계산 효율성을 높인 Vickrey 경매

오옥균° 공은배
충남대학교 컴퓨터공학과

{okoh°, keb}@ce.cnu.ac.kr

A Computationally Efficient Vickrey Auction

OkKyun Oh° EunBae Kong
Dept. of Computer Engineering, Chungnam National University

요 약

인터넷 경매는 객관적 정보획득이 쉽고 신분노출이 적어 크게 각광받고 있으나 불특정 다수의 참여로 이루어지기 때문에 안정성과 효율성을 전제로 해야 한다. 본 논문에서는 인터넷과 같은 불안전한 통신채널과 호스트를 신뢰할 수 없는 상황에서 확률론적 암호화 기법을 이용하여 자신들의 입찰정보는 최대한 숨기면서 효율적으로 낙찰자와 낙찰가를 계산할 수 있는 Vickrey 경매 모델을 제안한다. 제안된 모델은 Auctioneer와 Auction Issuer가 담합하지 않는다는 가정하에서 그 효율성이 입증된 Naor-Pinkas-Sumner의 시스템보다 훨씬 적은 계산량을 요구한다.

1. 서 론

인터넷의 급속한 발전은 전자상거래의 시장규모를 확대하였으며 그중 판매자의 물품을 구매자들의 가격경쟁에 의해 구입하는 인터넷 경매는 시공간적 제약이 완화됨에 따른 높은 효율성과 객관적 정보획득의 용이성, 적은 신분노출 등의 장점으로 오늘날 크게 각광받고 있다.

경매는 입찰가의 공개여부에 따라 open-cry 경매와 sealed-bid 경매로 구분되며 open-cry 경매는 영국식(오름차순) 경매와 네덜란드식(내림차순) 경매로 나뉜다. sealed-bid 경매는 입찰자와 경매인(auctioneer)의 공모(collusion)로부터 개별적인 입찰자들의 이익을 보호하기 위해 보편적으로 사용되는 경매형태로, 어떤 입찰가를 낙찰가로 결정하느냐에 따라 여러 변형이 있다. 이중 Vickrey 경매(Second Price Sealed Bid Auction)는 비공개 입찰을 통해 최고 입찰가를 제시한 입찰자를 낙찰자로 선정하되 최종 낙찰가는 두 번째로 높은 입찰가로 결정하는 방식이다. 이는 판매자에게는 영국식 경매 만큼의 수익을 보장하고, 구매자에게는 합리적인 가격을 제시해 주는 모델로서 구매자간의 과도한 경쟁과 불필요한 전략적 입찰을 막아주는 동시에 낙찰자는 개인적인 평가가 아닌 일반적인 가치로 물품을 구매할 수 있다는 장점이 있다[1,2].

본 연구에서는 Vickrey 경매에서 입찰자들의 개인정보 유출없이 공동의 목표(낙찰자와 낙찰가 계산)를 효율적으로 계산하기 위해 확률론적 암호화 기법을 사용하였으며 효율성이 이미 입증된 Naor-Pinkas-Sumner(NPS)의 시스템과 비교함으로 그 성능의 우수함을 입증한다.

2. 관련 연구

2.1 NPS system

Naor-Pinkas-Sumner(NPS)는 분산된 신뢰를 가진 실제적인 sealed-bid 경매 프로토콜 연구에 있어 상당한 진전을 가져오는 시스템을 제안하였다[5]. 이 시스템은 Auctioneer 이외에 Auction Issuer(AI)라는 제 3자를 둠으로서 두 Server로 신뢰를 분산시키며, Auctioneer와 AI가 담합하지 않는 한 불필요한 정보의 노출이 없다. 또한 Proxy-OT 프로토콜 수행을 통해 메시지의 비밀을 보장하며, 이중 암호화를 하여 통신 채널상의 안전성을 보장한다. 하지만 Auctioneer와 AI 사이에 경매 결과 계산을 위한 garbled circuit과 garbled value를 전송하는데 많은 통신·복잡도가 요구되며, AI의 연산 중 많은 부분을 차지하는 garbled circuit을 미리 생성하기 위해서는 그 경매에 참여하는 입찰자들의 최대 수를 가능한 정확하게 추정해야 하는 문제점이 있다. 최근에는 AI가 입찰가의 임의 bit를 수정하는 것이 가능하다는 심각한 취약점이 발견되었으며 부정한 AI를 검출하기 어렵다.

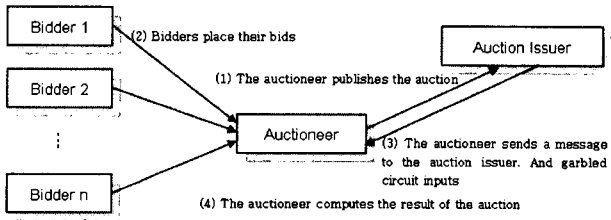

그림 1. NPS System

1) 이 연구는 BK21충남대학교 정보통신인력양성사업단의 지원을 받았음

2.2 확률론적 암호화

확률론적 암호화 기법은 결정론적인 암호화 기법에서처럼 하나의 평문 메시지가 단일 암호문으로 암호화되는 것이 아니라 여러 개의 가능한 암호문들 중의 하나로 암호화되는 방식을 말한다. 이러한 방법에서는 암호문으로부터 원본 메시지에 대한 부분적인 정보를 얻는 것이 힘들며 그것은 몇몇 어려운 문제를 푸는 것과 같다.

Goldwasser와 Micali는 확률론적 암호화 기법의 한 예로 이차잉여와 Legendre 기호를 응용한 Jacobi 기호를 사용하여 평문을 bit 단위로 암호화 하는 GM 암호화 알고리즘을 제안하였는데[6], 그 안전성은 이차잉여 가정에 의존하고 있다. 이는 정수 x가 제곱 modular 합성정수 n(x^2 mod n)인지 아닌지를 찾는 것인데, 만약 n의 인수가 알려져 있다면 쉽지만, 그렇지 않다면 어려운 문제이다.

[정리1]이차잉여 가정(Quadratic Residue Assumption)
모든 '확률적 다항식 시간 공격자 A'에 대하여, 다음과 같은 무시할 만한 $\nu(k)$가 존재한다:

$$Pr[n \leftarrow RSA\text{-}modulus(1^k); x_0 \leftarrow QR_n; x_1 \leftarrow QNR_n;$$
$$b \leftarrow \{0,1\}; b' \leftarrow A(n,x) : b = b'] = \frac{1}{2} + \nu(k)$$

이것은 어떤 암호화된 값이 있을 때, 이 값의 원래의 평문 bit를 추정하는 알고리즘의 성능이 랜덤하게 추측하는 알고리즘의 경우와 비슷하다는 것이다.

GM 암호화의 key생성 및 암호화, 복호화 과정은 다음과 같다.

- **Key 생성 :**

수신자 B는 공개되지 않은 충분히 큰 두 소수(prime) p,q의 곱 $n = pq$을 구하고 n을 법으로 한 이차비잉여로 Jacobi 기호 $\left(\frac{a}{n}\right) = 1$을 만족하는 $a \in Z_n^*$를 생성하여 (n,a)를 공개한다. 여기서 공개키는 (n,a)이고, 비밀키는 (p,q)이다.

- **암호화 :**

송신자 A는 수신자 B에게 길이가 k인 이진 메시지 $m = m_1 m_2 ... m_k$를 보내고자 한다. 수신자 B의 공개키가 (n,a)일 때, A는 각 m_i에 대응하는 $r_i \in Z_n^*$를 선택한다. 송신자 A는 (a,r,n)을 이용하여, $m_i \in \{0,1\}$에 대해, $c_i = a^{m_i} r_i^2 \bmod n$으로 암호화 하고, 암호문 $C = c_1 c_2 ... c_m$를 B에게 송신한다.

- **복호화 :**

수신자 B는 자신의 비밀키 $n = pq$를 이용하여 각 c_i가 법 n에 대하여 이차잉여인지 또는 이차비잉여인지를 판정하여 각 c_i가 이차잉여이면 $m_i = 0$으로, 이차비잉여이면 $m_i = 1$로 복호화 한다.

3. 제안하는 Vickery 경매 모델

제안하는 모델에서는 물품을 구매하고자 하는 입찰자(Bidder), 물품을 판매하고자 하는 판매자(Auctioneer), Auctioneer와 경매 결과 연산을 수행하는 경매 운영자 서버(Auction Issuer Server : AIS)로 구성된다.

3.1 제안 모델의 동작

3.1.1 물품 등록 단계

물품을 판매하고자 하는 경매 참여자(Auctioneer)는 AIS에 경매 등록 신청을 한다. 이때 물품 정보, 입찰 기간(시간)과 자신의 ID를 함께 보내며, AIS는 자신의 RSA키를 생성하여 DB에 기록후 Auctioneer에게 공개키로 전송한다.

3.1.2 물품 검색 단계

입찰자 B는 자신이 구매하고자 하는 물품을 AIS에서 검색한다. 해당하는 경매가 있을 경우, AIS는 B에게 Auctoneer의 ID정보, IP, Port Number와 물품 및 경매 정보를 보내준다.

3.1.3 입찰 단계

입찰자 B는 경매에 참가하기 위해 Auctioneer에게 참가 요청을 하고, Auctioneer는 자신의 공개키와 AIS의 공개키 그리고 경매 종료시간을 B에게 전송한다.

$$Msg < PKey(Auctioneer, AIS) \,||\, EndTime >$$

B는 상품의 가치를 평가하여 입찰 가격을 결정한다. 입찰 가격이 결정되면 우선 Auctioneer의 공개키로 암호화한 후 다시 AIS의 공개키로 암호화한다. 이렇게 입찰 가격을 이중 암호화하여 자시의 ID와 함께 Auctioneer에게 전송한다.

$$Msg < ID_B \,||\, E_{RSA}(PK_{AIS}, E_{GM}(PK_A, b_i)) >$$

이 과정을 좀더 자세히 보면 입찰자 B는 k bit의 입찰가 $b = (b_1, b_2, \ldots, b_k)$를 Auctioneer의 공개키로 GM 암호화 알고리즘을 이용하여 $G = (g_1, g_2, \ldots, g_k)$로 암호화한다.

$$\text{for } i = 1,2,...,k$$
$$\{$$
$$r_i \in Z_x^*$$
$$g_i = a^{b_i} r_i^2 \bmod n$$
$$\}$$
$$G = E_{GM}(PK_A, b)$$

입찰자 B는 이것을 다시 AIS의 공개키로 암호화하고 자신의 키로 G에 대해 서명을 생성한다.

$$C = E_{RSA}(PK_{AIS}, G)$$
$$S_B = Sig(SK_B, G)$$

입찰자 B는 자신의 입찰가와 그에 대한 서명(C, S_B)를 Auctioneer에게 전송한다.

3.1.4 계산 단계

Auctioneer는 AIS와의 GM 프로토콜을 수행함으로써 입찰자들의 입찰가에 대한 연산을 하게 된다.

Auctioneer는 경매 시간이 종료되면 각 입찰 정보의 서명을 검증하고 서명이 유효한 경우, 각 입찰 정보에

NewID를 부여하여 쌍을 저장한다.

$$< NewID_B \| ID_B >$$

Auctioneer는 자신이 생성한 NewID와 입찰가의 쌍에 대해 미리 규정된 Hash 함수를 이용하여 Hash 값을 계산하고, 그 값들에 자신의 키로 서명을 하여 공개된 게시판 등에 공개해 둔다.

$$Sig(SK_A, (H(C_1) \| H(C_2) \| ... \| H(C_m))$$

Auctioneer는 NewID와 입찰가를 AIS에게 전송한다.

$$Msg < NewID_B \| C_B >$$

AIS는 입력 받은 모든 암호화된 입찰 가격을 자신의 비밀키로 1차 복호화 한다. 하지만 Auctioneer의 공개키로 암호화가 되어 있기 때문에 입찰 가격 정보는 알 수가 없다.

$$E_{GM}(PK_A, b_i) = D_{RSA}(DK_{AIS}, E_{RSA}(PK_{AIS}, E_{GM}(PK_A, b_i)))$$

bit 단위로 암호화 된 입찰 가격의 앞쪽 bit 쌍을 Auctioneer에게 전송한다. 이때 AIS와 Auctioneer 사이의 통신량을 줄이기 위해, 전송하는 입찰 bit들을 경매 규모에 따라 하나가 아닌 여러 개의 bit들의 순차적인 쌍을 전송하도록 한다.

Auctioneer는 bit 단위로 복호화 하여, 두 bit의 크기를 비교하고 그 결과를 AIS에게 전달한다. 이 과정 중간 중간에 AIS는 임의로 두 bit를 생성하여 Auctioneer에게 전송하고 Auctioneer가 올바른 결과를 내는지 검사하여 Auctioneer가 공정하게 동작하고 있음을 검증한다.

가장 큰 값과 두 번째 큰 값을 찾을 때까지 Auctioneer와 AIS간 위의 과정을 반복한다. 가장 큰 값에 해당하는 NewID를 낙찰자로, 두 번째로 큰 값을 낙찰가로 선정하여 자신의 키로 서명한 후 공개된 게시판에 공지하고, 그것을 Auctioneer에게 전송한다.

$$Sig(SK_{AIS}, NewID_{winner} \| G_{win})$$

Auctioneer는 NewID에 해당하는 원래의 ID를 찾고, 낙찰가로 받은 값을 복호화 한다.

$$ID \leftarrow NewID_{winner}$$

$$D_{GM}(SK_A, G_{win})$$

3.1.5 결과 발표 단계

Auctioneer는 Auction Issuer가 보내준 계산 정보를 통해 나온 결과를 모든 참여자에게 공지하게 된다. 이때 낙찰자로 선정된 Bidder는 Hash 함수를 적용한 자신의 입찰정보를 Auctioneer에게 전송하여 낙찰자임을 인증 받는다.

3.2 제안 모델의 계산 복잡도

제안된 모델의 계산 복잡도를 계산하고 이것을 NPS system의 계산 복잡도와 비교함을 통해 제안 모델의 성능을 분석하고자 한다. 이때, 서명의 생성이나 검증 알고리즘, 공개키 암·복호화 연산은 두 모델에서 모두 사용되며, 그 계산량이 많지 않기 때문에 계산 복잡도의 고려 대상에서 제외하기로 한다. 아래 표 1은 k 를 입찰가의 비트 수, m을 입찰자의 수, σ를 circuit의 gate 수라 할 때, 제안된 기법과 NPS system의 계산량을 보여주는 것이다.

Protocol / Party	제안하는 모델	NPS system
Bidder i	$k \cdot$MOD SQR$+1 \cdot E()+1 \cdot Sig()$	$k \cdot$MOD EXP$+k \cdot$MOD DIV$+2k \cdot E()$
Auctioneer	$\{(m-1)(k+1)+k\} \cdot D_{GM}()$ $+2 \cdot Ver()+2 \cdot Sig()+1 \cdot H()$	$2mk \cdot D_{ElGamal}()+mk \cdot D()+\sigma \cdot F()$
Auction Issuer	$m \cdot D()+(m-1)(k+1) \cdot$MOD MUL $+(m-1) \cdot$MOD SQR$+2 \cdot Sig()+1 \cdot Ver()$	$2\sigma \cdot F()+mk \cdot$MOD DIV $+2mk \cdot E_{ElGamal}()+mk \cdot D()$

표 1. 제안 모델과 NPS system의 계산량 비교

Bidder 입장에서 볼 때, NPS 시스템의 MOD DIV 연산은 약 $O(n^2)$의 복잡도를 가지며, 제안 모델의 MOD SQR 연산은 이보다 더 적은 복잡도를 갖는다. Auctioneer의 경우, NPS 시스템은 각 입찰자에 대해 2k번의 ElGamal 공개키 복호화 연산($D_{ElGamal}()$)과 k번의 복호화 연산을 수행해야 하는데 이는 $O(n^3)$의 복잡도가 된다. 반면 제안모델의 Auctioneer는 최종 낙찰자와 낙찰가를 선정하기 위해 총 $(m-1)(k+1)$번의 $D_{GM}()$ 연산을 수행하고 이의 복잡도는 $O(n^2)$이다. Auction Issuer입장에서 볼 때에도 NPS 시스템의 ElGamal 암호화 연산은 두 번의 MOD EXP 연산을 필요로 하며 그 계산 복잡도는 약 $O(n^3)$이고, MOD DIV 연산은 약 $O(n^2)$의 계산 복잡도를 갖는다. 이것은 제안 모델의 AIS가 갖는 계산 복잡도 $O(n^2)$보다 더 큰 값이다.

따라서 모든 party의 계산 복잡도에 대해 제안 모델이 NPS system 보다 더 좋다는 것을 알 수 있다.

4. 결론

본 논문에서는 확률론적 암호화 기법을 사용한 효율적이고 안전한 Vickrey 경매 모델을 제안하였으며, 이를 그 안전성이 입증된 NPS 시스템과 비교하여 계산복잡도 측면에서 더 효율적임을 입증하였다.

향후 제안 모델의 가정 사항이었던 Auctioneer와 AIS 간의 담합을 금지할 수 있는 방법에 대한 추가적인 연구가 필요한다.

참고문헌

1. K. Omote, "A Study on Electronic Auctions", March 2002.
2. C. Boyd, W. Mao, "Security Issues for Electronic Auctions", May 2002.
3. O. Goldreich, "Secure Multi-Party Computation", 1998.
4. A. C. Yao, "Protocols for secure computations", FOCS'82, pp.160-164, 1982.
5. M. Naor, B. Pinkas, R. Sumner, "Privacy preserving auctions and mechanism design", ACM Conference on Electronic Commerce, pp.129-139, 1999.
6. S. Goldwasser, S. Micali, "Probabilistic encryption", Journal of Computer and System Sciences, Vol.28, No. 1, pp.270-299. 1984