안전하고 효율적인 인터넷 경매를 위한 ECC(Elliptic Curves Cryptosystem)의 Blind Signature Protocol

성순화° 공은배
충남대학교 컴퓨터공학과 {shsung°, keb}@ce.cnu.ac.kr

Blind Signature Protocol of ECC(Elliptic Curves Cryptosystem) for Safe and Efficient Internet Auction

Soon Hwa Sung° Eun Bae Kong
Dept. of Computer Engineering, Chungnam University

요 약

본 연구는 기존의 인터넷 경매에서 Auctioneer와 Auction Issuer(AI)의 결탁을 막기 위한 안전하고 효율적인 경매 프로토콜인 blind signature protocol을 제안한다. 제안한 프로토콜에 사용되는 blind signature의 키는 안전성과 속도면에서 우수한 ECC(Elliptic Curves Cryptosystem)에서 생성한다. 이는 이전의 blind signature키에 사용한 RSA 키사이즈의 정수위에서 구현하는 것 보다 훨씬 암호강도가 세며 속도가 빠르다. 따라서 제안한 프로토콜은 독단적인 Auctioneer의 행동을 막을 수 있으며, Auctioneer와 AI의 결탁이 없는 안전하고 효율적인 인터넷 경매를 할 수 있다.

1. 서론

최근 인터넷 발전으로 EC(Electronic Commerce)의 질적 양적 발전이 빠르게 확장하면서 인터넷 경매 또한 빠르게 발전하고 있다. 1995년 시작한 인터넷 경매 ebay는 현재 세계 최대의 인터넷 경매 사이트로 존재하며 국내에서는 1998년 4월 옥션이 서비스를 시작하여 불과 1년 사이에 70여개의 인터넷 경매 사이트가 등장할 정도로 빠르게 성장하고 있다. 인터넷 경매는 온라인 환경을 기반으로 개인과 사업자들이 구매자나 판매자로서 일대다수의 관계로 새제품이나 중고제품의 거래에 참여하여 가격을 협상함으로써 최고의 효용을 얻으려는 시장형태이다. Kumar와 Feldman[1]는 인터넷의 경매 상품에 대한 application뿐만 아니라 인터넷 경매에 관한 몇가지 issues를 설명하며, Chui와 Zwick[2]는 상업적 인터넷 경매의 완전한 조사를 기술하고 있다. 이와 같이 입찰 주체에 따라 순경매와 역경매로 나눌 수 있으며, 순경매는 여러 구매자가 공동의 품목에 대해 입찰하는 반면 역경매는 여러 판매자가 공동의 구매자를 대상으로 경쟁하게 된다. 또한 입찰 가격 결정 방법에 따라 최고가 밀봉 입찰 경매(First Price Sealed Bid Auction), 차 최고가 밀봉입찰경매(Second Price Sealed Bid Auction)등 여러 종류가 있다. 본 논문에서 사용한 차 최고가 입찰경매(예:Vickrey auction[3])는 가장 높은 가격을 매긴 사람에게 두번째 높은 가격을 낙찰하는 방식으로 최고가 밀봉 입찰 방식과 비슷하나 두번째 가격을 낙찰자에게 가함으로써 최고 낙찰자를 보호할 수 있는 장점이 있다. 또한 두번째 가격의 사람에 대한 정보를 보호할 수 있다는 장점이 있다.

Moni Naor, Benny Pinkas, Reuben Sumner[4]이 제안한 인터넷 경매는 bidder, auctioneer, AI로 구성되며, bidders는 구매자나 판매자로서 구매정보를 auctioneer에게 전달하여 경매가 끝난 후 경매 가격을 받아 정확하게 계산되었는지 확인한다. Auctioneer는 bidders로부터 bids를 받아 AI와 통신하여 프로토콜 결과를 계산하는 경매구조 요소 중 한부분으로 bidders 중 한 사람이 될 수 있다. 프로토콜은 auctioneer가 프로토콜 결과 계산이외 어떠한 정보도 노출해서는 안된다는 것을 보장해야 한다. 그리고 AI는 privacy를 보호하기 위해 프로토콜 결과를 계산하는 coding program에 대해 책임을 지며, 이 프로그램을 auctioneer에게 전해준다. 이러한 인터넷 경매는 반드시 auctioneer와 auction issuer가 서로 결탁해서는 안된다는 가정이 있어야 한다. 이는 안전성면에서 기존의 많은 통신 프로토콜이 불안전한 채널과 정직한 호스트를 가정하여 설계되었기 때문이다. 따라서 본 연구는 기존의 인터넷 경매설계에서 auctioneer와 AI의 결탁이 없다는 가정 없이도 안전하고 효율적인 경매를 할 수 있는 프로토콜을 제안한다.

2. 관련연구

인터넷 경매 참가자는 개인의 입찰정보가 비밀을 유지하면서 Auctioneer와 AI의 결탁이 없는 공정한 경매 결과를 원한다. 따라서 본 장에서는 불안전한 채널과 부정직한 호스트에서 서로 신뢰할 수 없는 여러 프로세스들이 자신들의 비밀은 최대한 지키면서 그들의 비밀을 입력으

로 공통의 목적을 그들 스스로 안전하게 이루어내는 안전한 다자계산을 하는 방법과 경매 참가자의 입찰정보를 blind signature로 Auctioneer와 AI의 결탁이 있어도 안전한 인터넷 경매를 할 수 있는 프로토콜을 설명한다. 또한 blind signature의 encryption, decryption에 사용될 키는 RSA 키사이즈의 정수위에서 구현하는것 보다 훨씬 암호강도가 세며 속도가 빠른 ECC(Elliptic Curves Cryptosystem)에서 생성된다.

2.1 Multiparty Computation

다자간의 계산은 많은 곳에서 제안되었고[5,6,7], 이러한 다자간 계산을 바탕으로한 프로토콜은 안전한 경매에 제공된다. n명의 참가자 $P_1,P_2,\cdots,P_n$가 각각의 비밀정보 s_i를 가지고 있어서 각 P_i는 s_i를 비밀로 한 채 임의의 함수값$(s_1,\cdots,s_n)$을 알고 싶다고 할 때, 다자간 프로토콜은 신뢰할 만한 센터를 사용하지 않고 $f(s_1,\cdots,s_n)$의 값을 얻기 위해 $P_1,P_2,\cdots,P_n$사이의 메시지를 주고 받는 규칙이다. 이를 제시한 경매에 적용하면 각각의 파티들은 bidder 혹은 auctioneer가 되며, 함수 F는 AI가 된다. 즉 기존의 경매에서 auctioneer의 역할을 많이 줄여 AI에게 역할을 분산시켰다. 기존의 AI는 privacy를 보호하기 위해 프로토콜 결과를 계산하는 coding program에 대해 책임을 지며, 이 프로그램을 auctioneer에게 전해준다. 즉 AI는 많은 auctioneers에 의해 수행되는 많은 auctions을 위한 프로그램을 제공하는 service provider이다. 따라서 auctioneer와 AI가 결탁을 하면 신뢰 받을 수 있는 경매가 될 수 없다.

2.2 Blind Signature

Blind signature scheme은 Chaum[8]에 의해 처음으로 소개되었다. 이는 사용자가 실제 메시지나 결과 시그너처에 대해 어떠한 정보도 모른채 시스너처를 얻게 한다. 즉 RSA signatures를 사용하여 다른 party에 관한 어떠한 정보도 노출하지 않고 또다른 party에 의해 message signed를 얻게 되는 scheme이다. Chaum은 RSA signatures를 사용하여 다음과 같이 실행하였다. Alice는 Bob에 의해 sign되기를 원하는 메시지 m을 가지고 있고, 이 메시지m에 대해 Bob은 어떠한 정보도 모른다고 가정한다. Bob의 public key는 (n,e)이고, private key는 (n,d)이라고 한다. Alice는 gcd(r,n)=1인 램덤값 r을 생성하여 Bob에게 $m'=r^e m \bmod n$을 보낸다.

값 m'는 램덤값 r에 의해 blind되어서 Bob은 그것으로부터 어떠한 정보도 유추할 수 없다. Bob은 signed value $s'=(m')^d=(r^e m)^d \bmod n$ 를 Alice에게 보낸다. $s'= r m^d \bmod n$ 이므로 $s= s' r^{-1} \bmod n$를 계산하여 m의 signatures를 얻을 수 있다. 이때 Alice의 메시지는 자신이 얻을 수 없는 signature를 가진다. 이 signature scheme은 random r이 signer가 어려운 문제를 해결할 수 있을지라도 signer가 메시지에 대해 어떠한 정보를 알지 못하게 한다.

2.3 ECC(Elliptic Curve Cryptosystem)

ECC는 1985년 N.Koblitz[9]와 V.S.Miller[10]가 RSA암호화 방식에 대한 대안으로 처음 제안되었다.타원곡선을 이용, 유한체 위에서 새로운 공개키 암호화알고리즘을 만들지 않지만 기존의 공개키 알고리즘을 타원곡선을 이용해 구현했다. 즉 ECC는 특정암호알고리즘이 아니라 암호알고리즘을 구현해 볼 수 있는 수학적인 장소를 제공하고 있는 것으로 RSA, ElGamal등의 알고리즘을 기존의 정수공간이 아닌 타원 쌍곡선위에서 구현할 수 있다. 타원 쌍곡선위에서의 암호 구현은 수학적 복잡도 때문에 동일한 키사이즈의 정수위에서 구현하는것 보다 훨씬 강도가 세다는게 일반적인 평가다. ECC는 타원곡선의 이산대수문제를 바탕으로 유한체보다 훨씬 작은 크기의 키를 사용하면서도 같은 안전성을 얻을 수 있다는 장점이 있다.

3. The Procedure to Generate a Public key in ECC

(1)[receiver]Select any prime number p

(2)[receiver]Select any integer number a, b for EC such that $y^2=x^3+ax+b$

(3)[receiver]Select randomly an initial point P among points on EC

(4)[receiver]Generates a random integer as private key K_r

(5)[receiver]Computes a public key K_rP by multiplying P by K_r and registers it in the public key directory

(6)[receiver]Transmits p,a,b,P, K_rP to sender

(7)[sender]Receives p,a,b,P, K_rP from receiver

(8)[sender]Generates a random integer K_s as a private key

(9)[sender]Computes a public key K_sP by multiplying P by K_s and registers it in the public key directory

3.1 The Comparison of ECC with RSA

제안한 Blind Signature Protocol은 RSA 대신 ECC를 사용한다. 이는 ECC의 encryption과 decryption 시간을 RSA의 encryption과 decryption 시간과 비교하면 <표 1,2>[11]에서와 같이 ECC의 encryption과 decryption 시간이 적게 걸리기 때문이다.

표1 A comparison for encryption time (unit: μs)

Method of encryption / Key size(byte)	RSA	ECC
5	0.05	0.05
10	0.54	0.20
15	1.54	0.29
20	2.55	0.38
25	4.33	0.42
50	5.53	0.85
100	7.28	1.30

표2 A comparison for decryption time (unit: μs)

Method of encryption / Key size(byte)	RSA	ECC
5	0.11	0.10
10	0.55	0.50
15	1.20	0.80
20	3.08	1.10
25	6.21	1.15
50	8.06	2.12
100	9.95	3.21

4.Generating ECC key for the Blind Signature Protocol

제안한 인터넷경매는 Blind Signature Protocol 을 사용하여 auctioneer와 AI의 결탁없이 안전하고 효율적인 경매를 할 수 있다. 이때 사용하는 Blind Signature에 사용할 key는 다음과 같이 생성이 된다. 3장에서 [sender]는 bidder이며, [receiver]가 auctioneer이다. P는 ECC의 랜덤 initial point이며, bidder의 private key는 K_{bidder} , bidder의 public key 는 private key와 P의 곱 $K_{bidder}P$이다. Auctioneer의 private key는 $K_{auctioneer}$, public key는 private key와 P의 곱 $K_{auctioneer}P$이다. 프로토콜에 사용되는 메시지는 ID tag와 bidding value의 경매 정보로 이루어진다. ID tag는 bidder의 private key로 암호화하여 bidder는 물론 auctioneer, AI도 알 수가 없다. Bidding value는 auctioneer의 public key로 암호화하여 경매가 끝난 후 입찰가격을 알 수 있다. 따라서 bidder는 auctioneer의 public key $K_{auctioneer}P$와 bidder의 private key를 곱한 K_{bidder} ($K_{auctioneer}P$)를 blind signature로 사용한다.

4.1 The Blind Signature protocol Used in Internet Bidding

The Blind Signature Protocol은 <그림1>에서와 같이 진행된다. [1]Bidder가 암호한 경매정보를 blind signature하여 auctioneer에게 보낸다. [2]Auctioneer는 등록된 bidder인지 확인한 후 sign하여 bidder에게 보낸다. [3]Bidder는 다시 경매정보를 unblind하여 AI에게 보낸다. [4]AI는 암호한 경매정보를 bidder에게 공표한다. [5]Bidder는 확인 후, private key K_{bidder}를 AI에게 보낸다. [6]AI는 키 K_{bidder} 와 경매정보를 bidder에게 공표한다. 따라서 bidders는 그들 스스로 비밀을 지키면서 입찰가격을 알 수 있다.

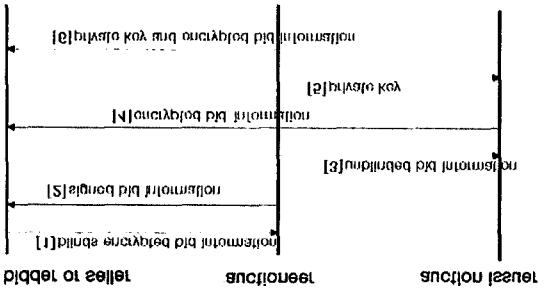

그림1 The Blind Signature Protocol in Internet Auction

5. 결론

인터넷경매의 구성요소가 bidder, auctioneer, AI로 이루어질 때, 안전한 경매가 되려면 auctioneer와 AI가 서로 결탁해서는 안된다는 가정이 있어야 한다. 본 연구에서는 auctioneer와 AI의 결탁이 있어도 안전하고 효율적인 경매가 이루어지는 프로토콜을 제시한다. 제시한 인터넷경매에서 blind signature에 사용되는 키는 타원곡선의 이산대수를 바탕으로 유한체보다 훨씬 작은 크기의 키를 사용하면서도 같은 안전성을 얻을 수 있는 ECC의 키를 사용한다. 이는 RSA 키사이즈의 정수위에서 구현하는 것보다 훨씬 암호강도가 세며 속도가 빠르므로 안전하고 효율적인 인터넷경매를 할 수 있다. 또한 기존 인터넷경매의 auctioneer의 역할을 분산시켜 그 역할을 감소시킴으로써 auctioneer의 독단적인 행위를 막을 수 있다.

참고문헌

[1]M.Kumar and S.I. Feldman, " Internet auctions" , 3rd USENIX Workshop on Electronic Commerce, 1999

[2]K. Chui and R. Zwick, " Auction on the Internet-A preliminary study" , manuscript, 1999. Available at http://home.ust.hk/~mkzwick/Internet_Auction.html

[3]D.Vickrey, " Counter speculation, auctions, and competitive sealed tenders" , journal of Finance, pp. 9-37, March 1961

[4]Moni Naor, Benny Pinkas, Reuben Sumner, " Privacy Preserving Auctions and Mechanism Design" , The Dept. of Computer Science and Applied Math, Weizmann Institute of Science, Rehovot 76100, Israel

[5]A.C.Yao. " Protocols for secure computations" , In Proc. 23rd IEEE Symposium on the Foundations of Computer Science(FOCS), pp.160-164, IEEE, 1982

[6]O.Goldreich, S.Micali, and A. Wigderson, " How to play any mental game-a completeness theorem for protocols with honest majority" , In Proc. 19th ACM Symposium on the Theory of Computing(STOC), pp.218-229, 1987

[7]O.Goldreich, " Secure Multi-Party Computation" , Working Draft, Version 1.3, pp.64, June 24,2001

[8]D.Chaum, R. Rivest, A. Sherman, " Blind signatures for untraceable payments" , Advances in Cryptology-Proceedings of CRYPTO, Corporation, 1982

[9]N.Koblitz, Elliptic Curve Cryptosystems. Math.Com. 48, pp.203-209, 1987

[10]V.S.Miller, Use of elliptic curve in cryptography. Advances in Cryptology-Proceedings of Crypto ' 85, Lecture Notes in Computer Science 218, pp.417-426, Springer-Verlag, 1986

[11]In-Seock Cho, Byung Kwan Lee, Tai-Chi Lee, " An ISEP(Improved Secure Electronic Payment) Protocol Design Using 3BC Algorithm" , SAM' 03(Security And Management' 03)International Conference Volume I, pp.78-84, CSREA, June 2003