情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

전자투표 시스템을 위한 효율적인 믹스넷*

전 웅 렬,[1†] 이 윤 호,[2] 원 동 호[1‡]
[1]성균관대학교, [2]광주대학교

An Efficient Mixnet for Electronic Voting Systems*

Woongryul Jeon,[1†] Yunho Lee,[2] Dongho Won[1‡]
[1]Sungkyunkwan University, [2]Gwangju University

요 약

2010년, Sebe 등은 원격 투표에 사용할 수 있는, 가벼우면서도 효율적인 믹스넷 방식을 제안하였다. 이 방식은 암호학적 해쉬연산 만을 이용하기 때문에 기존 방식처럼 복잡한 영지식증명(zero-knowledge proofs)이 필요없이 간단하면서도 믹스넷의 동작을 효율적으로 증명할 수 있는 장점이 있다. 본 논문에서는 Sebe 등이 이용한 가정 사항을 그대로 유지하면서 보다 효율적인 믹스넷을 제안한다.

ABSTRACT

In 2010, Sebe et al. proposed an efficient and lightweight mixnet scheme for remote voting systems. The scheme based on a cryptographic secure hash function, does not require complex and costly zero-knowledge proofs of their correct mixing operations, thus they claimed that their scheme is simple and efficient. In this paper, we propose more efficient and fast mixnet scheme than Sebe et al.'s scheme under the same assumption.

Keywords: e-Voting, Mix-net, ElGamal Encryption

I. 서 론

전자투표는 선거의 준비, 투표, 투표 결과의 집계 과정에 전자적인 기술을 도입하여 선거를 진행하는 것의 총칭이다. 전자투표가 현행 종이투표와 동일한 효력을 발휘하기 위해서는 전자투표 또한 선거의 4대원칙을 준수해야 한다. 선거의 4대 원칙은 아래 〔표 1〕과 같다[1].

보통선거와 평등선거의 원칙은 온라인에서도 보장하기가 어렵지 않다. 그러나 직접선거와 비밀선거는 조금 까다롭다. 직접선거와 비밀선거의 원칙이 지켜지기 위해서는 현행 종이투표 방식과 같이 물리적으로 격리된 투표공간이 필요한데, 이는 결국 시간적, 공간적 제한을 유발하기 때문이다. 이에 전자투표 또한 투

〔표 1〕 선거의 4대 원칙

원칙	설명
보통선거	- 성별, 학력, 재산의 많고 적음에 관계없이 일정한 나이가 된 모든 성인에게 선거권과 피선거권을 부여함을 보장하는 원칙
평등선거	- 모든 투표자의 표가 동일한 가치와 효력을 발휘하는 것을 보장하는 원칙
직접선거	- 선거권자가 직접 투표에 참여하는 것을 보장하는 원칙
비밀선거	- 선거권자가 투표에 참여하여 어느 후보를 선택하였는지를 유권자 본인만 알 수 있도록 보장하는 원칙

접수일(2011년 7월 4일), 수정일(2011년 11월 2일), 게재확정일(2011년 11월 7일)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2011-0026023).
† 주저자, wrjeon@security.re.kr
‡ 교신저자, dhwon@security.re.kr

표가 시행되는 장소를 중심으로 투표소 투표 방식(Poll Site Voting)과 원격 투표 방식(Remote Voting)으로 구분할 수 있다.

투표소 투표 방식은 일반적으로 DRE(Direct Recording Electronic) 시스템을 이용한다. 유권자가 DRE 시스템을 이용하여 투표를 하면 이를 전자적으로 기록하여 서버에 전송하고, 서버에서는 투표결과를 고속으로 집계하는 방식이다. 투표소 투표 방식의 전자투표는 현행 종이투표 방식에 비해 여전히 시간적, 공간적 제약사항을 포함하지만, 물리적으로 유권자를 안전하게 인증할 수 있고, 투표소가 기밀성을 보장할 수 있기 때문에 직접선거와 비밀선거의 원칙을 보장할 수 있는 장점이 있다. 이러한 방식의 전자투표는 현재 미국의 여러 주(州)에서 도입하여 시행하고 있다.

원격 투표 방식은 유권자에게 시간적, 공간적 제약을 두지 않는다. 유권자는 모바일, 인터넷, 휴대폰 등 다양한 수단을 통해 원격에서 투표가 가능하다. 그러나 이 경우 유권자에 대한 인증문제, 유권자의 매표가능성, 비밀선거의 원칙이 훼손될 가능성이 농후하기 때문에 섣불리 도입하기가 어렵다. 이러한 문제들은 기술적으로 해결되는 것이 아니기 때문에 사회적인 합의가 필요한데, 에스토니아에서 2005년에 세계 최초로 인터넷을 이용한 전자투표를 시행한 바가 있다.

DRE를 사용하는 전자투표 방식의 신뢰성 문제는 두 가지로 구분할 수 있다. 첫 번째는 Cast-as-Intended로 유권자가 투표기를 통해 투표를 하는 과정에 대한 신뢰성을 의미한다. 투표기는 공격 가능한 기기로 유권자의 투표값을 조작하여 기록할 가능성이 있다. 따라서 전자투표 방식은 이러한 공격에 대응하고 투표기의 신뢰성을 보장할 수 있는 방안을 마련해야 한다.

두 번째는 Counter-as-Cast로 집계과정에서 투표값들이 모두 공정하게 반영되는 것을 의미한다. 투표기가 투표값을 공정하게 기록했다해도, 집계과정에서 누락이 되거나, 투표값을 추적할 수 있으면 전자투표를 신뢰할 수 없다. 따라서 기록된 투표값이 빠짐없이 집계되고 있으며, 또 비밀선거의 원칙에 의거, 투표값으로부터 유권자를 추적할 수 없음을 보장해야 한다.

첫 번째, Cast-as-Intended의 경우 영수증을 발급하는 방법을 통해 신뢰성을 보장할 수 있다. 2002년 D.Chaum은 투표소 투표 방식의 전자투표 방식을 발표하였는데, 이 방식은 Visual Cryptography를 이용한 것으로, 특수한 용지 두 장을 겹쳐야 실제 투표값을 확인할 수 있는 형태였다[2,3]. 유권자는 두 장의 용지 중 한 장을 영수증으로 갖는다. 그러나 투표를 위해 특수한 용지와 특수한 프린터가 필요하다는 것이 단점으로 지적되었다. 이에 2003년 A.C.Neff는 코드북을 이용한 전자투표 방식을 제안하였다[4]. 그러나 Neff의 방식은 사전에 수많은 투표값을 미리 생성해야 하고, 코드북의 관리자를 신뢰해야 하는 단점이 있었다. 이후 2005년에 P.Ryan은 Pret a Voter라는 새로운 전자투표 방식을 제안하였다[5]. Pret a Voter는 현행 종이투표 방식과 매우 유사한 전자투표 방식으로 사용자에게 거부감 없이 친숙하게 다가갈 수 있다는 점이 가장 큰 장점이었다. 또 비용적인 측면 역시 현행 종이투표와 유사한 수준으로 기존에 발표된 연구에 비해 진보한 모습을 보여주었다. 그러나 후보자의 순서가 투표지마다 무작위로 변경되기 때문에 잘못 기표할 수 있다는 단점이 있었다. 이후 2010년, D.Chaum의 장점과 P.Ryan의 장점을 혼합한 형태의 전자투표 방식이 Lee에 의해 발표되었으며[6], 최근에는 Scantegrity라는 주제로 다양한 영수증 발급 방식의 전자투표가 연구되고 있다[7].

두 번째, Counter-as-Cast는 믹스넷을 통해 신뢰성을 보장할 수 있다. 믹스넷(Mixnet)[8-10]은 1981년 David Chaum에 의해 소개된 방법으로 입력값과 출력값 사이의 연결 정보를 알 수 없도록 섞는 기술이다. 믹스넷은 일반적으로 다수의 믹스서버로 구성이 되는데, 각각의 믹스서버는 초기 입력값 또는 이전 믹스서버의 출력값을 입력받아 섞는 과정을 반복한다. 이 때 각 믹스서버는 자신의 동작이 올바름을 증명해야 하는데, 증명방법으로는 일반적으로 영지식 증명방법이 많이 사용된다. 그러나 영지식 증명방법은 연산량이 많고 증명과정이 복잡하기 때문에 효율적이지 못하다는 단점이 있다[11-17].

2010년 Sebe 등은 다수의 믹스서버 가운데 최소한 하나의 믹스서버가 정직하다는 가정 하에 믹스 과정의 신뢰성을 증명하기 위한 방식을 제안하였다. Sebe가 제안한 믹스서버의 증명 방식은 기존 영지식 증명방식과는 달리 매우 단순하여 효율성을 향상시킨 장점이 있다[18]. 본 논문은 2010년 발표된 Sebe의 논문을 중심으로 믹스넷의 안전성 증명방식을 살펴보고, Sebe의 믹스넷 안전성 증명방법에서 효율성을 향상시킨 새로운 믹스넷의 증명방식을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 믹스넷과 관련한 배경 지식을 설명하고 3장에서는 Sebe 등이 제안한 믹스넷 증명방식을 설명한다. 그리고 4장에

서는 본 논문이 제안하는 새로운 믹스넷 방식을 설명하고, 마지막으로 5장에서 결론을 맺는다.

II. 관련연구

2.1 믹스넷

유권자가 전자투표를 신뢰하기 위해서는 우선 유권자의 투표가 집계에 정확히 반영되었음을 확인할 수 있어야 한다. 그러나 유권자의 투표 결과를 제 3자가 확인할 수 있어서는 안된다. 왜냐하면 유권자가 매표를 할 가능성이 있기 때문이다. 따라서 전자투표는 유권자에게 투표에 대한 신뢰성을 제공하되, 유권자가 투표 결과를 제 3자에게 증명하게 해서는 안된다. 믹스넷은 바로 이러한 요구사항을 충족시키기 위한 기술이다.

믹스넷은 1981년 David Chaum에 의해 소개된 방법으로 입력값과 출력값 사이의 연결 정보를 알 수 없도록 섞는 기술이다. 일반적으로 믹스넷은 다수의 믹스서버로 구성이 된다. 각각의 믹스서버는 초기 입력값 또는 이전 믹스서버의 출력값을 입력으로 받아 섞는 과정을 반복한다. 이때 믹스서버가 믹스를 올바르게 수행하였음을 확인할 수 있어야 하는데, 일반적으로 영지식 증명, RPC(Randomization Parity Check)을 많이 사용한다. 투표 결과는 믹스넷을 통과하고 나면 무작위로 섞여서 어떤 유권자가 어떤 값을 투표했는지 확인할 수 없게 된다. 따라서 유권자가 투표 결과를 제 3자에게 증명하는 것이 불가능하다.

그러나 전체 유권자의 수가 어마어마하게 큰 숫자이며, 영지식 증명은 계산량이 많기 때문에 다른 전자투표 과정에 비해 비효율적이라는 단점이 있다.

2.2 ElGamal 암호 알고리즘

ElGamal 암호 알고리즘은 이산대수 문제를 기반으로 하고 있다. 이산대수 문제란 큰 소수 p로 만들어진 집합 Z_p 상에서의 원시원소를 g라고 할 때, $g^x = y \bmod p$의 g값과 y값을 알고 있어도 $\log_g y = x \bmod (p-1)$을 구하는 것이 어렵다는 문제이다. 물론 g와 x를 아는 사람이 y를 계산하는 것은 간단하다.

ElGamal 암호 알고리즘은 우선 큰 소수 p를 선정하여 Z_p상의 원시원소 g와 함께 p를 공개한다. 사용자 A는 Z_p 상의 임의의 원소 x_A를 비밀정보로 선택하여, $y_A = g^{x_A} \bmod p$를 계산한다. 사용자 B 역시 마찬자기로 Z_p 상의 임의의 원소 x_B를 선택하여 동일한 방법으로 y_B를 계산한다. 이 때 y_A와 y_B가 바로 사용자 A, B가 선택한 공개키가 되고, x_A와 x_B가 개인키가 된다.

암호화 과정은 다음과 같다. 사용자 A가 평문 m을 암호화하여 사용자 B에게 전송하고자 할 때, A는 Z_p 상에서 임의의 난수 r을 선택하여 암호문 $(c, d) = (g^r, y_B^r m)$을 계산하고, 이를 전송한다.

복호화 과정은 다음과 같다. 사용자 B는 우선 암호문 c에 자신의 비밀키 x_B를 누승하여 $K = c^{x_B} \bmod p$를 계산하고, 이를 이용하여 평문 $m = d / K \bmod p$ 을 복호화 할 수 있다.

ElGamal 암호 알고리즘은 두 가지 중요한 특성을 지니고 있다. 첫 번째는 준동형성(Homomorphic Property)인데, 이는 암호문에 대한 연산이 평문에 대한 연산으로 대응하는 성질을 말한다. 두 번째 특징은 재암호화(Re-encryption Property)로 암호문 (c, d)에 새로운 난수 r'을 사용하여 새로운 암호문 $(c', d') = (cg^{r'}, dy^{r'})$을 생성할 수 있다.

덧붙여 ElGamal 암호 알고리즘은 비밀키를 공개하지 않고도 복호화 과정을 검증할 수 있는 방법을 제공한다. ElGamal 암호 알고리즘은 앞서 언급한 바와 같이, $(c, d) = (g^r, yr^m)$으로 계산되는데, 만약 $(g, c, y, \frac{d}{m})$이 주어지면, 개인키에 대한 정보가 없어도 정확히 복호화되었음을 확인할 수 있다. 이를 CP(Chaum-Pederson's proof) tuple이라고 한다.

2.3 타원곡선 암호 알고리즘

타원곡선 암호 알고리즘은 타원곡선 이산대수 문제에 기반하고 있는 암호 알고리즘이다. 만약 $GF(p)$를 p개의 원소로 구성된 유한체라고 하면, 타원곡선 위의 점 P의 위수 t는 $tP = O$를 만족하는 가장 작은 정수 t로 정의된다. $GF(p)$상에서 정의된 타원곡선과 점 Q, 그리고 위수가 t인 타원곡선 위의 점 P가 주어졌을 때, $Q = xP$를 만족하는 정수 x를 구하는 것을 타원곡선의 이산대수 문제라고 한다. 이 때 x를 구하는 가장 쉬운 해결방법은 Q를 구할때까지 P, $2P$, $3P$ 등 연속적으로 덧셈을 수행하는 것이지만 t가 무척 큰 경우에는 시간이 매우 오래 걸린다. 타원곡선 암호 알고리즘은 상대적으로 다른 암호 알고리즘에 비해 짧은 키를 사용하기 때문에 효율성이 우수하다. 따라서 최근 다

양한 표준에 타원곡선 암호 알고리즘을 적용하기 위한 노력이 이루어지고 있다. 실제 512비트의 키를 사용하는 타원곡선 암호 알고리즘과 동일한 수준의 안전성을 보장하기 위해 RSA 암호 알고리즘은 약 15,000 비트의 키를 사용해야 한다.

III. Sebe의 믹스넷 방식

Sebe 등은 2010년 해시함수를 이용한 새로운 믹스넷 방식을 제안하였다. Sebe가 제안한 방식은 해시함수를 기반으로 동작하기 때문에 기존 영지식 증명 방식에 비해 연산량이 적다는 장점이 있다. 본 장에서는 Sebe의 믹스넷 방식에 대해 살펴본다. Sebe는 ElGamal 암호 알고리즘을 사용하여 투표값을 암호화하는 것을 가정하였다. 이는 앞서 언급했듯이 ElGamal 암호 알고리즘의 재암호화 특성에 의한 것이다. 다음은 본 논문에서 사용할 표기를 나타낸다.

- TP : 신뢰된 파티
- x : TP의 개인키
- y : TP의 공개키($y = g^x \bmod p$)
- λ : 믹스서버의 개수
- ME_i : i번째 믹스서버
- n : 유권자의 수
- P_j : j번째 유권자
- C_j : j번째 유권자의 암호화된 투표값
- π : 순열

3.1 Setup

TP는 개인키 x를 선택하고, 공개키 $y = g^x \bmod p$를 계산한다. 또 TP는 타원곡선 상의 점 P에 대해 xE를 선택하고 $QE = xEP$를 계산한다. 마지막으로 TP는 g, y, p, QE, P를 공개한다.

3.2 Voting

우선 유권자 P_j는 투표값 v_j를 결정하고 이를 공개키 QE로 암호화한다($V_j = E_{QE}(v_j)$). 그리고 유권자는 암호화된 투표값에 대한 해시값 $h_j = h(V_j)$를 계산한다. 마지막으로 유권자는 b_j를 선택하고, 이를 바탕으로 자신의 메시지 $m_j = V_j \| h_j \| b_j$를 생성한다. 여기서 m_j는 Z_p^*상에서 이차잉여다.

이제 유권자는 자신의 메시지 m_j를 공개키 y를 사용하여 암호화하여, 암호문 $C_j = (c_j, d_j)$를 얻는다. 유권자 P_j의 메시지에 대한 암호문은 전자서명이 첨부된 후 공개게시판에 공개된다. 전자투표 과정에 참여하는 정당한 사용자는 암호문의 무결성을 전자서명을 통해 검증할 수 있다.

3.3 Vote Mixing

선거가 완료되고 나면 TP는 아래 단계를 걸쳐 투표결과를 섞는다. 각 단계는 다음과 같다.

1. TP는 투표값의 무결성을 확인하기 위해 C_{check}를 다음과 같이 계산한다.
   $C_{\text{check}} = \prod_{j=1}^{n} C_j = (\prod_{j=1}^{n} c_j, \prod_{j=1}^{n} d_j)$
2. 첫 번째 믹스서버 ME_1는 ElGamal 암호 알고리즘을 사용하여 s개의 더미 평문 m_i' ($1 \le i \le s$)에 대한 암호문 집합 $E' = \{ e_1', e_2', \dots, e_s' \}$를 무작위로 생성한다. 따라서 총 암호문의 개수는 $n + s$개가 된다.
3. ME_1은 더미 평문의 해시값 $H_1 = \{ h(m_1'), \dots, h(m_s') \}$를 계산하여 공개한다.
4. ME_1은 더미 암호문을 포함한 전체 암호문 $\{ C_j \}_{1 \le j \le n+s}$를 난수 r_j'을 사용하여 재암호화하고, 암호문의 순서를 무작위 순열 π_1을 사용하여 뒤섞는다. 그리고 이렇게 생성한 $C_{j\ 1 \le j \le n+s}'$을 다음 믹스서버에 대한 입력값으로 전달한다.
5. 이후의 믹스서버들은 2번부터 4번까지의 과정을 반복한다.

Sebe의 믹스넷 방식에서 믹스서버의 역할은 크게 3단계로 정리할 수 있다. 첫째, 믹스서버는 입력값에 대해 s개의 평문을 추가한다. 이때 추가된 s개의 평문의 해시값은 공개게시판에 공개된다. 둘째, 믹스서버는 확장된 집합 전체를 대상으로 새로운 난수를 사용하여 재암호화를 한다. 셋째, 믹스서버는 재암호화된 암호문을 무작위로 재배치한 후, 다음 믹스서버의 입력값으로 전달한다.

따라서 마지막 믹스서버 ME_λ는 H_λ와 $C_{j\ 1 \le j \le n+\lambda s}'$를 공개게시판에 게시한다.

3.4 Vote Opening

모든 믹스서버가 연산을 종료하고 나면, *TP*는 다음 과정을 통해 개표를 진행한다.

1. *TP*는 암호문 $C_j' = (c_j', d_j')$를 자신의 비밀키 x로 복호화하고, 복호화한 평문 $\{m_j\}_{1 \le j \le n+\lambda s}$를 공개게시판에 공개한다.
2. *TP*는 다음을 만족하는 평문 m_j'를 복호화한 평문의 목록에서 제거한다. 본 과정의 목적은 믹스서버가 임의로 추가한 더미평문 λs개를 제거하는 것이다.
   $h(m_j') \in H_i$
3. *TP*는 C_{check}를 복호화하고, 복호화된 평문 m_{check}의 신뢰성을 증명하기 위해 CP tuple $(g, C_{\text{check}}, y, \frac{d_{\text{check}}}{m_{\text{check}}})$을 공개한다. 전자투표에 참여하는 모든 구성원은 공개값을 이용하여 개표과정의 신뢰성을 검증할 수 있다.
   - $m_{\text{check}} = \prod_{j=1}^{m} m_j'$를 충족하는지 확인
   - $h_j' = h(V_j')$를 충족하는지 확인

믹스과정에서 λs개 만큼의 더미 평문을 추가했기 때문에 개표과정에서는 이를 제거해야 한다. 제거하는 방법은 더미 평문을 추가하면서 믹스서버가 공개한 H_i 값을 이용하는 것이다. 이를 통해 더미 평문만 선별적으로 제거할 수 있다.

3.5 효율성 분석

Sebe는 최소한 하나의 믹스서버는 정직하다는 가정을 기반으로 본 방법을 제안하였다. 만약 i번째 믹스서버가 유일하게 정직한 믹스서버이고, 다른 믹스서버는 믹스를 올바르게 수행하지 않는다해도, π_i의 기밀성이 보장되기 때문에, 믹스넷의 출력값과 입력값의 연관관계를 유추하는 것은 불가능하다.

그러나 Sebe의 믹스넷 방식은 오버헤드가 많다는 단점이 있다. Sebe의 방식은 λ개의 믹스서버가 각각 s개의 더미 암호문을 추가하기 때문에 총 λs개의 더미 평문이 추가되며, 이 때 λs개에 대한 해시 연산이 추가된다. 개표과정에서는 각 믹스서버가 추가한 더미 평문을 제거하기 위해 총 $(n+\lambda s)\lambda s$번의 비교연산이 필요하다.

이에 본 논문에서는 Sebe의 가정사항을 그대로 유지하면서, 효율성을 향상시킨 새로운 믹스넷 방식을 제안한다.

IV. 새로운 믹스넷 방식

본 장에서는 Sebe의 믹스넷 방식을 개선한 새로운 믹스넷 방식을 제안한다. Setup 과정과 Voting 과정은 Sebe의 방식과 동일하고, Vote Mixing 과정과, Vote Opening 과정에는 개선사항이 적용되어 효율성이 향상되었다.

기존 Sebe의 믹스넷 방식은 λ개의 믹스서버가 각각 s개의 더미 평문을 추가하도록 설계되어 있었다. 이는 믹스넷의 신뢰성을 보장하는데 유용하지만, 반대로 오버헤드가 크게 증가하는 단점도 있었다. 이에 본 논문에서는 첫 번째 믹스서버만 s개의 더미 평문을 추가하고, 나머지 믹스서버는 1개의 값만 추가하는 형태의 믹스넷 방식을 제안한다.

본 방식은 Sebe의 방식에 비해 효율성을 개선하면서도, 유사한 수준의 안전성을 보장할 수 있다. 변경사항에 대한 자세한 설명은 다음 장에서 진행한다.

4.1 Vote Mixing

선거가 완료되고 나면 *TP*는 아래 단계를 걸쳐 투표결과를 섞는다. 각 단계는 다음과 같다.

1. *TP*는 투표값의 무결성을 확인하기 위해 C_{check}를 다음과 같이 계산한다.
   $C_{\text{check}} = \prod_{j=1}^{n} C_j = (\prod_{j=1}^{n} c_j, \prod_{j=1}^{n} d_j)$
2. 첫 번째 믹스서버 ME_1는 ElGamal 암호 알고리즘을 사용하여 s개의 더미 평문 $m_i'(1 \le i \le s)$에 대한 암호문 집합 $E' = \{e_1', e_2', \dots, e_s'\}$를 무작위로 생성한다.
3. ME_1은 더미 평문의 해시값 $H_1 = h(m_1'), \dots, h(m_s')$를 계산하여 공개한다.
4. ME_1은 전체 암호문 $\{C_j\}_{1 \le j \le n}$을 난수 r_j'를 사용하여 재암호화하고, 무작위 순열 π_1, π_1'을 선택하여, 재암호화한 암호문을 순열 π_1을 이용하여 암호문을 재배치한다. 그리고 임의의 난수 $k_1 (1 \le k_1 \le n)$을 선택하여 새로운 더미 암호문 집합 $E' = \pi_1'(E \cup \{C_{k_1}\})$과 $\{C_j\}_{1 \le j \le n, j \ne k_1}$

를 생성한다.

5. ME_1은 $h(C_{k_1})$를 공개게시판에 공개하고 난수 r_j''을 사용하여 E'를 재암호화한다. 그리고 다음 믹스서버로 E'과 $\{ C_j \}_{1 \le j \le n, j \neq k}$를 전달한다.
6. 이후의 믹스서버는 4번과 5번 과정을 반복한다. 마지막 믹스서버 ME_λ는 총 $n-\lambda$개의 투표값 암호문과 $s+\lambda$개의 더미 암호문을 출력값으로 공개게시판에 공개한다.

본 논문에서 제안하는 새로운 믹스넷 방식은 각 믹스서버가 두 개의 암호문 집합을 입력받고 출력하는데, 하나는 익명성을 보장하기 위해 무작위로 뒤섞는 투표값의 암호문 집합이고, 다른 하나는 믹스서버의 동작을 증명하기 위한 암호문 집합이다.

다만 일반적인 믹스서버의 증명이 자신의 믹스 과정을 증명하기 위한 것과는 달리 본 논문에서는 전체 믹스 과정에서 해당 서버가 제외되지 않았음을 증명하기 위한 것이다.

4.2 Vote Opening

모든 믹스서버가 연산을 종료하고 나면 TP와 모든 믹스서버 $ME_i (1 \le i \le \lambda)$는 다음 과정을 통해 믹스과정이 정상적으로 진행되었음을 확인해야 하며, 이 과정은 투표 참가자 누구나 검증할 수 있다.

1. ME_i는 자신이 선택한 s개 평문의 곱 $m' = \prod_{i=1}^{s} m_i'$를 공개한다.
2. $1 \le i \le \lambda$에 대해, ME_i는 C_{k_i}를 공개한다. 이 때 모든 참가자는 이미 공개된 $h(C_{k_i})$를 이용하여 검증할 수 있다.
3. TP는 $\prod_{i=1}^{\lambda} C_{k_i}$를 계산하고, 이를 복호화한 값 $\widetilde{m}$를 증명값과 함께 공개한다. 모든 투표 참가자는 $\overline{m} = m' \cdot \widetilde{m}$이 성립하는지 검증한다.
4. TP는 ME_λ가 공개한 $\{ C_j \}_{1 \le j \le n-\lambda}$와 3번 과정에서 계산한 $\prod_{i=1}^{\lambda} C_{k_i}$을 이용하여 $\overline{C} = \prod_{i=1}^{n-\lambda} C_j \cdot \prod_{i=1}^{\lambda} C_{k_i}$를 계산한다.
5. TP는 C_{check}과 $\overline{C}$를 각각 복호화한 결과와 함께 이에 대한 CP 증명값을 공개한다. 모든 참가자는 이제 복호화한 결과를 거증할 수 있다.

이상의 과정을 마치면 최소한 하나의 믹스서버가 정직하다는 가정 하에 정확하게 익명성을 보장했음을 확신할 수 있다.

V. 제안하는 믹스넷 방식의 효율성 분석

본 장에서는 논문에서 새로이 제안하는 믹스넷 방식과 기존 Sebe의 믹스넷 방식의 안전성 분석을 수행한다. 앞서 언급한 바와 같이 본 논문에서 제안하는 새로운 믹스넷 방식은 기존 Sebe의 믹스넷 방식에 비해 매우 효율적이며, 유사한 수준의 안전성을 제공한다. 만약 i 번째 믹스서버가 유일하게 정직한 믹스서버이고, 다른 믹스서버는 믹스를 올바르게 수행하지 않는다해도, π_i의 기밀성이 보장되기 때문에, 믹스넷의 출력값과 입력값의 연관관계를 유추하는 것은 불가능하다. 또한 $i-1$번째 서버가 $i+1$번째 서버에게 은밀하게 출력값을 전달한다고 해도 C_{k_i}를 유추할 수 없기 때문에 i번째 서버를 제외하는 것은 불가능하다.

또, 본 논문에서 제안하는 새로운 믹스넷 방식은 Sebe의 방식에 비해 효율적이다. Sebe의 방식은 총 λs개의 더미 암호문이 추가되지만 본 방식에서는 단지 $s+\lambda$개만 추가된다. 자세한 효율성 비교는 아래 〔표 2〕와 같다.

〔표 2〕 믹스넷 효율성 및 안전성 비교

연산종류	Sebe의 방식	새로운 방식
해시연산	$s\lambda$	$s+\lambda$
비교연산	$(n+s\lambda)s\lambda$	1
더미 암호문의 복호화 연산	없음	2
곱셈연산	없음	$s+2\lambda$
안전성	$(\frac{s}{n})^s$	$\frac{1}{n-s}$

제안한 방식은 믹스과정의 검증을 위해 추가적으로 암/복호화와 곱셈 연산을 필요로 하지만, $s, \lambda \ll n$이기 때문에 계산량이 크지 않다. 반면 Sebe의 방식은 검증과정에서 많은 비교연산을 필요로 하기 때문에 전체적인 계산량은 제안한 방식이 훨씬 적음을 알 수 있다. 안전성의 경우 Sebe의 방식이 확률적으로 보다 안전하지만, n이 전체 유권자의 수로 매우 큰 수이기 때문에 제안한 방식도 충분히 안전하다고 할 수 있다.

수치를 정량화하여 살펴보면 효율성의 향상을 확실하게 확인할 수 있다. 예를 들어 우리나라의 경우 2011년 현재 약 4천만명의 유권자가 있다. 즉, $n = 4\times10^7$이다. 만약 믹스넷이 20개의 믹스서버로 구성되고, 각 서버가 100개의 더미 암호문을 생성한다고 하면, $\lambda = 20$, 그리고 $s = 100$이 된다.

이제 이 수치를 사용하여 Sebe의 믹스넷 방식과 본 논문에서 제안하는 방식을 비교하면 아래 〔표 3〕과 같다. 동일한 환경에서 시험함을 아래 표에서 언급하고 있는 연산 외 나머지 통신량 및 연산량은 모두 동일하다.

〔표 3〕 정량화된 효율성 및 안전성 비교

연산종류	Sebe의 방식	새로운 방식
해시연산	2000	210
비교연산	약 8×10^7	1
더미 암호문의 복호화 연산	없음	2
곱셈연산	없음	140
안전성	약 2×10^{-140}	약 4×10^{-7}

위 표를 살펴보면 Sebe의 믹스넷 방식은 약 8×10^{10}만큼의 비교연산을 필요로 함을 알 수 있다. 게다가 비교연산은 연산량 만큼의 저장공간을 필요로 하기 때문에, 본 논문에서 제안하는 믹스넷 방식은 Sebe의 믹스넷 방식에 비해 연산량 및 저장공간 측면에서 모두 효율적이다. 비교연산을 줄이기 위해 추가된 연산은 복호화 연산 2번과 곱셈연산 140번으로 비교연산에 비하면 무척 간소한 수준이다.

이제 안전성을 비교해보자. 믹스넷의 목적은 비밀투표의 원칙을 보존하는 것이다. Sebe의 믹스넷 방식은 특정 투표값에서 유권자를 추적하는데 성공할 확률이 약 2×10^{-140}으로 매우 낮은 확률이다. 이에 반해 본 논문이 제안하는 방식은 약 4×10^{-7}로 상대적으로 매우 높다. 그러나 로또에 당첨될 확률이 약 8×10^{-6}으로, 실제 4×10^{-7}은 매우 희박한 확률이며, 전체 유권자 수가 많은 국가일수록 본 확률은 더 떨어지게 된다.

즉, 4×10^{-7}은 비밀투표의 원칙을 보존할 수 있을 만큼 충분히 낮은 수치로써 투표결과의 안전성을 보장한다고 말할 수 있다. 따라서 본 논문에서 제안하는 새로운 믹스넷 방식은 Sebe의 방식에 비해 무척 효율적이며, 유사한 수준의 안전성을 제공한다.

VI. 결 론

전자투표의 투표과정 및 개표과정에서의 신뢰성을 확보하기 위해 현재까지도 다양한 암호학적 방법들이 연구되고 있는데, 특히 개표과정에서의 신뢰성은 믹스넷(Mixnet)을 통해 어느 정도 안전성에 대한 증명이 이루어진 상태다.

믹스넷은 1981년 David Chaum에 의해 소개된 방법으로 입력값과 출력값 사이의 연결 정보를 알 수 없도록 섞는 기술이다. 믹스넷은 다수의 믹스서버로 구성이 되는데, 각각의 믹스서버는 초기 입력값 또는 이전 믹스서버의 출력값을 입력받아 섞는 과정을 반복한다. 이 때 각 믹스서버는 자신의 동작이 올바름을 증명해야 하는데, 증명방법으로는 일반적으로 영지식 증명방법이 많이 사용된다. 그러나 영지식 증명방법은 연산량이 많고 증명과정이 복잡하기 때문에 효율적이지 못하다는 단점이 있다.

2010년 Sebe 등은 다수의 믹스서버 가운데 최소한 하나의 믹스서버가 정직하다는 가정 하에 믹스 과정의 신뢰성을 증명하기 위한 방식을 제안하였다. Sebe가 제안한 믹스서버의 증명 방식은 기존 영지식 증명방식과는 달리 매우 단순하여 효율성을 향상시킨 장점이 있다. 본 논문은 2010년 제안한 Sebe의 믹스넷 방식을 바탕으로 효율성을 개선한 새로운 믹스넷 방식을 제안하였다. 본 논문에서 제안한 새로운 믹스넷 방식은 기존 Sebe 방식의 가정사항을 그대로 유지하면서 연산량을 줄여 효율성을 향상시킨데 그 의의가 있으며, 안전한 전자투표의 도입 및 구현에 기여할 것이다.

참고문헌

〔1〕 전응렬, 이윤호, 원동호, "전자투표 실용화 현황과 전망," 한국정보보호학회지 21(2), pp86-92, 2011년 4월.

〔2〕 D.Chaum, "Secret-ballot receipt and Transparent integrity," working draft, 2002.

〔3〕 D.Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," IEEE Security and Privacy magazine, vol.2, no.1, pp38-47, Jan. 2004.

〔4〕 A.C.Neff and J.Adler, "Verifiable e-Voting Indisputable Electronic Elections at

Polling Places," http://votehere.com/vhti/documentation/VH_VHTi_WhitePaper.pdf, VoteHere Inc., 2003.
〔5〕 Peter Y.A. Ryan, and T.Peacock, "Pret a Voter: a System Perspective", http://www.cs.ncl.ac.uk/research/pubs/trs/papers/929.pdf, School of Computing Science, University of Newcastle, Sep. 2005.
〔6〕 Y.Lee, S.Park, M.Mambo. S.Kim and D.Won, "Towards trustworthy e-voting using paper receipts," Computer Standards and Interfaces, vol.32, pp305-311, 2010.
〔7〕 D.Chaun, A.Essex, R.Carback, A.Sherman, J.Clark, S.Popoveniuc and P.Vora, "Scantegrity: End-to-End Voter-Verifiable Optical Scan Voting", IEEE Security & Privacy, pp40-46, Jun. 2008.
〔8〕 D.Chaum, "Untraceable Electronic Mail Return Address and digital Pseudonyms," Comm. of the ACM, vol.24, no.2, pp84-88, Feb. 1981.
〔9〕 A.C.Neff, "A Verifiable Secret Shuffle and Its Application to E-Voting," Proc. of the 8th ACM Conference on Computers and Communications Security(CCS-8), pp116-125, 2001.
〔10〕 P.Golle, M.Jakobsson, A.Juels, and P.Syverson, "Universal Re-encryption for Mixnets," CT-RSA 2004, LNCS 2964, pp163-178, 2004.
〔11〕 K.Sako and J.Kilian, "Receipt-Free Mix-Type Voting Scheme - A Practical Solution to the Implementation of a Voting Booth," Proc. of Advances in Cryptology(Eurocrypt'95), LNCS 921, pp393-403, 1995.
〔12〕 M.Jakobsson and A.Juels, "Millimix : Mixing in small batches," DIMACS Technical Reports, pp33-99, 1999.
〔13〕 M.Jakobsson, A.Juels, and R.L.Rivest, "Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking," Proc. of the 11th USENIX Security Symposium, pp339-353, 2002.
〔14〕 M.Jakobsson, "A Practical Mix," Proc. of Advances in Cryptology(Eurocrypt'98), LNCS 1403, pp448-461, 1998.
〔15〕 M.Abe, "Mix-networks on permutation networks," Proc. of Asiacrypt'99, LNCS 1716, pp258-273, 1999.
〔16〕 B.Pfitzmann and A.Pfitzmann, "How to Break the Direct RSA-Implementation of Mixes," Proc. of Advances in Cryptology (Eurocrypt'89), LNCS 434, pp373-381, 1989.
〔17〕 J.Bryans and P.Y.A.Ryan, "A Dependability Analysis of the Chaum Digital Voting Scheme," Technical Report CS-TR:809, School of Computing Science, Newcastle University, 2003.
〔18〕 F.Sebe, J.M.Miret, J.Pujolas, and J.Puiggali, "Simple and efficient hash-based verifiable mixing for remote electronic voting," Computer Communications, vol.33, pp667-675, 2010.
〔19〕 R. Anderson and R. Needham, "Robustness principles for public key protocols," Advances in Cryptology, CRYPTO'95, LNCS 963, pp. 236-247, 995.
〔20〕 A. Juels and R. Pappu, "Squealing euros: privacy protection in RFID-enabled banknotes," Proc. of the Financial Cryptography, LNCS 2742, pp. 103-121, 2003.
〔21〕 J. Arkko, C. Vogt, and W. Haddad, "Enhanced route optimization for mobile IPv6," RFC 4866, May 2007.
〔22〕 W. Stallings, Cryptography and network security: principles and practices, 4th Ed., Prentice Hall, Nov. 2005.
〔23〕 홍길동, "정보보호에 관한 연구," 박사학위논문, 한국대학교, 2009년 2월.
〔24〕 S.A. Weis, "New foundations for efficient authentication, commutative cryptography, and private disjointness testing," Ph.D. Thesis, Massachusetts Institute of Technology, May 2006.

〔25〕 K. Nohl and D. Evans, "Quantifying information leakage in tree-based hash protocols," CS-2006-20, Computer Science Department, University of Virginia, 2006.

〈著者紹介〉

전 웅 렬 (Woongryul Jeon) 학생회원
2006년 2월: 성균관대학교 컴퓨터공학과 학사 졸업
2008년 2월: 성균관대학교 전자전기컴퓨터공학과 석사 졸업
2008년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
〈관심분야〉 정보보증, 정보보호, 암호이론 등

이 윤 호 (Yunho Lee) 정회원
2006년 2월: 성균관대학교 컴퓨터공학과 학사 졸업
2008년 2월: 성균관대학교 전자전기컴퓨터공학과 석사 졸업
2008년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
〈관심분야〉 정보보증, 정보보호, 암호이론 등

원 동 호 (Dongho Won) 종신회원
1976년~1988년: 성균관대학교 전자공학과 (공학사, 공학석사, 공학박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장