情 報 保 護 學 會 誌
第 15 卷 第 5 號, 2005. 10

전자 투표 시스템의 보안 기술 및 종이 영수증 동향

강 서 일*, 이 임 영**

요 약

IT 산업의 발달에 따른 기술의 변화로 인해 사용자들은 유/무선 단말기를 이용하여 여러 가지 서비스를 제공 받을 수 있을 정도로 IT 인프라가 발전하였다. 이러한 IT 발전은 전자 정부 구축에 대해 더욱 가속화 시키고 있으며, 민원 업무와 관공서의 업무가 인터넷을 통한 서비스로 국민에게 제공되어 편리성과 효율성을 높이고 있다. 전자 정부 서비스는 민원 서비스뿐만 아니라 민주주의 기반이 되는 대표자 선출의 투표에 대해서도 전자적인 서비스를 제공하여야 한다. 투표는 국민의 민주주의 의사가 방영되는 가장 기초적의 방식으로써 투표에 있어 전자 시스템을 도입하여 유권자의 편리성을 제공하고 투표 시스템의 효율성을 높이는 것이 전자 투표 시스템이다. 전자 투표 시스템은 국민의 의사를 방영하는 것으로 안전하게 투표의 과정이 이루어져야한다. 그러므로 본고에서는 전자 투표에서 적용되는 보안 기술 및 종이 영수증 기술에 대하여 알아보고 향후 연구 방향에 대해서 논의 한다.

Ⅰ. 서 론

현재의 IT기술의 발달로 인해 많은 오프라인 서비스가 온라인 서비스로 제공되고 있다. 이와 같은 과정에 있어, 정부는 e-Government를 구축하는데 있어 많은 서비스를 온라인상으로 제공하고 있다. 민주주의에 있어 투표는 참여자의 기본적인 의견을 수렴하고 방영할 수 있는 방안 중 하나이다. 이와 같이 가장 기초적이면서 가장 중요한 투표는 현재 투표 참여율의 감소와 무효표, 개표의 인력 및 투표 시간으로 인해 많은 비용과 시간을 활에 받고 있다. 이러한 투표의 방식에 전자 기기를 이용하여 투표의 시간을 단축하고 초기 비용은 높이지만 재활용을 통해 많은 투표의 비용 감소를 가지고 오며, 정확한 표기를 통해 무효표를 줄일 수 있다. 전자 기기를 이용하여 투표를 데이터로 저장하고 개표하는 방식을 전자 투표 시스템이라고 한다. 전자 투표는 다양한 방식으로 이루어지는데 전자 기기를 이용하는 방식을 모두 포함하는 포괄적 개념과 소괄적 개념으로는 투표부터 개표까지 모든 과정이 데이터와 전자 기기로 이루어지는 방식으로 말할 수 있다.

전자 투표의 발전 단계를 3단계로 분류하면 다음과 같다.

제 1단계 : 지정된 투표소에 유권자가 가서 투표를 하는 것으로 지정된 장소에 전자 투표 기기가 설치되어 있다.

제 2단계 : 임의의 투표소에서 유권자가 투표를 실시하는 것으로 유권자는 자신의 위치한 곳에서 가까운 투표소에 가서 투표를 한다. 이와 같은 방식에서는 유권자의 인증이 가장 중요한 기술로 부각되게 된다.

제 3단계 : 유권자는 자신이 있는 위치에서 전자 기기를 이용하여 투표를 실시할 수 있도록 하는 것으로 어디에 있더라도 투표가 가능하게 된다. 이와 같은 경우 인증 및 보안 기술이 적용되어 안전하게 투표가 이루어져야 한다.

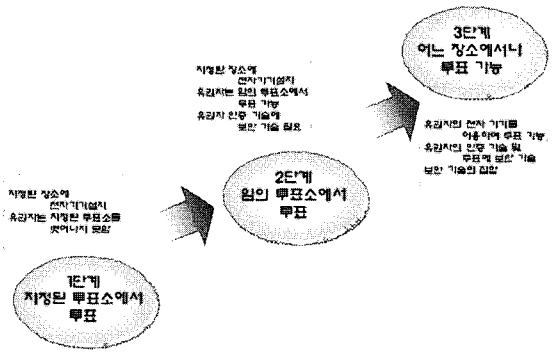
전자 투표 시스템의 발전단계로 제공되는 방안에서 있어서는 KIOSK(전자 투표 기기)를 이용하는 것과 인터넷 웹사이트를 이용하는 것, 모바일 단말기를 이용하는 방식으로 나눌 수 있다. KIOSK는 전자 투표 기기로써 독립적은 설치가 가능하고 투표의 결과를 저장하여 저장소에 보관하는 방안과 네트워크를 통해 전송하는 방안 등 각각의 구현하는 방안에 따라 특성을 가질 수 있다. KIOSK 자체는 독립적인 전자 투표 기기를 통칭하는 개념이 되며 많은 시스템들이 구현되

* 순천향대학교 정보기술 공학부 (kop98@sch.ac.kr)
** 순천향대학교 정보기술 공학부 교수 (imylee@sch.ac.kr)

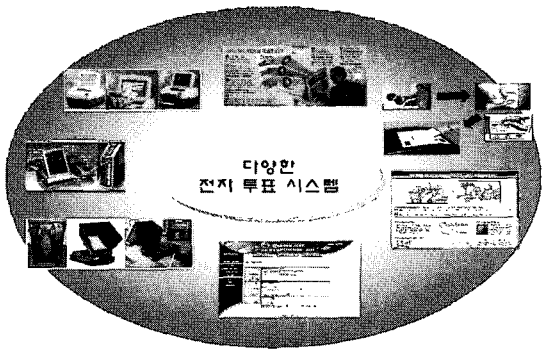
어 서비스를 제공하고 있다. 인터넷 웹 페이지를 이용한 투표 방식은 유권자가 투표를 제공하는 사이트에 접근하여 유권자임을 인증 받고 투표를 실시하는 것으로 공개된 네트워크상을 활용한다. 이로 인해 제 3자의 공격이나 시스템 자체의 보안성이 높아야 하며, 투표하는 유권자의 인증 기술이 중요하게 제공되어야 한다. 우리나라에서는 2002년 한국-일본 월드컵의 VIP를 선정하는 방안에서 웹사이트를 이용하는 투표 시스템을 제공한 적이 있다. 모바일 투표 시스템은 사용자가 모바일 단말기를 이용하여 투표를 실시하는 것으로 현재 구현된 서비스로는 제공되지 않고 있으나 유권자가 어디서든지 투표를 제공받기를 위해서는 서비스 단계로 발전되기 위해서는 필요한 기술이다.

II. 전자 투표 시스템 구성 및 보안 요구 사항

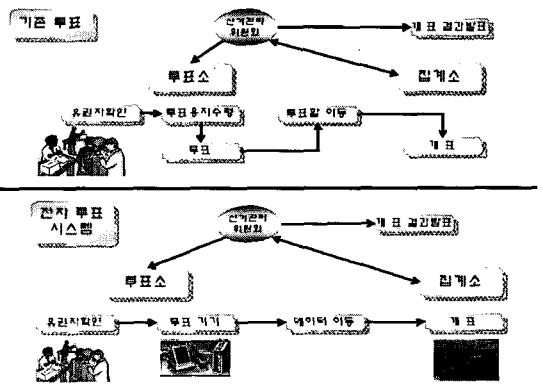
본 장에서는 전자 투표 시스템의 구성과 보안 요구 사항에 대하여 알아본다. 전자 투표 시스템의 구성은 전자 투표 시스템의 객체 및 일련의 과정에 대하여 살펴보고 이와 같은 시스템의 안전하게 제공되기 위한 보안 요구 사항을 알아본다.



〔그림 1〕 전자 투표의 단계 분류 그림



〔그림 2〕 다양한 전자 투표 시스템



〔그림 3〕 기존 투표 방식 및 전자 투표 시스템 구성

2.1 전자 투표 시스템의 구성

전자 투표 시스템은 큰 객체로 유권자, 후보자, 선거관리의원으로 나누어지고 물리적인 객체로는 전자 투표 기기, 개표 기기, 투표소 그리고 집계소로 나누어 질 수 있다. 이외의 분류로도 나누어질 수 있지만 본 논문에서는 객체를 위와 같이 정의한다. 전자 투표의 일련의 과정은 기존의 투표 과정과 동일한 절차로 이루어진다. 각각의 단계를 비교하면 그림 3과 같은 흐름을 갖는다.

전자 투표 시스템의 기술에 있어 유권자를 인증하는 방식으로 다양한 기술을 적용할 수 있으며, 그중에 하나가 스마트카드를 이용하는 방법이다. 투표 기기는 웹사이트를 이용하거나 터치스크린 등의 기기를 제공할 수 있으며, 각각의 투표 데이터는 물리적인 저장소에 저장되거나 전용선을 통해 이동하여 집계 서버나 집계 프로그램을 통해 개표가 이루어진다. 개표의 내용은 선거관리 위원회에 전송되고 선거관리 위원회는 투표의 내용을 공표한다. 이와 같이 일련의 과정을 거치는 것이 전자 투표 시스템이 되겠다.

2.2 전자 투표 시스템의 보안 요구 사항

전자 투표 시스템의 보안 요구 사항은 우선 공통적으로 적용될 수 있는 사항과 각각의 방식에 특성에 따라 다른 보안 요구 사항이 필요할 수 있다. 본 장에서는 전자 투표 시스템 중에 KIOSK(전자 투표 기기)를 이용하는 방안에 대한 요구 사항을 기술한다. KIOSK는 투표소를 설치하는 방식으로써 인증을 오프라인으로 제공할 수 있고, 투표한 데이터를 오프라인 이동이나 전용선을 통한 이동으로 정의 할 수 있다. 그러므로 다음과 같은 공통적인 투표의 보안 요구사항을 제시한다.

- 완전성(Completeness) : 투표한 내용이 집계에 정확하게 방영되어야 한다. 이는 투표한 내용이 누락되어서는 안 된다는 것이다.
- 비밀성(Privacy) : 유권자가 자신의 투표한 내용을 제 3자나 다른 인원이 알 수 없어야 한다.
- 선거권(eligibility) : 선거권은 유권자가 선거를 할 수 있는 권리를 가지고 있는지를 알아보는 것으로써, 전자 투표에서는 정당한 유권자인지를 확인하는 인증 과정으로 해결 할 수 있다.
- 이중투표방지(unreusability) : 이중투표방지는 정당한 유권자가 투표를 두 번하는 것으로써 1인 1표에 위배되는 행위이다.
- 검증성(verifiability) : 선거에서 유권자의 투표 집계가 정확히 이루어졌는지 검증 할 수 있어야 한다. 이는 개별 검증과 전체 검증으로 나누어지는데 개별 검증은 유권자의 표가 집계에 올바르게 되었는지 확인하는 것이고 전체 검증은 총 집계의 결과가 정당한지 확인하는 것이다.
- 매표방지(receipt-freeness) : 유권자가 제 3자나 다른 사람에게 자신의 투표한 내용을 매매하는 것으로 투표한 값을 증명할 수 있어서는 안 된다. 여기서 투표한 값을 증명한다는 것은 특정한 후보를 선택하였다는 것을 보여주는 것을 말한다.

이와 같은 보안 요구 사항이외에 디지털 데이터를 이용함으로 인해 다음과 같은 추가적이 보안 요구 사항이 필요하게 된다.

- 무결성 : 저장된 데이터나 유권자가 선택한 데이터가 변경되지 않았음을 제공하여야 한다.
- 기밀성 : 각각의 데이터는 접근할 수 있는 객체만이 데이터를 복호할 수 있어야 한다. 이는 투표소에서의 데이터를 집계소만이 확인 가능해야 한다.
- 가용성 : 투표 시스템은 어떠한 경우에도 투표 서비스를 제공할 수 있어야 한다. 제 3자의 방해나 시스템의 문제로 서비스가 정지된 경우 다른 방법으로 서비스를 지속적으로 제공하여야 한다.

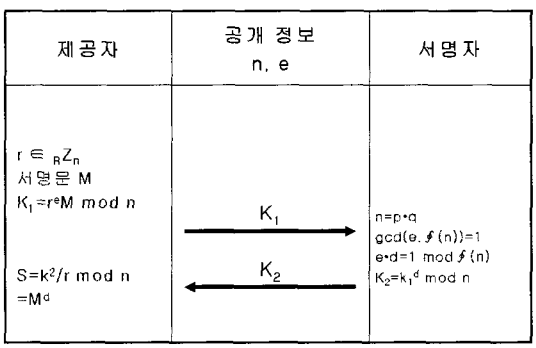
이상의 보안 요구 사항이 만족되어야지만 전자 투표 시스템을 활용하는 유권자들은 시스템에 대한 신뢰성을 가지고 투표를 실시할 수 있다. 보안 요구 사항을 만족시키기 위해 전자 투표 시스템들은 다양한 보안 기술을 적용하여 시스템을 구현하고 있다.

Ⅲ. 전자 투표 시스템의 보안 기술

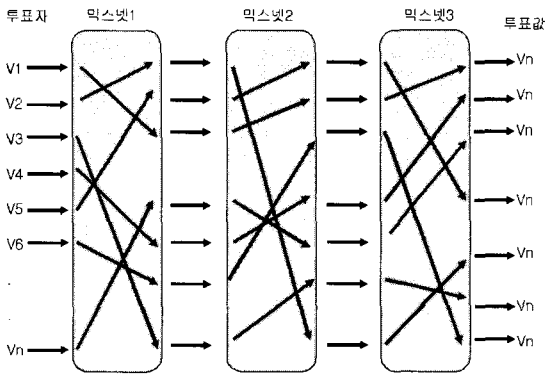
전자 투표 시스템의 보안 기술로는 기본적인 공개키 및 대칭키를 이용하는 방식부터 특수한 은닉 서명, 익명성 채널을 제공할 수 있는 믹스넷 그리고 준동형 암호화 방식이 있으며 유권자에게 프린트된 영수증을 제공하는 방식 등이 있다. 본 장에서는 전자 투표 시스템의 보안 기술로써 대표적인 은닉서명 방식과 믹스넷 그리고 준동형 암호화 방식에 대해서 알아본다.

3.1 은닉 서명

은닉 서명은 서명에 있어 서명을 제공하는 당사자가 메시지의 내용을 모르는 상태에서 서명을 제공하는 것이다. 이와 같은 경우 자신의 서명한 메시지의 내용과 서명을 받는 당사자를 연결할 수 없는 익명성을 제공한다. 이와 같은 은닉 서명은 전자 화폐에서 응용하며, 전자 투표에서는 유권자와 투표의 용지를 연결할 수 없는 익명성을 제공함으로 인해 비밀성과 프라이버시를 제공할 수 있다. 전자 화폐에 있어 익명성은 익명성제어 까지 연구가 되어 있다. 이와 같은 경우 익명성 제어는 부정한 경우 추적이 가능하도록 하는 것으로써 전자 투표에 있어 투표 값이나 부정이 발견된 경우 익명성을 철회하여 추적할 수 있어야 한다. 은닉 서명은 공개키 기반에서 사용되는 것으로 다음 그림 4를 참조하여 보면 메시지 제공자는 자신이 생성한 메시지 즉 정당하게 서명이 필요한 메시지와 임의 랜덤 값을 생성해서 임의 랜덤 값은 공개키로 암호화하여 서명 받을 메시지와 함께 서명자에 전송한다. 그럼 서명자는 전송 받은 메시지를 서명해서 다시 메시지 제공자에게 전송한다. 그럼 메시지 제공자는 자신이 생성한 랜덤 값을 삭제하고 정당한 메시지의 서명자의



〔그림 4〕 은닉 서명의 구성



〔그림 5〕 믹스넷 구성

개인키로 서명이 되어 있는 상태이다.

3.2 믹스넷 기술

믹스넷은 익명 통신 채널을 구성하는데 필요하다. 즉 전송되는 과정에서 믹스넷을 통과하게 되면 각각의 메시지가 믹스넷에서 섞이게 됨으로 누구의 메시지인지 알 수 없게 된다. 이와 같은 방식으로 믹스넷의 기술로 중복 암호화 방법을 이용하기도 한다. 그러나 믹스넷을 통과하는 경우 통과하기 전에 결과와 통과한 결과가 같아야 한다. 이는 믹스넷에서 메시지의 내용을 읽어버리는 경우가 발생해서는 안 된다. 그림 5를 참조하면 투표자의 값이 믹스넷을 통과하면서 내부적으로 섞이게 된다. 그 이후에 나온 투표 값을 어떠한 값이 누구의 값인지 알 수 없게 된다. 이와 같은 방법은 사용자의 익명성을 제공할 수 있는 방안도 된다.

3.3 준동형 암호화 방식

준동형 암호화 방식은 각각의 메시지를 암호화하는 값과 메시지 두 개를 합쳐서 암호화한 값이 동일하게 나오는 것으로 암호화에 따라 지수승 연산의 효율성을 제공하는 방법이다. 이와 같은 방법으로는 다음의 예를 볼 수 있다. RSA에서 (e, n)의 공개키로 보고 (d, n)를 비밀키로 보면 다음과 같은 수식을 이용할 수 있다.

$$m^{e}_{1} \bmod n = a_1,\ m^{e}_{2} \bmod n = a_2$$
$$(m_1 m_2)^{e} \bmod n = a_1 a_2 \bmod n$$
$$= m^{e}_{1} \bmod n * m^{e}_{2} \bmod n$$

위 식은 두 개의 메시지를 암호화하는 것과 메시지를 곱해서 암호화하는 것이 동일한 결과를 나타내고 있다. 이와 같은 방법을 전자 투표에 이용하는 것으로는 각각의 투표 값을 암호화 한 상태에서 곱하는 것으로 한 번의 복호화로 메시지의 값을 복호 할 수 있다.

3.4 종이 영수증 기술

종이 영수증 기술은 암호 기술은 아니지만 전자 투표 기술에서 유권자의 신뢰성을 보장할 수 있으며, 데이터만으로 이루어진 투표 시스템을 검증 할 수 있는 도구로 이용할 수 있다. 종이 영수증 기술을 적용하는 경우 다음과 같은 장점을 가질 수 있다.

- 전자 투표 시스템을 개표 결과를 감사할 수 있는 자료가 된다.
- 유권자가 투표한 내용에 대한 검증 자료가 된다.
- 종이 영수증은 제 3자의 개입이나 수정·위조가 어렵다.

이와 같은 장점이 있는 방면에 단점을 가지고 있기도 하다. 우선 종이 영수증 기술을 반대하는 가장 큰 이유는 매매가 가능할 수 있다는 것이다. 영수증 자체에 검증할 수 있는 값이 포함 되어 있어 보안 기술이 적용하지 않으면 각각의 유권자가 어떠한 후보를 선택하였는지 알 수 있게 된다. 그리고 종이 영수증을 새로 생성하여 자신의 선택 값을 부정할 수도 있다. 이와 같은 사항을 막기 위해 종이 영수증 기술을 사용하는 경우 새로운 보안 요구 사항이 필요하다.

Ⅳ. 다양한 전자 투표 시스템과 종이 영수증 기술

본 장에서는 3장에서 언급한 보안 기술을 적용한 전자 투표 시스템에 대하여 알아본다. 기존의 전자 투표 시스템으로 발표된 논문의 동향과 각각의 특징에 대하여 기술한다.

4.1 은닉 서명 방식을 적용한 전자 투표 시스템

은닉 서명을 적용한 전자 투표 시스템은 각각의 투표에 대한 사용자의 익명성을 제공한다. 다음의 논문들을 통해서 살펴보자.

4.1.1 An untraceable, universally verifiable voting scheme

본 방식은 Michael J.Radwin이 제안한 방식으로 은닉 서명을 이용하여 프라이버시와 일반적인 검증, 편리성을 제공하고 매표하려고 하는 경우 값을 추적할 수 없다.[9]

투표의 흐름은 아래와 같다.

ㄱ. x, r을 생성하고 스마트카드에서는 a_i, c_i, d_i와 r_i를 생성한다.

ㄴ. 투표자는 K의 은닉 후보자를 생성하여 다음과 같이 값을 연산한다. 여기서 u는 투표자의 사회 보장 번호로 유권자를 식별할 수 있는 방안이 된다. 그리고 3은 기관의 공개키로 예를 보여주고 있다.

$$B_i = r_i^3 * f(X_i, Y_i) \bmod n$$
$$X_i = g(a_i, c_i) \quad Y_i = g((a_i \oplus u), d_i)$$

ㄷ. 기관(투표를 관장하는 곳)은 사용자에게 총 수의 1/2에 해당하는 검증 값을 요구하고 투표자는 기관이 요청하는 것에 정확히 응답하여 검증할 수 있는 값을 전송한다.

ㄹ. 기관은 1/2값이 정확하면 다음과 같이 서명하여 돌려준다.

$$\prod_{i \notin R} B_i^{1/3} = \prod_{1 \le i \le K/2} B_i^{1/3} \bmod n$$

ㅁ. 투표자가 기관의 서명을 받은 값에서 r_i를 제거하여 다음과 같은 P값을 연산할 수 있다.

$$P = \prod_{1 \le i \le K/2} f(X_i, Y_i)^{1/3} \bmod n$$

ㅂ. 이후 투표자는 (w, P)로 투표를 하는데 w는 유권자가 투표 후보자 중 선택한 값이 되고 P는 기관으로부터 서명된 값이다. 그리고 인증기관의 공개키로 암호화하여 전송한다. 그러므로 정당한 유권자는 투표 이후 P값의 확인을 요청할 때 기관으로부터 서명된 1/2값에서 1인 경우 a_i, c_i 와 y_i를 증명하고 0인 경우 x_i, (a_i XOR u)와 d_i를 증명한다.

이 방식에서 유권자가 선택한 값은 P와 연관성이 없다. 즉 유권자의 정당한 인증을 위한 방안은 제시되어 있으나 w값의 변조의 경우 증명을 할 수 있는 방안이 없다. w가 방식에서 예를 든 Yes(=1), No(=0)의 두 가지 선택의 경우 Yes가 에러나 다른 사항으로 인해 No 로 바뀌어도 검증 할 수 있는 방안을 제공하지 못하고 있다. 이는 w와 P가 서로 독립적이기 때문이다.

4.1.2 Ballot-Cancellation Protocol of E-voting Based on Two Independent Authorities

본 방식은 Yong-Sork HER와 Kouichi SAKURAI가 발표한 것으로 은닉 서명과 투표 아이디 등을 이용하여 프라이버시, 공정성, 안전성, 검증을 제공할 수 있는 방안에 대하여 제안하였다.[16]

전자 투표 시스템의 참여 개체는 유권자, 관리자 그리고 집계소이며 공개 보드를 이용한다. 은닉서명은 유권자가 관리자로부터 받아 사용한다. 전자 투표의 흐름도는 다음과 같다.

ㄱ. 유권자는 투표값 v_i를 선택하고 집계소의 공개키$\langle N_T, Y_T \rangle$로 다음과 같이 암호화 한다.

$$Z_i = Y_T^{v_i} x^{r_{v_i}} \bmod N_T$$

ㄴ. 유권자는 암호화된 Z_i를 관리자의 공개키$\langle e_A, N_A \rangle$로 암호화 한다.

$$C_i = Z_i^{e_A} \bmod N_A$$

ㄷ. 유권자는 다음과 같이 은닉 값을 생성한다. 여기서 r_i는 랜덤하게 만들어진 은닉인자다.

$$e_i = x(C_i, r_i)$$

ㄹ. 유권자는 다음과 같이 자신의 ID, 은닉 값(e_i) 그리고 은닉 값에 자신의 서명을 하여 관리자한테 제공한다.

ㅁ. 관리자는 서명 값을 확인하고 아이디를 리스트에 있는지 확인한다. 만약 모든 확인이 끝나면 은닉 값(e_i)에서 관리자의 서명(d_i)을 하여 사용자에게 제공한다.

ㅂ. 유권자는 관리자로부터 받은 서명값(d_i)과 은닉을 제거할 수 있는 r_i를 포함하는 유권자 서명값 $y_i(=d_i, r_i)$를 생성한다.

ㅅ. 유권자는 C_i, Y_i를 관리자한테 전송한다. 관리자는 서명을 복호화 하고 복호화 값으로 은닉 인자를 알 수 있게 되어 C_i를 검증하게 된다. C_i는 자신의 공개키로 되어 있기 때문에 바로 개인키로 풀 수 있다. 이때 전체 곱을 통해서 빠른 복호화를 가지고 올 수 있다. 이후 Z_i는 집계소의 공개키로 되어 있으므로 관리자는 내용을 복호 할 수 없다. 이후 집계소로 이동된 Z_i도 동일한 전체 곱으로 빠른 복호화 연산을 제

공할 수 있다.

이 방식에서는 은닉 값에 투표 값이 포함 되어 있다. 그러므로 은닉 값을 풀기 이전까지는 투표 값을 알 수 없게 된다. 암호화에는 공개키를 이용한 두 번의 암호화가 진행된다. 이러한 시스템을 구현하는 데 있어 가장 취약할 수 있는 문제는 Reblocking문제이다. RSA에서 두 개의 암호화를 이용하는 경우 서명 후 암호화 혹은 암호화 후 서명이다. 현재 위 방식은 암호화 후 서명 방식을 선택하고 있는 데 이때 서로의 공개키에 적용되는 모듈러 값이 다르고 이에 따라 복호된 메시지가 동일하지 않게 나오는 확률이 존재하고 있다는 것이다. 보안 기술에서는 이러한 방법을 피하는 것으로 각각의 공개키 값을 확인하여 서명을 먼저 할 것인지 암호화를 먼저 할 것인지를 선택하여야 한다. 위 방식에서는 공개키로 암호화 후 서명을 이용하는 것으로 제안 되어 있기 때문에 규칙에 따른 사용자의 공개키와 개인키를 다시 생성하여 할 것이다. 만약 그렇지 않고 구현한다면 관리자의 공개키 와 사용자의 개인키 혹은 집계소의 공개키와 사용자의 개인키로 인해 문제가 발생할 수 있다.

4.2 믹스넷 기술을 적용한 전자 투표 시스템

믹스넷 기술을 적용하여 익명 채널을 구성한 전자 투표 시스템을 알아본다.

4.2.1 Receipt-Free Mix-Type Voting Scheme

본 방식은 Kazue Sako와 Joe Kilian이 발표한 것으로 믹스넷을 이용하여 투표 부스에서 투표를 하고 안전하게 저장하는 것이다.[11] 보안 적으로 제 3자가 데이터의 내용을 엿보지 못하게 하는데 있다. 전자 투표 시스템은 다음과 같이 진행된다.

ㄱ. 센터의 공개키 $y_j = g^{x_j} \bmod n$이고 비밀키는 x_j이다. 유권자 i의 공개키는 $\alpha_i = g^{a_i} \bmod n$이고 비밀키는 a_i이다. 투표 메시지는 m_0, m_1로 구성되어 있다.

ㄴ. 센터는 임의 랜덤 비트의 길이 $\Pi^{(i,n)}$을 유권자의 공개키로 암호화해서 맡긴다. 유권자는 다음과 같은 연산을 할 수 있다.

$$v^0 = (\overline{G_n}, \overline{M_n}) = (g^{r_{2n}}, m_0 \cdot \overline{y}^{r_{2n}})$$
$$v^1 = (\overline{G'_n}, \overline{M'_n}) = (g^{r_{2n-1}}, m_1 \cdot \overline{y}^{r_{2n-1}})$$

ㄷ. 유권자는 $\Pi^{(i,n)} = 0$이면 (v_0, v_1)으로 하고 아니면 (v_1, v_0)로 한다.

ㄹ. 집계 센터는 한 번의 투표에 $\Pi^{(i,n)}$를 사용한다는 것을 알아낸다.

ㅁ. 센터는 다음의 유권자에게 $\Pi^{(i,n-1)}$을 유권자에게 보낸다. 유권자는 다음과 같은 연산을 할 수 있다.

$$(\overline{G_{n-1}}, \overline{M_{n-1}}) = (\overline{G_n} g^{r_{2(n-1)}}, \overline{M_{n_0}} \cdot \overline{y}^{r_{2(n-1)}})$$
$$(\overline{G'_{n-1}}, \overline{M'_{n-1}}) = (\overline{G_n} g^{r_{2(n-1)-1}}, \overline{M_{n_0}} \cdot \overline{y}^{r_{2(n-1)-1}})$$

위와 같이 각각의 믹스 서버를 통과하면서 암호화 메시지는 계속 증가하게 된다. 하지만 복호에 있어서는 총 곱의 합으로 나누면 메시지(m)의 값만 나온다.

위와 같은 방식은 모든 믹스넷의 단계를 모두 통과하여야하고, 다른 제 3자가 값을 수정하려고 한다면 임의 값을 동일하게 곱해주면 된다. 이는 앞에 G의 연산과 뒤에 M의 연산은 동일하게 처리됨으로임의 값을 뒤에 곱해주면 m의 메시지가 변경되더라도 변경되었다는 것을 알 수 없게 된다. 즉 믹스넷 자체가 안전하며, 중간 값을 검증할 때 메시지는 복호화 될 수 있다.

4.2.2 Almost Entirely correct Mixing With Applications to Voting

본 방식은 Dan boneh와 Philippe Golle이 발표한 것으로 기존의 믹스네트워크 보다 검증 기술에 있어 새로운 방식을 적용하여 전자 투표에 있어 익명성을 제공할 수 있다.[3] 이 방식에서의 믹스넷을 이용하는 방법은 다음과 같다.

초기 세팅으로는 키를 생성하는데 있어 ELGamal 방식을 이용하고, 비밀 분산을 통해서 키를 각각의 믹스넷에 분배한다. 개인키는 x가 되고 공개키는 $y = g^x$가 된다. 이후 시스템의 흐름은 다음과 같다.

ㄱ. 믹스 서버는 다음과 같은 값을 공개 보드에서 가지고 와서 암호화를 한다.

$$C_i = (g^{r_i}, m_i \cdot y^r)$$

ㄴ. M_j의 믹스 서버의 무작위로 다음과 같은 암호문을 생성한다.

$$C'_i = (g^{r'_i}, m_i \cdot y^{r'})$$

ㄷ. 생성되는 암호문에 있어 r은 비밀리에 보관하고 있다.

검증의 단계에 있어서는 암호문을 적용하기전의 곱이 적용한 후의 곱과 동일하게 나와야 한다. 다음과 같은 수식이 성립되어야 한다.

$$\prod_{i=1}^{n} m_i = \prod_{i=1}^{n} m'_i$$

각각의 값은 영지식 증명을 통해서 믹스서버가 생성하였다는 것을 증명할 수 있다.

4.2.3 An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness

본 방식은 Riza Aditya, Byoungcheon Lee, Colin Boyd 와 Ed Dawson이 제안한 것으로써 믹스 네트워크의 기반의 Lee의 투표 기술을 변경하여 적용하는 것으로 관리자가 랜덤값을 제공하고 투표 단계는 믹스 네트워크를 이용하여 익명성 채널을 제공받는다.[14]

투표의 흐름은 다음과 같다.

ㄱ. 각각의 유권자(V_i)는 각각의 투표 값 (α_i, β_i) $E_y(v_i, r_i)$로 r_i는 투표자가 임으로 선택한 랜덤값이 되고 관리자에게 암호화 한 메시지와 서명한 메시지를 전송한다. 관리자는 각각의 서명을 검증한다.

ㄴ. 관리자는 랜덤한 값 t_i를 선택하여 재 암호화를 한다. 그 암호화 값은 공개 보드에 올려 둔다.

$$(\alpha'_i, \beta'_i) = (\alpha_i g^{t_i}, \beta_i h^{t_i})$$

ㄷ. 유권자는 다음과 같이 연산을 통해서 값을 검증할 수 있다.

(1) 검증을 위해 다음과 같은 랜덤 값을 선택한다.

$$k, r, t \in_R Z_q$$

(2) 다음과 같은 값을 생성할 수 있다.

$$(a, b) = (g^k, y^k)$$
$$d = g^r y_i^t$$

(3) 해쉬를 이용하여 생성하는 것으로 다음과 같은 값을 연산한다.

$$c = H(a, b, d, \alpha'_i, \beta'_i)$$

(4) 다음의 값을 생성해서 전송 받는다.

$$u = k - t_i(c + r)$$

(5) 다음의 값을 검증자에게 전송한다.

$$(c, r, t, u)$$

(6) 검증자는 다음과 같이 검증을 한다.

$$c = H(g^u(\alpha'_i/\alpha_i)^{c+r}, y^u(\beta'_i/\beta_i)^{c+r}, g^r y_i^t, \alpha'_i, \beta'_i)$$

ㄹ. 믹스넷을 통해서 각각의 투표 내용을 믹스한다. 믹스넷의 수식은 다음과 같다.

$$(\alpha_i, \beta_i) \rightarrow (\alpha'_i, \beta'_i) = (\alpha_i g^{r_i}, \beta_i y^{r_i})$$

위 방식은 믹스넷의 서버를 이용하여 재 암호화를 하여 전송하고 각각의 검증 과정에서는 해쉬의 값을 확인한다. 이와 같이 믹스넷을 이용하는 경우 생성되는 값이 정확한지를 복호화하지 않고도 확인 가능하다.

4.3 준동형 암호화를 이용한 전자 투표 시스템

준동형 암호화 시스템은 앞에서 기술의 설명에 이용된 것으로 하나씩 암호화 하는 것과 메시지를 모아서 암호화는 것과 같은 결과로 개표를 하는 동안 암호화된 메시지를 한 번의 복호화로 메시지를 알아낼 수 있다. 하지만 투표의 값이 다양하면 결과를 확인하기 어려운 단점을 가지고 있다. 다음의 방식들을 통해서 전자 투표에 준동형 암호화 방식을 어떻게 적용했는지 알아본다.

4.3.1 Multiplicative Homomorphic E-Voting

본 방식은 Kun Peng, Riza Aditya, Colin Boyd, Ed Dawson와 Byoungcheon Lee가 제안한 것으로 새로운 전자 투표 시스템으로 곱을 이용한 중동형 암호화 방식을 이용한다.[6] 유권자는 인수분해를 이용할 수 있으며, 투표 시스템의 흐름은 다음과 같다.

ㄱ. 예비 단계

m명의 후보자의 데이터는 C_1, C_2, ..., C_m이 된다. 그리고 ElGamal의 방식으로 각각의 공개키와 개인키를 생성한다. 이후 각각의 값을 생성하는데 사용되는 수의 집합을 Q라고 하면 $Q_1 = \{0\}$이면 Q_2는 공집합이 된다. 이때 택하는 정수 두 개가 $S_1 = 1$, $S_2 = 0$이 된다.

ㄴ. 투표 단계

각각의 유권자가 V_1, V_2, ..., V_n은 Q를 선택하여

자신의 투표값 V_i를 다음과 같이 연산한다.

$$C_i = E(v_i) = (a_i,\ b_i) = (g^{r_i},\ v_i y^{r_i})$$

ㄷ. 개표 단계

각각의 투표 데이터를 모아 다음과 같이 곱으로 계표한다.

$$v = D(\prod_{j=1}^{k} C'_i)$$

v는 다음 같이 인수 분해 되어 결과를 나타낼 수 있다. 만약 $1 \notin Q$이면, $v = \prod_{j=1}^{m} p_j^{t_i}$로 계산되어 지고, 만약 $1 \in Q$이면 $v = \prod_{j=1}^{m-1} p_j^{t_i}$로 계산 할 수 있다.

위에서는 두 개의 각각의 투표의 결과를 합한 것과 곱한 것이 같다는 것을 이용하는 것이다. 즉 위의 곱을 구하고 나면 모든 메시지의 합이 나온다. 그러나 메시지의 값이 다양한 경우 각각의 합을 구하기 어렵게 된다. 준동형 암호화 방식은 Yes, No 투표에서는 효율성을 가져 올 수 있다.

4.3.2 Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots

본 방식은 준동형 암호화 방식을 이용하며 공개키 방식 기술을 이용하여 메시지를 암호화 한다. 다음은 전자 투표 시스템의 흐름이다.

ㄱ. 다음과 같이 투표 기관 A에서는 Ai를 생성한다. 각각의 $A_i = C_{i,j}$로 j=1, ..., l이 된다. $c_{i,j}$는 PKC로 암호화하고 개인키로 서명하면 다음과 같은 메시지가 된다.

$$(E^{C}(c_{i,j}))_{SK_A}$$

ㄴ. 각각의 투표자의 공개키로 메시지를 암호화해서 전송하는데 투표에서 이용하는 공개키로 $C_{i,j}$를 암호화 하여 전송한다. 다음과 같은 메시지가 된다.

$$E^{v_j}(E^{V}(c_{i,j}), P_{v_j})$$

ㄷ. 유권자는 다음과 같이 $EV(c_{i,j})$를 검증하고 $EC(c_{i,j})$일치하는지 확인한다. 다음과 같은 수식을 이용하여 합을 구할 수 있다.

$$\prod_{j=j,i=1,\ldots,s} (E^{V}(c_{i,j})) = E^{V}(\sum_{j=j,i=1,\ldots,s} c_{i,j}) \equiv E^{V}(C_J)$$

ㄹ. 유권자는 자신의 투표 값을 투표키로 암호화한다. 각각의 암호화 메시지($E^{V}(b_j^t)$)는 다음과 같은 준동형 암호화로 값을 얻을 수 있다.

$$E^{V}(C_J)E^{V}(B_s^t) = E^{V}(\sum_{i=1,\ldots,s} c_{i,j} + \sum_{i=1,\ldots,s} b_i^t) \equiv E^{V}(C_J + B_J^t)$$

위의 메시지는 준동형 암호화 성질로 각각의 곱을 합으로도 구할 수 있다는 것이다.

4.4 종이 영수증 기술

종이 영수증 기술을 암호화 방식을 이용하는 보안 기술은 아니다. 하지만 전자 투표 시스템에 있어 데이터를 검증할 수 있는 방안이며, 감사할 수 있는 도구로 이용될 수 있다. 또한 유권자가 투표한 결과를 보거나 프린트 내용을 보유함으로 신뢰성을 제공할 수 있게 된다. 전자 투표 시스템의 보안 기술은 기존의 암호 기술을 이용하며 그 내용을 프린트해서 제공한다. 그러나 프린트된 종이 영수증 기술에 의해서 매표가 가능할 수 있으며, 비밀 투표를 하지 못하게 되는 경우가 발생할 수 있다. 그래서 프린트되는 내용에도 암호 기술을 적용하거나 종이 영수증의 내용을 알아보지 못하게 하는 방법이 있으며, 다른 방법으로는 프린트된 영수증 자체를 가지고 나가지 못하게 하는 것이다. 다음의 기술은 종이 투표 영수증 기술의 대표적인 기술이다.

4.4.1 암호화되지 않은 내용을 출력하는 영수증 기술

영수증 기술 중에 유권자가 선택한 내용을 그대로 투표해서 보여준 것으로 대표적인 방식으로 VVPAT와 VVPB가 있다. 두 기술 모두 유권자가 선택한 내용을 그대로 프린트하여 보여주고 유권자가 영수증을 가지고 투표소 밖으로 나갈 수 없으며, 투표함에 자동적으로 제출하게 된다.

ㄱ. VVPAT

VVPAT(Voter Verified Paper Audit Trail)

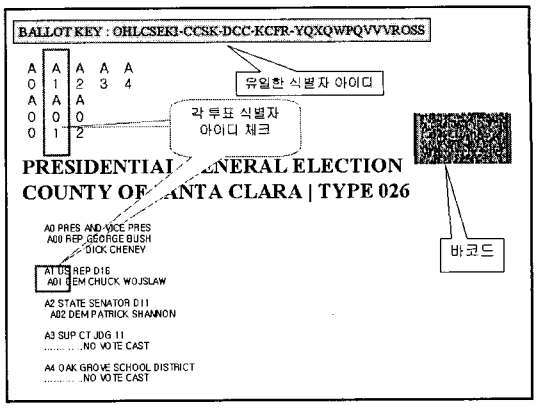
방식은 독립기기를 이용하는 투표 시스템 있어 투표에 대한 프린트 영수증을 제공하는 것이다.[17] 유권자는 독립기기가 설치된 투표 장소에 가서 투표를 실시한다. 유권자가 투표를 완료하고 나면 자신의 투표한 결과를 프린트하여 제공해주는 영수증을 받을 수 있다. 이때 영수증을 제출하는 방식과 영수증 자체가 투표함에 자동적으로 들어가는 방식 두 가지가 있다. 둘 다 영수증의 결과를 가지고 투표 장소를 벗어나지는 못한다. 하나의 예로 AccuPoll사의 VVPAT는 종이에 투표의 기록을 남기는 방식으로 사용되고 투표용지로는 편지지 크기를 이용하고 있다. 프린트 시스템으로는 잉크젯을 이용하고 있으며, 프린트되는 내용에는 워터마크 혹은 특수한 용지를 이용하고 이용한다. 독립 기기 시스템은 투표에 대한 데이터를 저장하는 것과 투표 영수증을 출력하여 저장하는 것 이렇게 두 가지로 나누어 관리된다. 투표 영수증으로 출력되는 내용은 그림 6과 같다.

- 유권자의 식별자 아이디 : 투표하는 유권자마다 식별자를 부여하여 차후 검증이 가능하도록 제공
- 전자 기록과 일치하는 바코드 : 데이터의 내용과 투표용지의 내용이 매칭 되도록 정보를 바코드를 제공한다. 이로 인해 종이 영수증과 전자 데이터를 검증할 수 있다.
- 투표 내용 : 자신이 선택한 투표의 내용이 그대로 프린트됨으로 인해 유권자는 투표내용을 검증하기 쉽도록 하였다. 또한 선택한 내용과 앞에 코드 두 개가 일치하도록 하여 선택한 내용이 올바른 것임을 검증하도록 하였다.

이 방식은 투표내용을 그대로 출력함으로써 유권자는 쉽게 자신의 투표 내용을 확인 할 수 있으며, 전자적으로 저장되는 데이터와 동일한 정보를 가지고 있는지 매칭할 수 있는 방안을 제공해주고 있다.

ㄴ. VVPB

VVPB(Voter Verified Paper Ballots)로 notablesoftware.에서 제공하는 것으로 이와 같은 기술이 나오게 된 이유는 물리적인 하드웨어나 소프트웨어는 외부의 위험이 존재한다. 이와 같은 위험으로부터 투표의 결과를 검증하거나 안전한 방안으로 제공될 수 있는 방안이다. 그러므로 투표의 내용을 프린트하여 보관하는 기술로 나오게 되었다. VVPAT기술과 유한 기술로 분류될 수 있다. VVPB에서 사용되는 정의된



〔그림 6〕 AccuPoll사의 VVPAT의 종이 영수증

기술은 다음과 같다.

- 바코드 : 컴퓨터에서 처리될 수 있는 데이터 이미지를 출력한다.
- 투명한 창 : 투표용지에 출력되는 내용을 볼 수 있는 장소로써 유권자가 투표한 내용이 프린트되어 나오는 용지를 유권자가 확인한다.
- 터치스크린 : 유권자가 투표 내용을 보고 클릭할 수 있는 스크린으로 유권자가 투표하는 기기로 이용한다.
- 프린트 기기 : 유권자가 선택한 내용을 프린트하는 것으로 투명한 창안에서 프린트하여 출력한다. 이때 유권자는 출력되는 내용을 창을 통해 확인 할 수 있으며 잘못된 내용이 출력되면 다시 투표를 한다.
- VVPB : 인쇄되는 투표용지를 말하며 투표함에 자동적으로 투입된다.

4.3.2 암호화된 투표 메시지 내용을 출력하는 영수증 기술

전자 투표 기기에서 출력되는 내용이 암호화된 것으로 각각의 메시지가 암호화된 것을 출력하는 것이다. 이와 같은 방식은 유권자의 투표 값에 서명한 것을 출력해서 제공하거나 암호화 값을 프린트해서 제공하는 것이다. 이와 같은 방식은 기존의 암호화한 내용을 프린트하면 된다 하지만 암호화된 내용이 각각의 유일한 값이 되거나 유추가 가능하지 않도록 되어야 한다.

대표적인 방식으로 David Chaum의 SRTI방식(Secret-ballot Receipt and Transparent Integrity)은 투표의 결과를 두 개의 종이에 나누어 프린트하도록 하였다. 두 개로 표현하는 방법으로 상위

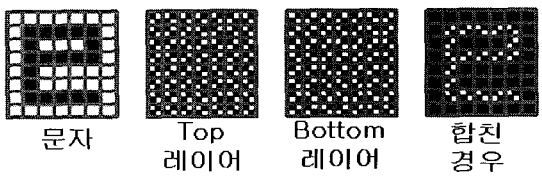
(Top)레이어와 하위(Bottom)레이어를 이용하였고 한 문자를 표현하는데 있어 상위와 하위 레이어를 합치면 하나의 문자를 볼 수 있다.[1,2](그림 7 참조)

이와 같은 프린트를 제공하기 위해서는 다음과 같은 수식을 이용한다.

$$R^t \oplus W^b = B^t$$
$$R^b \oplus W^t = B^b$$

위의 수식은 XOR을 이용하여 각각의 적색과 백색이 겹치거나 겹치지 않도록 출력하는 방법을 제시하였다. R은 붉은색을 W는 흰색을 B는 겹친 색을 나타내며, t는 상위 레이어로 b는 하위 레이어를 표시한다. 위의 수식으로 인해 상위 레이어와 하위 레이어에 프린트 될 색이 정해진다. 프린트되는 수식이 4개를 하나의 마크로 보면 다음과 같이 확장된다.

$$L^t_{i,2j-(i \bmod 2)} = R^t_{ij}$$
$$L^t_{i,2j-(i+1 \bmod 2)} = W^t_{ij}$$
$$L^b_{i,2j-(i+1 \bmod 2)} = R^b_{ij}$$
$$L^b_{i,2j-(i \bmod 2)} = W^b_{ij}$$



〔그림 7〕 문자 표현 방법

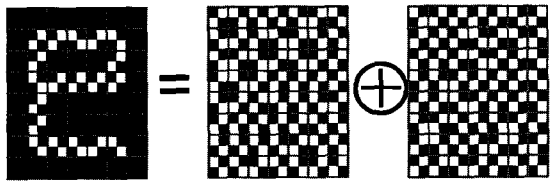
여기서 i, j는 행렬을 표시하며, L은 각 내용의 프린트 값이 된다. 그럼으로 프린트 값이 출력되면 이에 따른 색이 정해지고 각각의 행과 열값으로 인해 프린트 된다. 영수증에 프린트 되는 값으로는 투표에서 사용한 임의 선택 값과 각각의 신뢰기관의 공개키로 암호화 된 값, 그리고 서명 값이 된다. 암호화 된 값을 상위와 하위 레이어로 프린트하여 하나는 버리고 다른 하나는 유권자가 선택하여 보관하게 된다. 이때 유권자가 보관하는 투표용지는 암호화된 값의 나머지 반(상위 혹은 하위 레이어)으로 보이기 때문에 어떠한 값인지는 알 수 없게 된다. 하지만 검증 과정에서는 나머지 반을 사용자가 신뢰기관 혹은 검증기관에 제공함으로 인해서 나머지 반을 저장하고 있는 신뢰기관 혹은 검증기관 데이터에서는 검증이 가능하다. 이 기술에서는 투표의 내용을 그대로 프린트하는 것이 아니고 암호화 된 값을 프린트함으로써 보관하는 영수증에서 어느 후보자를 선택하였는지 알 수 없으며, 각각의 데이터가 무엇인지 알 수 없도록 하였다.

ㄱ. Subtractive System

종이 영수증 기술로 David Chaum의 기술을 적용한 것으로 두 개의 레이어를 이용하는 것으로 그림 8을 참조하기 바란다. 하지만 이와 같은 기술을 구현하기 어려우면 동시에 두 개의 레이어를 보더라도 확인하기 어렵다. 그럼으로 개표 과정에 있어서도 확인이 어려운 취약성이 있다.

ㄴ. Additive System

종이 영수증 기술로 동일하게 사용되나 투표 이후 영수증의 레이어를 광학 기기를 통해서 합성할 수 있으며 합성하면 유권자가 선택한 후보가 된다. 이는 프린트되는 기술은 그림 9와 동일하다. 이와 같은 방식은 투표 방식은 유권자의 투표한 내용을 확인하기 용이하다는 것이다.



〔그림 8〕 Subtractive System의 예시

〔그림 9〕 Additive System의 예시

V. 결 론

전자 투표 시스템은 국민의 여론을 방영하는 것으로써 투표의 결과나 투표의 내용에 있어 비밀성을 제공하며, 보안 사항을 만족 시켜야 한다. 본 내용에서는 전자 투표 시스템에서 보안 기술에 대하여 알아보면,

각각의 적용 방식에 대하여 알아보았다. 유권자의 투표 내용에 제공하는 보안 기술은 공개키부터 시작해서 비밀 분산, 영 지식 증명, 은닉 서명, 준동형 암호화, 믹스넷 등 다양한 기술을 이용하고 있다. 그 중에 본고에서는 은닉 서명, 믹스넷, 준동형 암호화 및 부가적인 기술로 종이 영수증 기술에 대하여 알아보았다. 유권자의 익명성을 제공하면 동시에 믹스넷을 이용하여 익명 채널을 구성한다. 이와 같이 보안 기술을 두 가지 이상 접목하여 보다 안전한 시스템을 구성할 수 있다. 다음의 표 1을 보고 보안 기술을 참조하기 바란다.

종이 영수증 기술은 전자 투표 기기에 있어 부가적인 장치이지만 역할로는 감사 자료 및 검증 자료로 이용될 수 있다. 전자 투표 시스템의 동향을 보면 보안 요구 사항을 만족시키기 위해서는 은닉서명과 믹스넷 채널을 이용하고 있으며, 동시에 개표에 대한 효율성을 제공하기 위해서는 준동형 암호화 방식을 적용해야 한다.

향후 전자 투표 시스템은 독립기기인 1단계인 지정된 투표소에서 하는 것과 2단계의 임의 투표소에서 투표하는 방향으로 발전할 것이며, 최종적으로 3단계인 유권자가 어디서나 자신의 단말기를 이용하여 투표 하는 것이다. 이와 같이 각각의 사항이 변함으로 전자 투표의 보안 요구 사항도 추가되거나 변경될 것이다. 이에 따른 보안 기술 또한 더욱 필요하게 될 것이며, 안전하게 투표값을 검증할 수 있어야 한다. 종이 영수증 기술은 유권자가 신뢰 있게 투표 값을 검증할 수 있는 방안이 될 수 있으며, 앞서 말한 것과 같이 감사 자료로 이용될 수 있다. 그러나 종이 영수증 기술을 적용하는 경우 제일 주의할 것으로는 매표가 불가능해야 한다. 이와 같은 취약성을 보안하기 위하여 보안 기술 및 종이 영수증 기술에 대한 지속적인 연구가 필요하다.

참 고 문 헌

[1] David Chaum, "Secret-Ballot Receipts and Transparent Integrity," Courtesy advance draft, 2002, 3

[2] David Chaum, "Secret Ballot Receipts: True Voter-Verifiable Elections," RSA Laboratories, volume 7, no.2, 2004

[3] D.Boneh and P.Golle, "Almost entirely correct mixing with application to voting," In ACM conference on Computer and Communication Security 2002

[4] Donald P.Moynihan, "Building Secure Elections: E-Voting, Security and Systems Theory," ABI/INFORM Global, 2004. 9

[5] Dennis Vadura, Frank Wiebe, what is

[표 1] 각 기술 비교 표

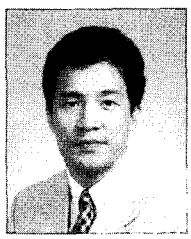
보안 기술		비밀성	익명성	검증성	매표방지	비 고
은닉 서명	An untraceable, universally verifiable voting scheme	제공	제공	제공	제공	투표값이 독립적 (공개키 기반)
	Ballot-Cancellation Protocol of E-voting Based on Two Independent Authorities	제공	제공	제공	미제공	투표값이 은닉값에 의존 (공개키 기반)
믹스넷	Receipt-Free Mix-Type Voting Scheme	제공	제공	미제공	제공	중간 검증값이 필요 (공개키 기반)
	Almost Entirely correct Mixing With Applications to Voting	제공	제공	제공	제공	믹스넷 중간에 검증 가능 (공개키 기반)
	An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness	제공	제공	제공	제공	믹스넷에서 중간에 검증 가능 (공개키 기반)
준동 암호화	Multiplicative Homomorphic E-Voting	제공	제공	미제공	제공	곱의 준동형 암호화 방식 (공개키 기반)
	Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots	제공	제공	제공	제공	합의 준동형 암호화 방식 (공개키 기반)
종이 영수증 기술	VVPAT	보안 기술은 시스템에서 제공 (데이터와 연결할 수 있는 바코드 생성)				유권자의 표를 그대로 프린트 (투표함에 제출)
	Subtractive System	보안 기술은 시스템에서 제공 (공개키 기반 및 서명 제공)				유권자의 표를 암호화하여 출력 (특정 방식적용)
	Additive System	보안 기술은 시스템 (공개키 기반 및 서명 제공)				유권자의 표를 암호화하여 출력 (특정 방식적용)

a meaningful "Voter Verified Paper Audit Trail?", 2003. 12
[6] Kun Peng, Riza Aditya, Colin Goyd, Ed Dawson and Byoungcheon Lee, "Multiplicative Homomorphic E-Voting," INDOCRYPT 2004, Volume 3348, p.61, 2004.
[7] Margaret McGaley, J. Paul Gibson, "Electronic Voting: A Safety Critical System," Technical Report, NUIM-CS-TR2003-02, 2003. 3
[8] Michael Ian Shamos, "Paper v. Electronic Voting Records-An Assessment," electiontech.org, 2004. 4
[9] Michael J.Radwin, "An untraceable, universally verifiable voting scheme," 1995.
[10] Safevote, "Voting System Requirements", Safevote, Inc. and The Bell, 2001. 2
[11] Sako, Kazue and Kilian, Joe, "Receipt-free Mix-Type voting Scheme: A Practical Solution to the Implementation of a Voting Booth," EUROCRYPT'95, vol 921, Lecture Notes in Computer Science, pp.393-403, Springer-Verlag, 1995
[12] Susan King Roth, "Disenfranchised by design: voting systems and the election process," Information design Journal, vol.9, no.1, 1998
[13] Pedro A.D. Rezende, "Electronic Voting Systems-Is Brazil Abead of its Time?," RSA Laboratories, Volume7, no.2, 2004
[14] Rixa Aditya, byoungcheon Lee, Colin Boyd and Ed Dawson, "An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness," TrustBus 2004, LNCS 3184, pp. 152-161, 2004.
[15] Wen-shenq Juang, Student Member and Chin-Laung Lei, "A Secure and Practical Electroni Voting Scheme for Real World Environments", IEICE TRANS. FUNDAMENTALS
[16] Yong-Sork HER and Kouichi SAKURAI, "Ballot-Cancellation Protocol of E-voting Based on Two Independent Authorities," the, XIII ACME International conference on Pacitic Rim Management.
[17] http://accupoll.com, AccuPoll
[18] http://www-db.stanford.edu/pub/keller/2004/electronic-voting-machine.pdf Arthur Keller, "A PC-Based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot"
[19] http://realex.nist.gov/conferences/voting/dayone/session2.3/index.htm, David Dill. NIST Voting Standards Symposium, 2003. 12
[20] http://citeseer.ist.psu.edu/cache/papers/cs/31785, Ronald L. Rivest, "Electronic Voting"
[21] http://theory.lcs.mit.edu/~cis/theses/DuRette-bachelors.pdf Brandon William DuRette, "Multiple Administrators for Electronic Voting"
[22] http://votehere.net, VoteHere
[23] http://verifiedvoting.org, VerifiedVoting

〈著 者 紹 介〉

강 서 일 (Kang Seo Il)
학생회원

2003년 2월 : 순천향대학교 정보기술 공학부 졸업
2004년 6월~2005년 2월 : 순천향대학 교 전산학과 석사
2005년 3월~현재 : 순천향대학교 전산학과 박사 과정
〈관심분야〉 전자 투표, 전자 화폐, 전자 상거래



이 임 영 (Lee Im Yeong)
종신회원

1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학전공 석사
1989년 3월 : 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재 : 순천향대학교 정보기술공학부 교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안