검증 가능한 영수증을 발급하는 전자투표 시스템의 구현†

정한재, 이광우, 이윤호, 김승주, 원동호*

성균관대학교 정보통신공학부 정보보호연구소

Implementation of Voter Verifiable Receipts in E-Voting System†

HanJae Jeong, Kwangwoo Lee, Yunho Lee, Seungjoo Kim, Dongho Won*

Information Security Group, School of Information and Communication Engineering, Sungkyunkwan University.

요 약

최근 전자투표 시스템에 대한 투표자의 신뢰성을 높이기 위해 영수증을 발급하는 기술에 대한 연구가 활발히 진행되고 있다. 전자투표 영수증은 투표자가 자신이 투표한 결과가 최종집계에 올바르게 반영되었음을 확인할 수 있어야 하며, 매표 방지 기능도 함께 가지고 있어야 한다. 본 논문에서는 기존의 연구되었던 기술 중에서 일반 용지 및 프린터를 이용하여 검증 가능한 영수증을 발급하는 전자투표 시스템을 구현하고자 한다.

I. 서론

전자투표 시스템에서 발급되는 영수증은 투표소 반출여부에 따라 크게 두 가지로 나눌 수 있다. 투표소 밖으로 가지고 나갈 수 없는 영수증은 투표값을 암호화하지 않고 그대로 기록하는 것으로 VVPAT(Voter Verified Paper Audit Trail) 방식이 있다[1]. 이 방식의 경우 투표자는 폐쇄된 유리창으로 영수증을 확인하여 투표값을 쉽게 검증할 수 있지만, 전자적인 기록은 검증할 수 없으므로 영수증을 통한 재검표가 필연적이다. 반면, 투표소 밖으로 가지고 나갈 수 있는 영수증은 매표를 방지하기 위하여 암호화된 투표값을 기록하며, 이를 이용하여 전자적인 기록에 대해 신뢰를 가질 수 있다.

투표소 밖으로 가지고 나갈 수 있는 영수증 발급 기술은 2002년에 발표된 D.Chaum의 Visual Cryptography 방식, 2003년에 A.Neff가 제안한 코드북 방식, 그리고 2005년에 D.Chaum이 발표한 투표지 선택 방식과 2006년에 Lee 등이 제안한 안전성 파라미터 선택 방식[2]이 있다.

[2]에서 제안된 방식은 투표자가 안전성 파라미터 t만큼의 검증값을 선택한 후에 발급되는 영수증을 이용하면, 투표기를 검증 할 수 있고 자신의 투표값이 최종집계에 올바르게 반영되었음을 확인할 수 있다. 본 논문에서는 일반 용지와 프린터를 이용하며, 별도의 코드북이 필요 없는 [2]의 방식을 구현하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 요소 기술로서 2차원 바코드와 Base64[RFC 3548] 인코딩을 살펴보고, 3장에서는 실용적으로 활용할 수 있는 전자투표 영수증 발급 기술을 구현한다. 4장에서 향후 연구를 살펴보고, 마지막 5장에서 결론을 맺는다.

* 교신저자 : 원동호(dhwon@security.re.kr)

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학IT연구센터(ITRC) 육성·지원사업의 연구결과로 수행되었음.

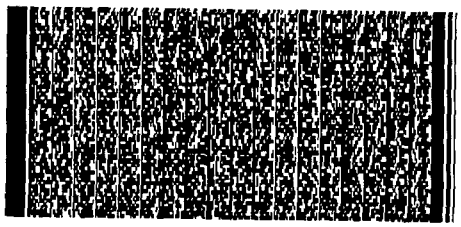
II. 요소 기술

전자투표 영수증 발급 기술을 구현하기 위해서 2차원 바코드와 Base64 인코딩을 이용한다.

1. 2차원 바코드

2차원 바코드는 기존의 1차원 바코드가 가진 정보 저장의 한계를 뛰어넘어 한 심볼(symbol) 당 약 2Kbyte의 정보를 기록할 수 있다. 또한 여러 심볼에 걸쳐 무한정의 데이터를 저장할 수 있어 PDF(Portable Data File)로 불리기도 한다[3].

1989년에 개발된 PDF417은 최대 2725byte를 저장할 수 있으며, $1in^2$당 300~500byte를 기록할 수 있다. 또한 텍스트뿐만 아니라 소리나 그림도 기록할 수 있으며, 오류가 발생하였을 경우 발견(detection) 뿐만 아니라 정정(correction)까지 가능하여 바코드가 약 50%까지 손상되어도 완벽하게 읽을 수 있다[4].



<그림 1> PDF417 2차원 바코드

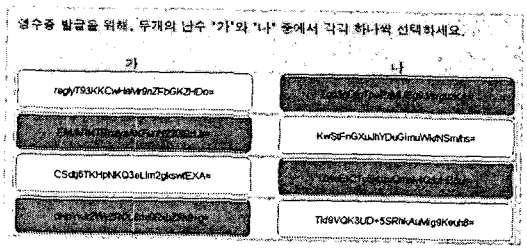
2. Bas64 인코딩

Base64 인코딩은 이진 데이터(Binary Data)를 3byte 단위로 나누어서 6bit의 인쇄 가능한 텍스트로 변환하여 가독성을 높이는 방법이다.

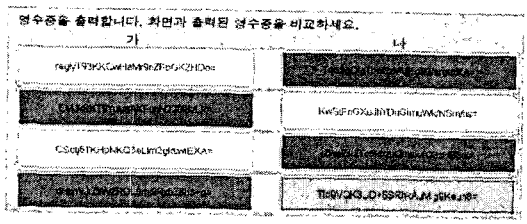
변환문자는 알파벳 대·소문자(A~Z, a~z), 숫자(0~9), 특수문자(+, /)로 구성된다. 3byte로 나누는 과정에서 나머지 byte들이 생길 때에는 '='를 패딩한다.

III. 영수증 발급 시스템 구현

본 논문에서는 [2]의 연구 결과를 이용하여 투표소 밖으로 가지고 나갈 수 있는 전자투표 영수증 발급 시스템을 구현하였다. 투표자는 정당한 신원확인 절차를 거친 후 시스템을 이용하며, 후보자는 4명으로 가정한다. 투표기는 투표가 시작되기 전에 후보자의 번호를 서로 다른 난수를 이용하여 각각 두 번씩 암호화하고, 그 값을 해쉬하여 검증값을 생성한 후 화면에 출력한다. 투표자는 투표기의 부정을 막기 위하여 <그림 2>처럼 후보자마다 서로 다른 두개의 검증값 중 하나씩 선택해야 한다. 그 후 선택하지 않은 값 중 투표할 후보의 검증값을 선택함으로써 투표를 완료한다.(<그림 3> 참조)



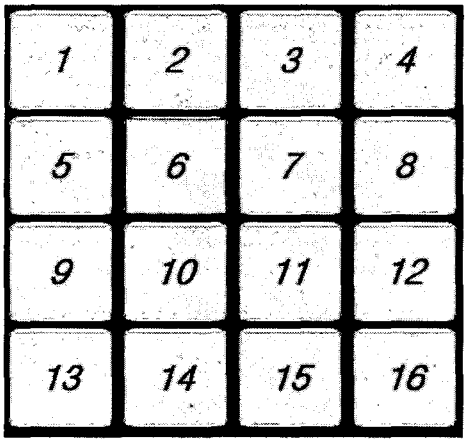
<그림 2> 후보별 검증값 선택



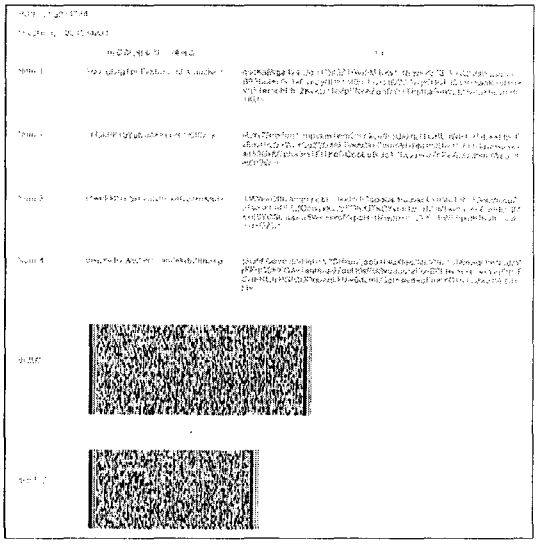
<그림 3> 투표할 후보 선택

높은 보안성을 유지하기 위하여 난수와 암호화에 사용되는 키의 길이는 1024bit로 한다. 그러나 영문과 숫자로 무작위 조합된 긴 문자를 그대로 출력하면 가독성이 떨어져서, 해쉬 함수 SHA1을 이용하여 1024bit를 160bit로 줄인 후에 *Base64*로 인코딩하여 화면에 표시한다. 본 논문에서는 후보자 수를 4명으로 가정하였기 때문에 투표자는 검증값을 4번 선택해야한다. 이러한 무작위 선택은 바람직하지 않은 것으로 알려져 있는데 심리학적으로 사람은 무작위 선택에 상당히 취약하기 때문이다[5]. 이러한 문제를 해결하기 위해 본 논문에서는 t회의 이진 무작위 선택(Binary random selection)을 1회의

난수 선택으로 바꾸었다. 즉, 투표자에게 선택 범위($1\sim2^4$)에서 하나의 수만 선택하도록 하는 <그림 4>와 같은 인터페이스를 구현하였다. 따라서 투표자는 검증값 4개를 선택하는 대신 16개의 번호 중 하나를 선택하는 것으로 대신할 수 있다.

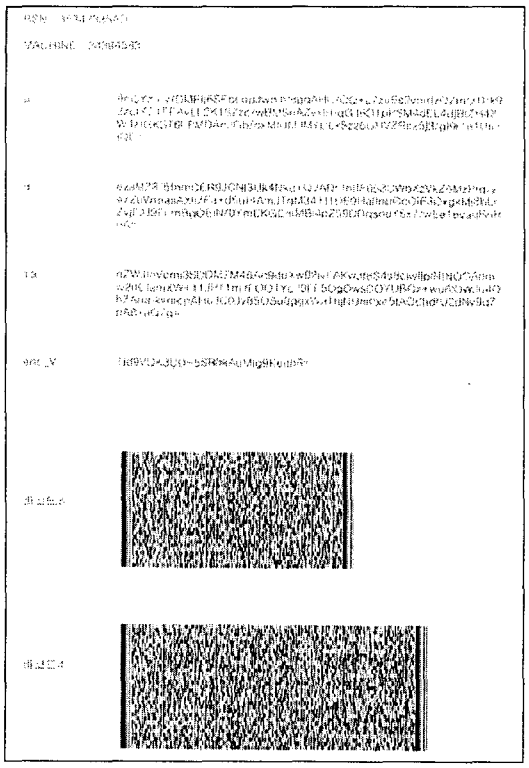


<그림 4> 검증값 선택 인터페이스



<그림 5> 첫 번째 영수증

발급하는 영수증은 총 2장이며, 출력되는 문자열들은 가독성을 높이기 위하여 모두 Base64로 인코딩하였다. 첫 번째 영수증에는 투표자가 선택한 검증값이 출력된다. 이를 검증하기 위하여 암호화에 사용된 난수도 출력된다. 투표자는 난수를 인자로 암호화하여 검증값이 나오는 것을 확인함으로써 투표기의 오동작 여부를 검증할 수 있다.



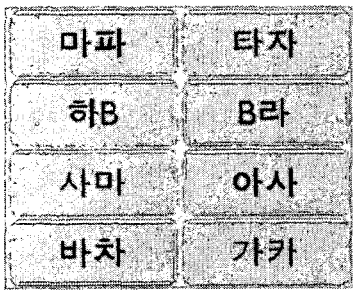
<그림 6> 두 번째 영수증

두 번째 영수증에는 투표자가 선택한 후보자의 검증값이 출력된다. 그리고 암호화에 필요한 소수 p와 mod p상에서의 원시원소 g, 그리고 공인기관의 공개키 Y_a가 출력된다. 투표자는 영수증에 출력된 투표한 후보자의 검증값과 공개게시판의 값을 비교함으로써 자신의 투표 내용이 전자적으로 올바르게 기록되었음을 검증할 수 있다.

IV.향후 연구

영수증에 출력된 값들은 Base64로 인코딩을 하였어도 제일 짧은 길이가 28자이므로, 투표소에서 짧은 시간 동안 화면에 표시된 내용과 영

수증을 비교하기에는 불편한 점이 있다. 향후 안전성을 유지하면서 출력되는 문자의 길이를 짧게 하여 검증을 용이하게 할 수 있는 기술이 필요하다.



<그림 7> 향후 인터페이스

V.결론

본 논문에서는 전자투표에서 투표기의 부정을 최소화 시키면서, 투표자가 자신의 투표가 올바르게 집계 결과에 포함됨을 확인할 수 있는 영수증 발급 기술을 구현하였다. 일반 용지 및 프린터를 이용하여 비용적인 측면이나 범용성에서 우수하여 실제 전자투표에서 활용될 수 있을 것으로 기대된다.

[참고문헌]

[1] R. Mercuri. "Physical Verifiability of Computer Systems," 5th International Computer Virus and Security Conference, March, 1992.

[2] Yunho Lee, Kwangwoo Lee, Seungjoo Kim and Dongho Won, "Efficient Voter Verifiable E-Voting Schemes with Cryptographic Receipts," Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2006/167, 2006.

[3] S. Itkin and J. Martell, "A PDF417 Primer", Bohemia, NY:Symbol Technologies, 1992.

[4] Robert B. Johnston and Alvin Khin Choy Yap, "Electronic Data Interchange using Two Dimensional Bar Code", Thirty-First Annual Hawaii International Conference on System Sciences Volume 4, page 83, 1998

[5] David Chaum, Peter Y. A. Ryan, Steve A. Schneider, "A Practical Voter-Verifiable Election Scheme," Proc. of ESORICS 2005, LNCS 3679, pages 118-139, Sep. 2005.

[6] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Information Theory, vol.IT-31, no-4, pages 469-472, 1985.

[7] M.Naor and A.Shamir, "Visual Cryptography," Proc. of Advances in cryptology (Eurocrypt' 94), LNCS 950, pages 1-12, 1995.

[8] C.A.Neff, "A Verifiable Secret Shuffle and Its Application to E-Voting," Proc. of the 8th ACM Conference on Computers and Communications Security(CCS-8), pages 116-125, 2001.

[9] C.A.Neff and J.Adler, "Verifiable e-Voting," IEEE Security and Privacy Magazine, vol.2, no.1, pages 38-47, Jan. 2004.

[10] D.Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," IEEE Security and Privacy Magazine, vol.2, no.1, pages 38-47, Jan. 2004.

[11] D.Chaum, P.Y.A.Ryan, and S,Schneider, "A Practical, Voter-Verificable Election Scheme," Technical Report CS-TR-880, University of Newcastle upon Tyne, 2004.