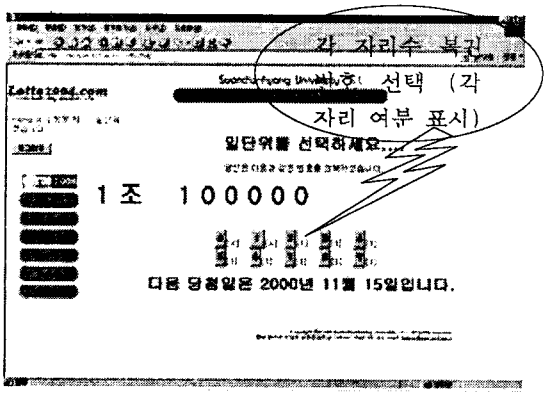

그림 4. 복권번호 선택

Step 1. 복권 신청 - 다른 사용자가 먼저 구입한 복권은 구입할 수 없으며 구입되지 않은 복권은 원하는 만큼 구입할 수 있다

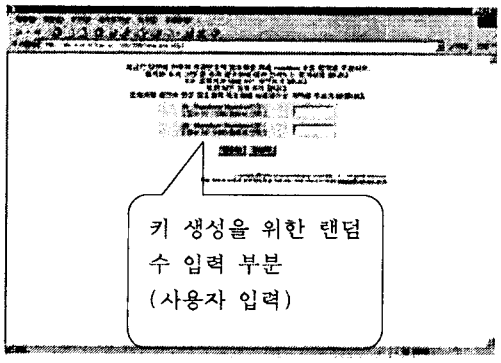

그림 5. 공개키·개인키 생성을 위한 랜덤 수 선택

Step 2. 복권 발급 - 사업자는 사용자가 구입한 복권을 Time Stamp와 ID 등을 사용자의 공개키로 암호화한 후 사업자의 서명과 같이 사용자에게 보낸다.

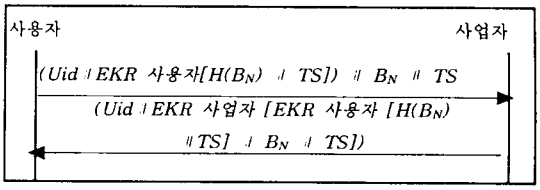

그림 5. 복권 구입 프로토콜

Step 3. 사업자는 은행에게 판매된 복권 금액을 요청
Step 4. 은행은 사용자가 산 복권에 대한 화폐를 지불
Step 5. 은행은 사용자에게 지불한 것에 대한 통보

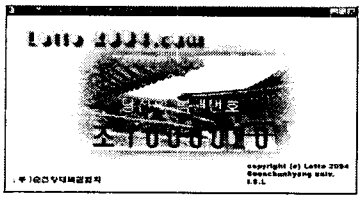

그림 6. 사업자가 전송하는 복권 화면

4.1.5 당첨·발표단계

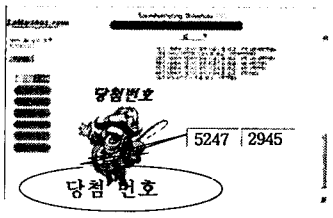

그림 7. 당첨자 추첨 사용자 확인 후 모습

Step 1. 지정한 날(일주일 혹은 1달)이 되면 사업자와 인증기관은 번호를 생성한다.

▶ 사업자와 인증기관은 4자리씩 생성하되 순서는 없다.
▶ 사업자는 Random Generator를 이용하여 4자리의 수를 만든다.
▶ 인증기관도 Random Generator를 이용하여 4자리의 수를 만든다.
▶ 사업자와 인증기관은 생성한 번호를 서로 교환한다.

Step 2. 사업자는 사용자에게 당첨자로 뽑혔음을 통보한다.

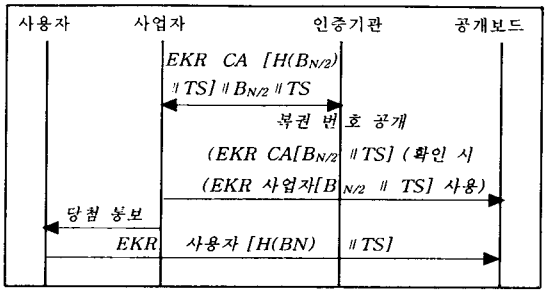

그림 8 복권 당첨 프로토콜

Step 3. 당첨자나 모든 사용자는 공개 보드를 이용하여 확인한다.
Step 4. 사업자는 은행에게 당첨금을 지급한다.
Step 5. 은행은 당첨자의 계좌의 당첨자가 원하는 유형으로 금액을 지불한다.

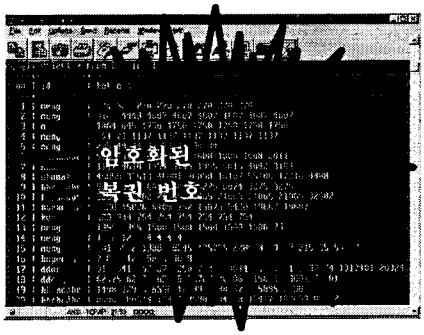

그림 9. 사업자 DB에 저장되는 암호화된 복권번호

5. 각 제안 방식별 비교·분석

5.1 제안 방식의 분석

새로운 제안 방식에서의 가장 큰 장점으로 말할 수 있는 것은 다른 복권사이트의 운영방식과는 다르게 당첨번호를 복권이 발매된 후 맨 마지막에 추첨을 한다는 것이다. 이렇게 함으로써 우리가 일상생활에서 사고 파는 복권의 재미를 한층 더 증가시키고 있다. 그리고 안전성에 관한 장점 또한 제안방식의 장점 중 하나라고 말할 수 있다.

회원가입으로 복권구입에서 추첨단계까지 일사천리로 이루어진다. 다른 타 사이트에서 볼 수 없었던 편안함이다. 우리는 안전성이 뛰어난 사이트여야만이 사용자들이 신뢰성을 가지고 이용할 수 있을 것이라는 것에 초점을 뒀다. 예를 들면 이러한 안전성을 한층 더 증가시키기 위하여 금전적인 면의 모든 것을 은행이 맡아 하도록 구현하였다.

5.2 기존의 방식과 제안방식의 비교

기존방식과 새로운 제안 방식에는 많은 차이점이 있다. 복권판매의 호기심과 재미로 보았을 경우 일반적으로 사람들이 사는 복권은 당첨번호가 복권발매가 끝난 후 공개적인 방법을 통하여 추첨을 한다. 복권 번호는 사용자가 다시 한 번 확인을 하게끔 하였다. 이렇게 함으로써 복권의 호기심과 재미를 더하는 것인데 기존의 방식에서는 당첨번호가 처음에 나와있는 상태에서 이를 맞추는 방식이므로 사용자들이 이용하였을 경우 원래 복권방식에서 많이 벗어나고 있다. 그러므로 복권의 원초적인 호기심과 재미가 떨어지기 마련인데 새로운 제안방식에서는 당첨번호를 일반적인 복권과 마찬가지로 마지막에 추첨하고 있다.

다음으로는 안전성에서의 차이점을 찾아 볼 수 있는데 기존의 방식에서는 안전성에 많은 문제점을 가지고 있다. 예를 들어 앞에서 언급한 문제를 다시 되짚어 보도록 하겠다.

- **서버와 사용자의 결탁문제**에 있어서는 서버가 복권번호를 1/2만 생성하기 때문에 이러한 문제를 방지할 수 있다. *(EKR CA[$B_{N/2}$ / TS]*
- **사용자와 사업자의 결탁문제**는 서버와 사용자간의 결탁과 같은 문제로 해결될 수 있다. *(EKR 사업자 [$B_{N/2}$ / TS]*
- **서버와 사업자의 결탁문제**는 서버와 사업자간에 1/2복권 번호를 짜고 할 수 없도록 Time Stamp를 붙여 그러한 문제를 막았다. *(EKR CA[$B_{N/2}$ / TS]*
- **사업자, 서버와 사용자의 결탁문제**는 사용자와 서버가 결탁을 한다고 하더라도 서버와 사업자간의 결탁이 힘들기 때문에 해결된다.

이러한 것으로 새로운 제안방식에서는 암호학적인 기법을 확실히 구현하고 있으므로 기존방식의 문제성을 극복하고 보완하고 있다. 복권번호에 공개키로 암호화를 해 사업자에게 확인을 받을 뿐 아니라 나중에 자신의 키로만 풀리도록 하였다.

[표 1] 기존방식과 제안방식의 비교

	기존의 방식	새로운 제안방식
호기심과 재미	X	O
신뢰성	X	O
당첨번호 선택	O	O
서버와 사용자의 결탁 방지	X	O
서버와 사업자의 결탁 방지	X	O
사용자의 사업자의 결탁 방지	X	O
사업자 서버, 사용자의 결탁 방지	X	O
편리성	X	O
당첨자추첨방식의 문제점	X	O

제안방식은 그 구현이 어렵지가 않고 사용자들이 이용을 할 경우 손쉽게 할 수 있도록 하였다. 그러나 기존의 방식은 그 구입절차와 당첨절차가 복잡하여 사용자들이 사용을 할 경우 사용상 혼란을 줄 수 있다.

6. 결론

인터넷의 발전으로 인한 전자상거래의 많은 발전은 사람이 살아가는데 많은 편리성을 제공해 주었다. 그 응용분야 또한 연구하고 이를 실제로 운영하는 사이트들도 많이 생겨나고 있다. 전자경매, 전자입찰 등 이러한 사이트들은 집안에서 움직이지 않고 마우스 버튼하나로 하고 싶은 모든 일들을 할 수 있는 그런 시대가 온 것이다. 그러나 이러한 사이트들은 많은 문제점을 띄고 있는 것이 사실이며, 이를 위해 암호학적 기법과 네트워크의 안전성을 위한 방법 또한 많은 연구가 이루어지고 있는 것도 사실이다.

본 논문에서 제안한 방식은 네트워크 상에서의 거래에 안전성을 제공할 수 있는 프로토콜이라 사료된다. 앞으로의 발전 응용분야를 논한다면 전자경매, 전자입찰 등 여러 분야에서의 이용이 확대할 수 있을 것이다.

[참고문헌]

[1] 이만영,김지홍,류재철,송유진,염흥열,이임영, "전자상거래 보안 기술", 생능 출판사, 1999
[2] 박성준, 김지영, "공개키 기반구조에 관한 고찰", 정보처리 학회 발표 자료집, p55-71, 1997
[3] 김용운, "Protocols for the WWW Service", 제 4회 WWW Workshop강의 자료집, p9-55, 1996
[4] 충남대학교, "안전한 전자복권 구현:", 정보과학회, 1999
[5] 김지홍, "공개키 기반구조", 제 4회 정보통신망 정보보호 워크숍 발표자료집, p9-32, 1998
[6] 심영철, "인터넷 보안 기술", 제 4회 정보통신망 정보보호 워크숍 발표자료집, p117-171, 1998
[7] 이임영, 송유진 "현대암호", 생능 출판사, 1999
[8] 이임영, 최용락, 소우영, 이재광, "통신망 정보 보호", 도서 출판 그린, 1996
[9] 박남규, "국내외 전자상거래 솔루션 현황", 생능 출판사, p9-15, p349-350, 1999
[10] 김찬웅, "미국의 전자상거래 사례 연구", 생능 출판사, p121-167, 2000
[11] Enkol CO. Ltd, "http://www.enkol.co.kr"