안전한 전자중매 프로토콜

이병천, 김광조
한국정보통신대학원대학교 정보보호그룹
e-mail:{sultan,kkj}@icu.ac.kr

Secure Match-Making Protocol

Byoungcheon Lee, Kwangjo Kim
Information Security Group, Information and Communications University

요 약

전자중매 프로토콜(Match-making protocol)은 남녀간의 그룹미팅에서 커플을 구성하거나 특정 그룹 내에서 팀을 구성하기 위한 프로토콜이다. 본 연구에서는 두 사람이 서로 상대방을 선택했을 때에만 커플로 인정된다고 하는 규칙을 사용할 때 커플이 성립되었음을 확인하고 이를 증명하기 위한 안전하고 효율적인 프로토콜을 설계하였다. 이를 구현하기 위한 하부 프로토콜로서 두개의 이산대수 원소가 같은 지수값을 가지는지 여부를 증명하는 방법과 이를 이용하여 두개의 ElGamal 암호문이 제공되었을 때 복호화를 하지 않고도 평문 메시지가 일치하는지 여부를 확인하고 증명할 수 있는 프로토콜을 제시하고 이를 전자중매 프로토콜 설계에 이용하였다. 이러한 방법은 전자중매 프로토콜 뿐만 아니라 실생활에서 요구되는 다양한 문제들을 해결하는 방법론으로 이용될 수 있을 것으로 예상된다.

1. 서론

최근 다수의 참여자가 존재하는 환경에서 안전하고 공정한 계산을 수행하기 위한 안전한 다수 참여자간 계산(Secure multi-party computation)에 대한 연구가 매우 활발하다. 그 예로서 전자화폐, 전자투표, 전자경매 등의 서비스를 구현하기 위한 많은 연구들이 수행되고 있다.

본 연구에서는 실생활에서 흔히 사용되는 사례 중의 하나인 남녀간의 그룹미팅에서 커플을 구성하는 방법을 모델로 하여 안전하고 공정한 전자중매(match-making) 프로토콜을 설계하고자 한다. 여기서 고려하는 중매 규칙은 두 사람이 서로 상대방을 선택했을 때에만 커플이 성립된다는 것이다. 이러한 프로토콜에서 참가자의 선택 내용은 안전하게 보호되어야 한다. 커플이 성립된 참여자에 대해서는 선택내용이 공개되어도 문제가 없겠지만 커플이 되지 못한 참여자에게는 자신의 선택내용이 공개되지 말아야 할 매우 중요한 비밀정보가 되는 것이다. 이렇게 특정 그룹 내에서 팀을 구성하는 방법은 학급 내에서의 프로젝트 팀의 구성, 사업 참여를 위한 컨소시엄의 구성, 온라인 게임에서의 파트너의 선정 등 다양한 응용분야에 적용될 수 있다.

본 연구에서 고려하는 전자중매 시스템은 m명의 남성그룹 M_i $(i=1,\ldots,m)$와 n명의 여성그룹 F_j $(j=1,\ldots,n)$ 그리고 중개기관인 TTP로 구성된다. 시스템의 개략적인 운영방법을 기술해 보면 커플을 선정하기 위하여 남성그룹과 여성그룹의 각 참여자들은 상대 그룹에서 원하는 파트너를 선정하고 TTP의 공개키로 암호화한 비밀위탁값을 계산하여 공개게시판에 게시한다(위탁단계). TTP는 이것을 분석하여 커플을 찾아내고 공개하며(공개단계) 커플로 공개된 참여자는 이에 대한 증명을 제시하게 된다(증명 단계).

이러한 전자중매 시스템이 가져야 할 보안 요구사항들은 다음과 같이 정리될 수 있다.

- o 기밀성(privacy) : 커플이 성립된 참여자를 제외한 모든 참여자의 선택 내용은 TTP를 포함한 타인에게 공개되지 않아야 한다.
- o 공정성(fairness) : 위탁단계에서 중간에 프로토콜이 중단된다고 하더라도 어떤 참여자도 다른 참

여자들에 비해 유리한 상황이 되어서는 안된다. 즉 어떤 참여자가 다른 참여자들의 선택 내용에 관한 어떤 부분정보도 얻을 수 없어야 한다.

o 정확성(correctness) : 공개단계 및 증명단계에서의 공개된 결과는 누구나 정확성을 검증할 수 있어야 한다.

o 부인방지(non-repudiation) : 커플이 성립된 참여자는 자신의 선택 내용에 대해 추후 부인할 수 없어야 한다.

본 연구에서는 이러한 요구사항을 만족하는 안전한 전자중매 프로토콜을 구성하기 위하여 두개의 이산대수 원소가 같은 지수값을 갖는지 여부를 증명하는 기법[MS97]을 이용하여 두개의 ElGamal 암호문이 제시되었을 때 복호화를 하지 않고도 평문 메시지가 일치하는지 여부를 확인하고 증명할 수 있는 기법을 제안하였다.

2장에서는 프로토콜 구현을 위한 여러가지 프리미티브들에 대해 설명하고 3장에서는 제안된 전자중매 프로토콜을 기술한다. 4장에서는 시스템의 보안 특성, 효율성을 분석하고 5장에서는 결론 및 향후과제를 기술한다.

2. 암호 프리미티브

본 논문에서 중요하게 사용되는 것은 이산대수 기반의 암호시스템이다. 충분히 큰 소수 p에 대하여 Z_p^*는 모듈러 p에 대한 곱셈군이다. $q|p-1$인 소수 q를 위수로 갖는 Z_p^*내의 순환군을 고려하고 이것의 기저를 g로 표시하자.

2.1 비밀 정보의 안전한 분배

참여자간에 비밀정보를 안전하게 분배하기 위하여 서명되고 암호화된 전자봉투를 이용한다. 남성그룹의 참여자 M_i가 여성그룹의 참여자 F_j에게 보내는 비밀정보를 m_{ij}라고 하자. 이것은 메시지 공간 M 내에서 임의로 선택된다. 이 메시지는 다음 수식으로 표현한 바와 같이 송신자 M_i의 개인키로 서명하고 수신자 F_j의 공개키로 암호화한 전자봉투(envelop)를 만들어 전송한다.

$m_{ij} \in_R M$

$$Env(SK_i, PK_j, m_{ij}) = [Sig_{SK_i}(m_{ij}), E_{PK_j}(m_{ij})]$$

이렇게 전송된 비밀정보는 정당한 수신자만이 복구할 수 있으며 추후 비밀정보가 m_{ij}라는 것을 제3자에게 증명할 수 있게 된다.

2.2 두 개의 이산대수 원소의 동일지수 여부 증명

α와 β는 위수가 q인 Z_p^*내의 순환군에 있는 두 개의 독립적인 원소라고 하자. 증명자는 두 개의 이산대수 원소 y와 z가 기저 α와 β에 대하여 $(y, z) = (\alpha^x, \beta^x)$와 같이 동일한 지수 x로 구성되어 있는지 여부를 영지식으로 증명하고자 한다. Michels와 Stadler는[MS97] 이를 위한 효율적인 프로토콜을 제시하였다. Chaum과 Pedersen의[CP92] 증명기법은 동일한 지수를 가지는 것을 증명할 수 있지만 지수값이 다르다는 것을 증명하지는 못한다. [MS97]은 다음 프로토콜에 나타낸 바와 같이 추가적인 메시지와 프로세스를 이용하여 지수값이 다르다는 것도 증명할 수 있게 하였다. 여기에서는 전체 검증성을 제공하기 위하여 다음과 같은 비대화형(non-interactive) 프로토콜을 고려한다.

프로토콜 1 [이산대수의 동일지수 여부 증명]

증명자는 $(y, z) = (\alpha^x, \beta^x)$가 기저 α,β에 대하여 동일지수 x를 갖는지 여부를 x를 노출시키지 않고 영지식으로 증명하고자 한다. 여기서 H는 충돌저항성 해쉬함수이다.

(1) 증명자

- $k, k' \in_R Z_q$를 임의로 선택한다.
- $r_\alpha = \alpha^k, r_\beta = \beta^k, r'_\alpha = \alpha^{k'}, r'_\beta = \beta^{k'}$을 계산한다.
- $v = H(\alpha, y, \beta, z, r_\alpha, r_\beta, r'_\alpha, r'_\beta)$를 계산한다.
- $s = k - vx, s' = k' - vk$를 계산한다.
- $(r_\alpha, r_\beta, r'_\alpha, r'_\beta, s, s')$을 전송한다.

(2) 검증자

- $v = H(\alpha, y, \beta, z, r_\alpha, r_\beta, r'_\alpha, r'_\beta)$를 계산한다.
- $r_\alpha = \alpha^s y^v, r'_\alpha = \alpha^{s'} r_\alpha^v, r'_\beta = \beta^{s'} r_\beta^v$를 만족하는지 검증한다. 만족하지 않으면 증명자의 메시지가 유효하지 않은 것이며 검증단계를 중지한다.
- 만일 $r_\beta = \beta^s z^v$ 이면 $\log_\beta z = \log_\alpha y$ 이고 만일 $r_\beta \neq \beta^s z^v$ 이면 $\log_\beta z \neq \log_\alpha y$ 이다.

2.3 ElGamal 암호문의 동일메시지 여부 증명

TTP의 비밀 개인키가 x이고 공개키가 $y = g^x$인 경우 메시지 m에 대한 TTP의 공개키를 이용한 ElGamal 암호문은 다음과 같이 주어진다.

$k \in {}_R Z_q$

$c = (a, b) = (g^k, y^k m)$

TTP가 다음과 같이 두 개의 메시지 m_1, m_2에 대한 암호문 c_1, c_2를 가지고 있다고 하자.

$c_1 = (a_1, b_1) = (g^{k_1}, y^{k_1} m_1)$

$c_2 = (a_2, b_2) = (g^{k_2}, y^{k_2} m_2)$

TTP는 복호화를 해서 메시지를 공개하지 않고도 두 개의 암호문이 동일한 메시지를 가지는지 여부를 다음과 같이 증명할 수 있다.

**** 프로토콜 2 [암호문의 동일메시지 여부 증명]***

TTP는 두 개의 암호문 c_1, c_2가 동일 메시지를 갖는지 여부를 메시지를 복호화하지 않고 증명하고자 한다.

(1) TTP

- $c_1/c_2 \equiv (a_3, b_3) \equiv (a_1/a_2, b_1/b_2)$를 계산한다.
- *프로토콜 1*을 이용하여 $(y, b_3) = (g^x, a_3^x)$ 여부를 증명한다.

(2) 검증자

- 만일 $a_3^x = b_3$이면 $m_1 = m_2$이고 $a_3^x \neq b_3$이면 $m_1 \neq m_2$이다.

2.4 복호화의 유효성 증명

메시지 수신자의 공개키가 $y = g^x$라고 할 때 수신자는 ElGamal 암호문 $(a, b) = (g^k, y^k m)$을 복호화하여 메시지 m을 얻을 수 있다. 그런데 복호화 과정의 유효성을 제 3자에게 증명할 필요가 있는 경우에는 비밀키 x를 노출시키지 않고 m의 유효성을 다음과 같이 영지식으로 증명할 수 있다.

**** 프로토콜 3 [복호화의 유효성 증명]***

TTP는 자신의 비밀키 x를 노출시키지 않고 암호문 $(a, b) = (g^k, y^k m)$의 복호화된 메시지가 m이라는 것을 증명하고자 한다. TTP는 *프로토콜 1*을 이용하여 $(y, b/m) = (g^x, a^x)$임을 증명한다.

3. 제안된 전자중매 프로토콜

여기에서는 앞장에서 제시된 프리미티브들을 이용하여 안전한 전자중매 프로토콜을 제시한다. 전자중매 프로토콜의 참여자는 다음과 같다.

- o m명의 남성그룹 M_i $(i = 1, \ldots, m)$
- o n명의 여성그룹 F_j $(j = 1, \ldots, n)$
- o 중개기관 T

이들은 공개된 통신채널로서 공개게시판을 이용하며 이를 통하여 전체검증성과 부인방지 기능을 제공하게 된다. 중개기관 T는 참여자와 불법적으로 공모하지 않는 신뢰기관이라고 가정한다.

제안된 전자중매 프로토콜은 참가자 등록단계, 비밀정보 분배단계, 비밀선택값 위탁단계, 커플 공개단계, 커플 증명단계의 다섯 단계로 이루어진다. 이하 각 단계별로 자세한 프로토콜을 기술한다.

(1) 참가자 등록단계

전자중매 프로토콜에 참여하고자 하는 사람은 TTP에 등록을 신청하고 이름, 공개키, 인증서를 등록한다. 이들은 공개게시판에 공개된다.

(2) 비밀정보 분배단계

각 참여자들은 다른 그룹의 참여자들과 비밀정보를 사전 교환해야 한다. 남성그룹의 참여자 M_i가 여성그룹의 참여자 F_j에게 보내는 비밀정보를 m_{ij}라고 하면 다음과 같이 전자봉투를 만들어 메시지를 분배한다.

$m_{ij} \in {}_R M$

$Env(SK_i, PK_j, m_{ij}) = [Sig_{SK_i}(m_{ij}), E_{PK_j}(m_{ij})]$

같은 방법으로 여성그룹의 참여자 F_j가 남성그룹의 참여자 M_i에게 보내는 비밀정보를 f_{ji}라고 하면 메시지를 다음과 같이 분배한다.

$f_{ji} \in {}_R M$

$Env(SK_j, PK_i, f_{ji}) = [Sig_{SK_j}(f_{ji}), E_{PK_i}(f_{ji})]$

각 참여자들은 자신이 수신한 메시지를 복호화하여 비밀정보 m_{ij}, f_{ji}를 복구한다.

(3) 비밀선택값 위탁단계

M_i가 F_j를 선택한다고 하면 M_i는 비밀선택값 c_{ij}와 이것을 자신이 서명하고 TTP의 공개키로 암호화하여 비밀위탁값을 다음과 같이 생성한다.

$c_{ij} = H(m_{ij}, f_{ji})$

$Env(SK_i, PK_T, c_{ij}) = [Sig_{SK_i}(c_{ij}), E_{PK_T}(c_{ij})]$

마찬가지로 F_j가 M_i를 선택한다고 하면 F_j는 비밀선택값과 비밀위탁값을 다음과 같이 생성한다.

$c_{ji} = H(m_{ij}, f_{ji})$

$Env(SK_j, PK_T, c_{ji}) = [Sig_{SK_j}(c_{ji}), E_{PK_T}(c_{ji})]$

각 참여자는 위와 같이 생성된 비밀위탁값을 공개게시판에 게시한다. 여기에서 볼 수 있듯이 M_i와 F_j가 서로 상대방을 선택했다면 $c_{ij} = c_{ji}$가 됨을 알 수 있다. 여기에서 사용되는 공개키 암호 $E_{PK}()$는 확률적 특성을 가지는 ElGamal 암호를 사용한다.

(4) 커플 공개단계

비밀선택값의 위탁단계가 끝나면 TTP는 모든 가능한 커플의 쌍에 대하여 *프로토콜 2*를 이용하여 동일메시지가 있는지 여부를 판단하고 그 결과와 증명을 공개게시판에 게시한다. 동일메시지가 있다면 해당되는 M_i와 F_j는 커플이 되는 것이다.

(5) 커플 증명단계

커플이 성립되었음이 공개된 참여자 M_i와 F_j는 그들간에 공유하고 있는 비밀정보 m_{ij}와 f_{ji}를 공개하고 그것의 유효성을 증명한다. 이것의 인증성은 전자봉투의 서명을 통해 검증할 수 있다. 이것의 유효성은 메시지의 송신자와 수신자가 모두 증명할 수 있다. 송신자는 확률적 ElGamal 암호에 사용되었던 난수정보를 공개함으로써 비밀정보의 유효성을 증명할 수 있고 수신자는 *프로토콜 3*을 이용하여 자신의 비밀키를 공개하지 않고도 비밀정보의 유효성을 증명할 수 있다. 그러므로 한쪽 참여자가 일방적으로 자신의 행위를 부인하지는 못한다.

4. 프로토콜의 특성 분석

앞장에서 제안된 전자중매 프로토콜은 다음과 같은 보안특성을 만족한다.

- o 기밀성 : 비밀위탁값은 TTP의 공개키로 암호화되고 결코 복호화되지 않으므로 기밀성이 보장된다. TTP가 복호화를 하더라도 각 참여자간의 비밀정보를 알지 못하므로 참가자의 선택 내용을 알 수는 없다.
- o 공정성 : 비밀위탁값은 TTP의 공개키로 암호화되어 전송되므로 위탁단계에서 어느 누구도 타인의 선택내용에 대한 어떤 유용한 정보도 획득할 수 없다.
- o 정확성 : TTP의 커플 결정 내용은 누구나 검증할 수 있다.
- o 부인 방지 : 참가자들간의 비밀정보 분배단계와 비밀선택값 위탁단계에서 전자서명을 사용하므로 커플로 결정된 참여자들은 추후 자신의 행위를 부인할 수 없다.

제안된 전자중매 프로토콜에 대해서 다음과 같은 부정한 공격상황을 고려해 볼 수 있을 것이다.

- o TTP가 비밀위탁값을 복호화하여 공개하면 각 참여자들은 자신이 공유하고 있는 비밀정보를 이용하여 자신과 관계된 위탁값이 있는지 검사해 볼 수 있다. 그러므로 TTP는 비밀위탁값을 복호화하여 공개하지는 말아야 하며 암호문의 동일메시지 여부만을 확인해야 한다.
- o 참여자가 TTP와 공모하여 자신이 소유한 비밀정보를 제공하고 TTP가 협조하면 누가 자신을 선택했는지 검사해 볼 수 있다.

제안된 전자중매 프로토콜의 효율성을 분석해보면 비밀정보의 사전분배에 $O(mn)$의 통신량과 계산량이 필요하다. 또한 커플의 공개 단계에서 TTP가 수행해야 하는 계산량도 모든 가능한 쌍에 대해 조사해야 하므로 $O(mn)$의 계산량이 필요하다. 효율성을 좀더 향상시키기 위해서는 비밀정보의 사전분배가 필요없는 프로토콜의 설계, TTP에 의존하지 않는 프로토콜의 설계 등 추가적인 연구가 필요하다.

5. 결론 및 향후과제

본 논문에서는 남성그룹, 여성그룹간에 두 명으로 이루어지는 커플을 구성하는 방법으로서 두 사람이 서로 상대방을 선택하는 경우에만 커플이 이루어진다고 하는 특정 모델 하에서 프로토콜을 설계하였다. 구체적인 구현 방법으로서 참여자간 비밀정보를 사전 분배하고, TTP의 공개키로 암호화하여 비밀선택값을 위탁하며, 두 개의 암호문이 주어진 경우 복호화를 하지 않고도 동일메시지를 가지는지 여부를 증명하는 기법을 이용하여 안전한 전자중매 프로토콜을 설계하였다.

이러한 전자중매 프로토콜을 좀 더 확장하면 우선순위를 가지고 여러명을 선택하는 경우, 2명이상의 팀을 구성하는 경우 등 다양한 상황에 맞는 프로토콜을 구성할 수 있을 것으로 생각된다.

참고문헌

[MS97] M. Michels, M. Stadler, "Efficient convertible undeniable signature", Proc. of 4th annual workshop on selected areas in cryptography, 1997

[CP92] D. Chaum, T. Pedersen, "Wallet databases with observers", LNCS 740, Advances in Cryptology - Crypto'92, pp. 89-105