2008－ICS－153 (6)
2008／10／30

セキュアキーワード広告オークションプロトコルの提案

櫻井 祐子[†a)] 鈴木幸太郎[††] 横尾 真[†††] 岩崎 敦[†††]

Secure Keyword Auction Protocol

Yuko SAKURAI[†a)], Koutarou SUZUKI[††], Makoto YOKOO[†††], and Atsushi IWASAKI[†††]

Abstract. キーワード広告オークションは，検索エンジンが検索結果に関連する広告の掲載順位を決定するために行われている．広告主は入札額を主催者（検索エンジン）に表明するが，主催者が入札額を知ることで，オークション結果を不正に操作する可能性が考えられる．従って，入札額を秘匿したまま，オークション結果を決定できることが望ましい．しかしながら，我々は，既存のキーワード広告オークションプロトコルの場合，入札額を秘匿したとしても，主催者は，支払額から入札額を求めることができることを示した．そこで，支払額から入札額が漏洩しにくいオークションプロトコル，及びそれを実現する暗号プロトコルを提案する．

Keywords. 電子商取引，メカニズムデザイン，暗号技術，キーワード広告オークション

1. はじめに

インターネットオークションは，電子商取引の重要な一分野となっている．インターネット上では，低コストで大規模なオークションを行うことが可能であり，日々，多数のオークションサイトで取引が行われている．また，インターネットオークションは，マルチエージェントやエージェント技術の有望な適用領域であり，多数の研究が存在する [1], [2].

インターネットオークションでは様々な財の取引が行われているが，近年，キーワード広告オークションと呼ばれるオークションの取引高が増加している．Yahoo!や Google などの検索エンジンでキーワードを検索した場合，検索結果の周囲に関連する広告が表示される．これらの広告はキーワード／検索連動型広告と呼ばれ，広告の掲載順位と支払額はオークションによって決定される．学術的にも，キーワード広告オークションに関する研究が多数行われている [3]〜[6].

キーワード広告オークションでは，一般化第二価格入札 (Generalized Second Price Auctoin, GSP) [4], [6] と呼ばれるオークションプロトコルが主に適用されている．GSP は第二価格秘密入札 (Vickrey オークション) を拡張したプロトコルである．まず，広告主は，主催者 (検索エンジン) に 1 つの検索キーワードに対して自分の広告がクリックされたときに支払ってよいと考える価格 (クリック単価) に基づく入札額を申告する．基本的には入札額の高い順に掲載順位が決定される．Vickrey オークションでは最高入札額者が 2 番目に高い入札額を支払うが，GSP では，掲載スロットを割り当てられた入札者は，直感的には自分の次の掲載順位の入札額を支払う．

GSP は，秘密入札型と呼ばれるオークション形式であり，入札者は主催者に入札額を申告しなければならない．入札者にとって入札に関する情報は私的情報であり，可能ならば誰にも公開しない方が望ましいと考えられる．一方，主催者は全ての入札額を知ることができるため，自らの収入を多くするために支払額を操作する可能性が指摘されている．例えば，Vickrey オークションの場合，主催者が集めた入札額の結果から最高入札額と 2 番目に高い入札額を知ることで，最高入札額よりもぎりぎり低い値を支払額として提示することで支払額を操作することが可能となる．

そこで，オークションを安全に実行するために，オークションプロトコルと暗号プロトコルを組み合わせて，セキュアなオークションプロトコルを提案する研究が行われている [7], [8], [10], [11]. 文献 [7] では，入札額が秘匿されたまま，割当てと支払額を計算することが

† 日本学術振興会特別研究員 (RPD)，九州大学大学院システム情報科学研究院
†† NTT 情報流通プラットフォーム研究所
††† 九州大学大学院システム情報科学研究院
a) E-mail: sakurai@agent.is.kyushu-u.ac.jp

可能となるセキュアなVickreyオークションが提案されている．さらに，組合せオークションプロトコルに拡張した一般化Vickreyオークション (VCG) に関しても暗号プロトコルを組み合わせることで，セキュアなVCGプロトコルが提案されている[10], [11].

キーワード広告オークションは同じ検索キーワードに対して何回も入札が繰り返される．従って，主催者に入札額を提示することで支払額を操作されるといった不正行為はより深刻な問題となりえる．また，主催者にとっても，掲載順位と支払額を決定する際に使用するパラメータ等は重要な企業情報の一つと考えられる．そこで，本論文では，入札額や主催者のパラメータを秘匿したままの状態で，掲載順位と支払額を決定することが可能なセキュアなキーワード広告オークションの提案を行う．

我々は，セキュアなキーワード広告オークションを考案するにあたり，既存プロトコルのGSPとVCGプロトコルに暗号プロトコルを組み合わせても，主催者は支払額を知ることで入札額を算出できることを示した．具体的には，GSPは支払額が次の入札額であるため，入札額を秘匿しても，支払額から，直接，入札額を知ることができる．また，VCGプロトコルでは支払額は入札額を変数とした一次方程式で表わされ，主催者は各掲載順位の支払額を知ることで，この一次方程式からなる連立方程式が得られる．この連立方程式では方程式の数と変数の入札額の個数が一致する．よって，入札額を秘匿しても，連立方程式を解くことで入札額を知ることができる．

そこで，本論文ではGSPを改良し，支払額から入札額が漏洩しにくい新しいキーワード広告オークションの提案を行う．基本的なアイデアは，主催者が支払額を知ることで，入札額を変数とした連立方程式を得たとしても解を求めることが不可能なように支払額を決定することである．さらに，このプロトコルに文献[8]で提案されているgarbled curcuitの手法を適用して，入札額を秘匿したままで正しい落札結果を計算する，セキュアなキーワード広告オークションを実現する．

本論文の構成は以下のとおりである．まず，第2.章で，キーワード広告オークションの問題の定式化を行う．次に，第3.章にて，既存プロトコルのGSPとVCGについて議論し，第4.章で新しいキーワード広告オークションプロトコルの提案を行う．さらに，第5.章で暗号プロトコルを組み合わせることでセキュアなキーワード広告オークションが実現できることを示す．最後に，第6.章で，計算機実験により，主催者の期待収入の比較を行う．

2. 問題の定式化

本章では，本論文におけるキーワード広告オークションの問題の定式化を行う．最大掲載広告数 K のキーワード広告オークションを考える．入札者 i は1つの検索キーワードに対して，自分の広告が1クリックされる毎に支払ってよいと考える価格 (クリック単価) を入札する．入札者 i のクリック単価の評価値を v_i，入札額を b_i とする．

GoogleやYahoo!は，入札者の入札額だけでなく，広告の品質とクリック率といったパラメータを考慮して掲載順位を決定する．広告の品質は，広告テキストとの関連性，過去の掲載結果，その他の関連性に関する要因によって決定される．クリック率は一般にClick-Through-Rate (CTR) と呼ばれ，広告のクリック数を表示回数で割った値である．広告の品質とクリック率を考慮した値は，Googleでは品質スコア，Yahoo!では品質インデックスと呼ばれている．品質スコアが低ければ入札額が高くても上位に掲載されない場合がある．一方，品質スコアが高ければ入札額が低くても掲載される場合がある．

品質スコアは，一般に，キーワード広告オークションの理論的な解析において広告の品質とクリック率は分離可能であると仮定している[5], [6]．広告の品質は各入札者に依存し，クリック率は掲載順位に依存するとする．具体的には，入札者 i の広告の品質を q_i，上位 j 番目のクリック率を C_j とし，$C_j > C_{j+1}$ を仮定する．よって，広告の品質が q_i の入札者 i に関して上位 j 番目の掲載順位における品質スコア $\theta_{i,j}$ は

$$\theta_{i,j} = C_j q_i \tag{1}$$

となる．

GoogleやYahoo!では，最低入札額が設定されており，最低入札額以上の入札者が掲載できる権利を得る．品質スコアによって，各入札者の最低入札額が異なり，高い品質スコアの入札者は低い品質スコアの入札者より最低入札額は低くなる．本論文では，広告の品質 q_i と入札額 b_i の積 $q_i b_i$ に閾値 r を設定する．すなわち，

$$q_i b_i \geqq r \tag{2}$$

を満たす入札者が掲載対象となる権利を得る．

入札者の効用は準線形効用とする．上位 i 番目の掲

載順位の入札者 $b_{(i)}$ が 1 クリック毎に支払うクリック単価を $p_{(i)}$ とする．このときの期待利得 $u_{(i)}$ は次の通りに定義する．

$$u_{(i)} = C_i q_{(i)}(v_{(i)} - p_{(i)}) \tag{3}$$

本論文では，セキュアなキーワード広告オークションとは，入札者や主催者が個々に有する情報を誰にも知られることなく，掲載順位と支払額が決定され，主催者は支払額から各入札額が漏えいされないオークションと定義する．

3. 既存プロトコル

本章では，Google や Yahoo!のキーワード広告オークションで適用されている一般化第二価格入札 (GSP) と戦略的操作不可能性を満たすオークションプロトコルとして知られている一般化 Vickrey オークション (VCG) プロトコルについて述べる．

3.1 GSP

3.1.1 プロトコルの詳細

以下，GSP プロトコルの詳細を述べる．

（1） 主催者は最大掲載数 K と最低入札額 r を決定する．

（2） 入札者 i は入札額 b_i を主催者に申告する．$q_i b_i \geq r$ ならば，入札できる権利を得る．

（3） 主催者は入札額 b_i と品質 q_i の積の降順に並べ替える．

$$q_{(1)}b_{(1)} \geq q_{(2)}b_{(2)} \geq \ldots \geq q_{(i)}b_{(i)} \geq \ldots \tag{4}$$

$b_{(i)}$ は上位 i 番目の掲載順位の入札額を表し，$q_{(i)}$ はその入札者の品質を示す．

（4） $q_{(K)}b_{(K)} \geq r$ ならば，上位 K 番目までの入札者が広告を掲載できる．$q_{(K)}b_{(K)} < r$ ならば，$q_{(i)}b_{(i)} \geq r$ を満たす入札者が広告を掲載できる．

（5） i 番目の入札者の支払額 $p_{(i)}$ は

$$p_{(i)} = q_{(i+1)}b_{(i+1)}/q_{(i)} \tag{5}$$

$q_{(j+1)}b_{(j+1)}$ が最低入札額 r よりも低ければ，r を用いて支払額を計算する．

GSP の具体例を下記に示す．

[例 1] 最大掲載数 K が 3，入札者が 4 人存在するとする．広告の品質は全てのエージェントで同一 $(\forall i,\ q_i = 1)$，最低入札額は 0，クリック率は $(C_1, C_2, C_3) = (1, 0.8, 0.6)$ とする．入札者の評価値はそれぞれ $v_1 = 12$，$v_2 = 10$，$v_3 = 8$，$v_4 = 6$ とする．このとき，入札者は各々の評価値を入札すると仮定する $(b_i = v_i)$．

$q_i b_i$ に関して，$q_i = 1$ より，$12 > 10 > 8 > 6$ となり，入札者 1 が最上位，入札者 2 が 2 番目，入札者 3 が 3 番目となる．各々の支払額は $p_{(1)} = 10$，$p_{(2)} = 8$，$p_{(3)} = 6$ となる．結果，主催者の収入の期待値は $C_1 p_{(1)} + C_2 p_{(2)} + C_3 p_{(3)} = 18$ となる．効用は $u_{(1)} = 12 - 10 = 2$，$u_{(2)} = 0.8(10 - 8) = 1.6$，$u_{(3)} = 0.6(8 - 6) = 1.2$ となる．

なお，GSP は，過大申告 (真の評価値よりも高い入札をする) によって効用が増加する可能性がない一方，過少申告 (真の評価値よりも低い値を入札する) を行うことで，効用が増加する可能性があることが知られている．

3.1.2 セキュアオークションの実現可能性

本節では GSP を適用してセキュアなキーワード広告オークションが実現できるかという課題に関して考察する．GSP では，i 番目の支払額 $p_{(i)}$ は 式 (5) から，$i+1$ 番目の掲載順位の入札額 $b_{(i+1)}$ によって決定される．従って，b_i を秘匿したまま，掲載順位と支払額を計算したとしても，主催者が支払額の情報を得ることで，$b_{(2)}$ から $b_{(K+1)}$ までを知ることが可能となる．よって，GSP を適用して，セキュアキーワード広告オークションを実現することはできない．

3.2 VCG

前節で，我々は，GSP がセキュアキーワード広告オークションを実現できないことを指摘した．従って，次の検討として，本節では，支払額が GSP よりも複雑であり，真の評価値を申告することが最適な戦略である，すなわち，戦略的操作不可能性を満たす，VCG プロトコルに対して議論する [12]．

3.2.1 プロトコルの詳細

VCG プロトコルをキーワード広告オークションに適用した場合のプロトコルの詳細を示す．

（1） 主催者は最大掲載数 K と最低入札額 r を決定する．

（2） 入札者 i は入札額 b_i を主催者に申告する．$q_i b_i \geq r$ ならば，入札できる権利を得る．

（3） 主催者は入札額 b_i と品質 q_i の積の降順に並べ替える．

$$q_{(1)}b_{(1)} \geq q_{(2)}b_{(2)} \geq \ldots \geq q_{(i)}b_{(i)} \geq \ldots \tag{6}$$

（4） i 番目の入札者の支払額 $p_{(i)}$ は

$p_{(i)} =$

$$\frac{1}{C_i q_{(i)}}\{(\sum_{j=1}^{i-1} C_j q_{(j)} b_{(j)} + \sum_{j=i}^{K} C_j q_{(j+1)} b_{(j+1)})$$
$$-(\sum_{j=1}^{K} C_j q_{(j)} b_{(j)} - C_i q_{(i)} b_{(i)})\} \quad (7)$$

$q_{(j+1)}b_{(j+1)}$ が最低入札額 r よりも低ければ，r を用いて支払額を計算する．

VCG の具体例を下記に示す．

［例 2］ 例 1 と同様に，最大掲載数 K が 3，入札者が 4 人存在するとする．広告の品質は全てのエージェントで同一 ($\forall i,\ q_i = 1$)，最低入札額は 0，クリック率は $(C_1, C_2, C_3) = (1, 0.8, 0.6)$ とする．入札者の評価値はそれぞれ $v_1 = 12$，$v_2 = 10$，$v_3 = 8$，$v_4 = 6$ とする．

結果，入札者 1 が最上位，入札者 2 が 2 番目，入札者 3 が 3 番目となる各々の支払額は $p_{(1)} = 7.2$，$p_{(2)} = 6.5$，$p_{(3)} = 6$ である．よって，主催者の収入の期待値は 15 となる．

3.2.2 セキュアオークションの実現性

VCG に関しては，一般的な財を対象とした組合せオークションにおいて，暗号技術を適用することでセキュアな VCG プロトコルの提案が行われている [10]．しかしながら，VCG をキーワード広告オークションプロトコルとして適用した場合，セキュアなオークションを実現できない．

以下，$K = 3$ のときの支払額を具体的に示すことで，実現不可能であることを説明する．

$$\begin{aligned}
&p_{(1)} \\
&= 1/C_1 q_{(1)}\{(C_1 q_{(2)} b_{(2)} + C_2 q_{(3)} b_{(3)} + C_3 q_{(4)} b_{(4)}) \\
&\quad -(C_2 q_{(2)} b_{(2)} + C_3 q_{(3)} b_{(3)})\} \\
&= 1/C_1 q_{(1)}\{(C_1 - C_2) q_{(2)} b_{(2)} \\
&\quad +(C_2 - C_3) q_{(3)} b_{(3)} + C_3 q_{(4)} b_{(4)}\} \\
&p_{(2)} \\
&= 1/C_2 q_{(2)}\{(C_2 q_{(3)} b_{(3)} + C_3 q_{(4)} b_{(4)}) - C_3 q_{(3)} b_{(3)}\} \\
&= 1/C_2 q_{(2)}\{(C_2 - C_3) q_{(3)} b_{(3)} + C_3 q_{(4)} b_{(4)}\} \\
&p_{(3)} = q_{(4)} b_{(4)} / q_{(3)}
\end{aligned}$$

CTR C_j と品質 q_i は主催者が決定する値である．主催者は，$p_{(3)}$ から $b_{(4)}$ を知ることができる．さらに，$p_{(2)}$ は $b_{(3)}$ と $b_{(4)}$ から計算されるため，$p_{(2)}$ と $p_{(3)}$ の値を知ることで $b_{(3)}$ がわかる．同様に，$p_{(1)}$ を知ることで，$p_{(2)}$ と $p_{(3)}$ の値から $b_{(2)}$ がわかる．結果，GSP と同様に，掲載数が K のとき，主催者に $b_{(2)}$ から $b_{(K+1)}$ の入札額の値を知られることとなる．

VCG の支払額は，直感的には，その入札者がいないときに得られる最適な社会的余剰 (第 1 項) から，実際の最適な社会的余剰から入札者の効用を引いた値 (第 2 項) の差分となっている．キーワード広告オークションに VCG を適用した場合，支払額 $p_{(i)}$ の第 1 項と第 2 項を構成する入札額について見ると，第 1 項目 $b_{(i+1)}$ から $b_{(K+1)}$ であり，第 2 項目は $b_{(i+1)}$ から $b_{(K)}$ で構成されている．従って，全ての $p_{(i)}$ は $b_{(i+1)}$ から $b_{(K+1)}$ までの線形方程式で表現される．すなわち，主催者は $b_{(2)}$ から $b_{(K+1)}$ までの K 個の変数と $p_{(1)}$ から $p_{(K)}$ までの K 個の線形方程式からなる連立方程式を得ることとなる．従って，変数と方程式の数が一致する連立方程式であるため，主催者は入札額を知ることが可能となる．

一方，一般の組合せオークションでは，入札者は財の組合せに対して入札するため，勝者ごとの支払額の第 1 項と第 2 項を構成する入札者や財の組合せがより複雑である．従って，変数と方程式の数が同一の連立一次方程式とはならず，支払額から入札額を算出することは不可能である．

4. GSP の改良

前章では，既存プロトコルに暗号プロトコルを組合わせても，主催者が支払額を知ることで，入札額を計算できることを示した．そこで，我々は，新しいオークションプロトコルと，それを実現する暗号プロトコルの提案を行う．

新しいオークションプロトコルの提案に関して，支払額の計算が容易でありながら，主催者に支払額から入札額が漏洩しにくいことをメカニズム設計の目標とする．オークションプロトコルの支払額の計算方法が難しくなれば，支払額から入札額が漏洩されることが困難になる．しかしながら，利用者にとって支払額の計算方法が難しいことは望ましくないと考えられる．従って，我々は，現在適用されている GSP をベースに新しいプロトコルを提案する．

さらに，支払額から入札額が漏洩しないようにするためには，支払額 $p_{(i)}$ に関する連立方程式の数と変数 $b_{(i)}$ の数が一致しないように支払額を決定しなければならない．VCG では，支払額 $p_{(i)}$ に関する連立方程式の数と変数 $b_{(i)}$ の数が一致したため，入札額を秘匿したとしても，主催者は支払額を知ることで，入札額

を算出することができた．そこで，変数 $b_{(i)}$ の数を連立方程式の数よりも多くなるように支払額を定義する．

4.1 プロトコルの詳細

プロトコルの詳細は以下のとおりである．支払額の決定方法以外は GSP と同様である．

（1） 主催者は最大掲載数 K と最低入札額 r を決定する．

（2） 入札者 i は入札額 b_i を主催者に申告する．$q_i b_i \geq r$ ならば，入札できる権利を得る．

（3） 主催者は入札額 b_i と品質 q_i の積の降順に並べ替える．

$$q_{(1)}b_{(1)} \geq q_{(2)}b_{(2)} \geq \ldots \geq q_{(i)}b_{(i)} \geq \ldots \qquad (8)$$

（4） i 番目の入札者の支払額 $p_{(i)}$ は

$$p_{(i)} = \frac{q_{(i+1)}b_{(i+1)} + q_{(i+2)}b_{(i+2)}}{2q_{(i)}} \qquad (9)$$

$b_{(i+1)}$，$b_{(i+2)}$ が最低入札額よりも低ければ，最低入札額を用いて支払額を決定する．

[例 3] 例 1 と同様に，最大掲載数 K が 3，入札者が 4 人存在するとする．広告の品質は全てのエージェントで同一 ($\forall i,\ q_i = 1$)，最低入札額は 4，クリック率は $(C_1, C_2, C_3) = (1, 0.8, 0.6)$ とする．入札者の評価値はそれぞれ $v_1 = 12$，$v_2 = 10$，$v_3 = 8$，$v_4 = 6$ とする．

結果，入札者 1 が最上位，入札者 2 が 2 番目，入札者 3 が 3 番目となる各々の支払額は $p_{(1)} = 9$，$p_{(2)} = 7$，$p_{(3)} = 5$ である．よって，主催者の収入の期待値は 17.6 となる．

4.2 セキュアオークションの実現可能性

本節では，提案メカニズムは GSP，VCG と異なり，主催者が入札額を知ることが困難であることを示す．

以下，簡単化のため，全て入札者の品質 q_i について $q_i = 1$ の場合を考える．このとき，i 番目の入札者の支払額は $p_{(i)} = (b_{(i+1)} + b_{(i+2)})/2$ となる．従って，$p_{(1)}$ から $p_{(K)}$ からまでの K 個の支払額を知ることで，$b_{(2)}$ から $b_{(K+2)}$ の値の範囲を知ることが可能となる．具体的には，$b_{(2)}$ について，

$$p_{(1)}/2 \leqq b_{(2)} \leqq (2p_{(1)} - p_{(2)})/2 \qquad (10)$$

3 から $K+2$ 番目の入札者 i $(3 \leqq i \leqq K+2)$ の入札額 $b_{(i)}$ に対して，

$$p_{(i-2)}/2 \leqq b_{(i)} \leqq p_{(i-1)}/2 \qquad (11)$$

というように，入札額の範囲 (上限と下限) を知ることが可能である．

しかしながら，主催者は，支払額が $p_{(i)} = (b_{(i+1)} + b_{(i+2)})/2$ であることより，支払額 $p_{(1)}$ から $p_{(K)}$ からまでの K 個の一次方程式からなる連立方程式を得ることとなる．この連立方程式は，$b_{(2)}$ から $b_{(K+2)}$ までの $K+1$ 個の変数 $b_{(i)}$ で構成されている．従って，方程式の数よりも変数の方が 1 つ多いため，$p_{(i)}$ の連立方程式から $b_{(i)}$ を算出することはできない．

以上より，提案プロトコルでは，主催者は $b_{(2)}$ から $b_{(K+2)}$ の入札額の範囲を知ることが可能であるが，既存プロトコルのように，入札額そのものを知られることはない．

4.3 プロトコルの戦略的操作不可能性

オークションプロトコルの望ましい性質の 1 つに，戦略的操作不可能性 (真の評価値を申告することが最適な戦略) がある．GSP は過大申告に関して頑健であるが，過小申告に対しては脆弱であることが知られている．新しいプロトコルも同様に過小申告に関しては脆弱である．一方，過大申告に関しては，以下の性質を導くことができる．

[定理 1] 新しいプロトコルは，過大申告に関して，以下を保証する．

- 真の評価値を申告した場合の掲載順位と比較して 2 つ以上の順位が上がるような過大申告をしても効果がない，
- 1 つ上の順位になるような過大申告に関して，各入札者の評価値の分布に上限があるとき，
  - 真の評価値を申告した場合の掲載順位が i のとき，$C_{(i-1)} < 2C_{(i)}$ ならば過大申告の効果がない．
  - また，$C_{(i-1)} \geq 2C_{(i)}$ の場合でも，効用の増加分はある上限で抑えられる．

[証明 1] まず，i 番目の入札者は順位が 2 つ以上，上がるような過大申告をしても効果がないことを示す．

i 番目の入札者が 2 つ上がるような入札をしたときの支払額は，

$$p'_{(i-2)} = (q_{(i-2)}b_{(i-2)} + q_{(i-1)}b_{(i-1)})/2q_{(i)}$$

となる．このとき，$p'_{(i-2)} > q_{(i-1)}b_{(i-1)}/q_{(i)}$ であり，自分の評価値以上を支払うこととなる．

次に，i 番目の入札者は順位が 1 つ以上，上がるような過大申告をしたとき，その効用の増加分には上限が存在することを示す．いま，$[0, v_{max}]$ の範囲で評価値は与えられ，全ての入札者 i に対して $q_i = 1$ とす

る．さらに，留保価格は $r=0$ とする．このとき，$v_{(i)}$ と $b_{(i-1)}$，$b_{(i+1)}$，$b_{(i+2)}$ には下記の関係で値が与えられるとする．

- $b_{(i-1)} = v_{(i)} + a_1$
- $v_{(i)}$
- $b_{(i+1)} = v_{(i)} - a_2$
- $b_{(i+2)} = v_{(i)} - a_3$

このとき，過大申告して 1 つ上の順位に上がることで効用が増加する場合，すなわち，効用 $C_{(i-1)}(v_{(i)} - (b_{(i-1)} + b_{(i+1)})/2)$ が正となるとき，以下が導かれる．

$$v_{(i)} - (b_{(i-1)} + b_{(i-2)})/2 > 0 \text{ より } a_1 < a_2.$$

従って，$a_1 < a_2 < a_3$.

真の評価値を申告した場合と効用の比較を行うと

$$\begin{aligned} & C_{(i-1)}(v_{(i)} - (b_{(i-1)} + b_{(i+1)})/2) \\ & \quad -C_{(i)}(v_{(i)} - (b_{(i+1)} + b_{(i+2)})/2) \\ & = (C_{(i-1)} - C_{(i)})a_2/2 - C_{(i-1)}a_1/2 - C_{(i)}a_3/2 \\ & < (C_{(i-1)} - 2C_{(i)})a_2/2 \\ & < (C_{(i-1)} - 2C_{(i)})v_{max}/4 \end{aligned}$$

よって，$C_{(i-1)} - 2C_{(i)} < 0$，すなわち，$C_{(i-1)} < 2C_{(i)}$ のときは効用の増分が負になるため効果がない．さらに，$C_{(i-1)} \geqq 2C_{(i)}$ の場合においても，効用の増分の上限は $(C_{(i-1)} - 2C_{(i)})v_{max}/4$ で抑えられる．

5. セキュアキーワード広告オークション

本章では，文献 [8] で提案されている garbled circuit を用いた方式を適用することにより，前章で提案したオークションプロトコルを入札額などを秘匿したまま計算できる暗号プロトコルを提案する．提案暗号プロトコルでは，主催者は最大掲載数 K，最低入札額 r，品質 q_i を，入札者 i は入札額 b_i を秘匿したまま，主催者が掲載順位と支払額 $p_{(i)}$ を計算することができる．

5.1 準　　備

まず，提案暗号プロトコルに必要な garbled circuit と proxy oblivious transfer について説明を行い，文献 [8] で提案されている garbled circuit を用いた方式の概要を説明する．

5.1.1 garbled circuit の概要

garbled circuit は，Yao [13] により提案された，任意の回路 F の出力値 $F(x)$ を入力値 x を秘匿したまま計算できる手法であり，疑似ランダム関数を用いて以下のように構成される．

k をセキュリティパラメータとする．$f_w(c) : \{0,1\}^{2k} \times \{0,1\}^2 \longrightarrow \{0,1\}^{k+1}$ を鍵 $w \in \{0,1\}^{2k}$ を持つ疑似ランダム関数とする．

乱数 $w_i^0, w_i^1 \in \{0,1\}^k$ と乱数 $c_i^0 \in \{0,1\}$ を生成し，$c_i^1 = c_i^0 \oplus 1$ とし，回路 F の論理ゲートをつなぐワイヤ i に対して値 $((w_i^0, c_i^0), (w_i^1, c_i^1))$ を割り当てる．(w_i^0, c_i^0) はワイヤ i の値が 0 であることを，(w_i^1, c_i^1) はワイヤ i の値が 1 であることを表す．

入力ワイヤ i と j，出力ワイヤ k を持つ，回路 F の論理ゲート $g : \{0,1\} \times \{0,1\} \longrightarrow \{0,1\}$ に対して，以下のような表を割り当てる．

$$(c_i^0, c_j^0) : (w_k^{g(0,0)}, c_k^{g(0,0)}) \oplus f_{w_i^0||w_j^0}(c_i^0||c_j^0)$$

$$(c_i^0, c_j^1) : (w_k^{g(0,1)}, c_k^{g(0,1)}) \oplus f_{w_i^0||w_j^1}(c_i^0||c_j^1)$$

$$(c_i^1, c_j^0) : (w_k^{g(1,0)}, c_k^{g(1,0)}) \oplus f_{w_i^1||w_j^0}(c_i^1||c_j^0)$$

$$(c_i^1, c_j^1) : (w_k^{g(1,1)}, c_k^{g(1,1)}) \oplus f_{w_i^1||w_j^1}(c_i^1||c_j^1)$$

入力 b_i, b_j に対応する値 $(w_i^{b_i}, c_i^{b_i}), (w_j^{b_j}, c_j^{b_j})$ を知っていれば，$f_{w_i^{b_i}||w_j^{b_j}}(c_i^{b_i}||c_j^{b_j})$ を計算することができ，表から出力 $b_k = g(b_i, b_j)$ に対応する値 $(w_k^{b_k}, c_k^{b_k})$ を求めることができる．

回路 F の各論理ゲートに対して上記の表を構成し，それらの表を並べたものが回路 F に対応する garbled circuit F' である．ただし，回路 F の出力段の論理ゲートに対応する表では，$c_k^0 = 0$ とする．

入力 $x = (x_1, x_2, ...)$ に対応する値 $((w_1^{x_1}, c_1^{x_1}), (w_2^{x_2}, c_2^{x_2}), ...)$ と，回路 F に対応する garbled circuit F' が与えられると，上記のように論理ゲートごとに表を引くことにより，回路 F の出力値 $F(x)$ を入力 $x = (x_1, x_2, ...)$ を知らずに計算することができる．

5.1.2 proxy oblivious transfer の概要

oblivious transfer は，秘密情報 w^0, w^1 を持つ送信者と，秘密情報 b を持つ受信者が行う暗号プロトコルである．oblivious transfer を実行すると，送信者に b を，受信者に $w^{b\oplus 1}$ を秘匿したまま，受信者は w^b を得ることができる．

proxy oblivious transfer は，文献 [8] で提案された，秘密情報 w^0, w^1 を持つ送信者と，受信者と，秘密情報 b を持つ選択者が行う暗号プロトコルである．proxy oblivious transfer を実行すると，送信者と受信者に b

を，受信者に $w^{b\oplus 1}$ を秘匿したまま，受信者は w^b を得ることができる．

5.1.3 文献[8]の方式の概要

文献[8]は，garbled circuit と proxy oblivious transfer を用いた，以下のようなセキュアオークションプロトコルを提案した．

（1） 回路生成者は，入力が入札額 b_i，出力がオークションの結果，であるオークション計算回路 F に対応する garbled circuit F' を作成し，主催者に送信する．

（2） 入札者 i は，proxy oblivious transfer を用いて，入札額 b_i に対応する F' の入力値を，回路生成者から主催者に送信してもらう．

（3） 主催者は，受信した F' の入力値を用いて garbled circuit F' の計算を行い，オークション計算回路 F の出力値であるオークションの結果を得る．

5.2 提案セキュアキーワード広告オークション

提案暗号プロトコルは以下の3者により実行される．

- 回路生成者: garbled circuit を作成する．
- 主催者: 秘密情報である最大掲載数 K，最低入札額 r，品質 q_i を持つ．
- 入札者 i: 秘密情報である入札額 b_i 持つ．

提案暗号プロトコルは以下のように実行される．

（1） 回路生成者は，入力が最大掲載数 K，最低入札額 r，品質 q_i，入札額 b_i，出力が掲載順位と支払額 $p_{(i)}$，であるオークション計算回路 F に対応する garbled circuit F' を作成し，主催者に送信する．

（2） 入札者 i は，proxy oblivious transfer を用いて，入札額 b_i に対応する F' の入力値を，回路生成者から主催者に送信してもらう．

（3） 主催者は，oblivious transfer を用いて，最大掲載数 K，最低入札額 r，品質 q_i に対応する F' の入力値を，回路生成者から送信してもらう．

（4） 主催者は，受信した F' の入力値を用いて garbled circuit F' の計算を行い，オークション計算回路 F の出力値である掲載順位と支払額 $p_{(i)}$ を得る．

提案暗号プロトコルは，ほぼ文献[8]の手法を前章で提案したオークションプロトコルに適用したものであるが，主催者も秘密情報を持っているため上記ステップ (3) が追加されている点が文献[8]の手法とは異なる．

回路生成者について，回路が何の回路かは分かるが，oblivious transfer で受信者がどちらのメッセージを受け取ったかが回路生成者には分からないため，入力の値を知ることは一切ない．回路生成コストに関しては，回路のゲート数を n とするとき，$O(n)$ のハッシュ関数の計算が必要となる．さらに，計算を行う際に，入力の総ビット数を l とすると $O(l)$ の (proxy) oblivious transfer が必要である．このため，$O(l)$ の公開鍵暗号演算と $O(l)$ の通信が必要となるが，文献[9]の方式を適用することにより，公開鍵暗号の計算を行わずに効率的に実行することができる．

表1 (C1), (V1) の場合の GSP に対する期待収入の比較

K	n	VCG	提案プロトコル	VCG の方が高いインスタンス数
3	5	0.817	0.851	31
5	10	0.836	0.936	3
10	100	0.971	0.995	0

表2 (C2), (V2) の場合の GSP に対する期待収入の比較

K	n	VCG	提案プロトコル	VCG の方が高いインスタンス数
3	5	0.643	0.761	6
5	10	0.617	0.828	0
10	100	0.852	0.965	0

表3 (C2), (V1) の場合の GSP に対する期待収入の比較

K	n	VCG	提案プロトコル	VCG の方が高いインスタンス数
3	5	0.746	0.824	12
5	10	0.809	0.930	0
10	100	0.975	0.995	0

6. 評価実験

提案プロトコルは GSP，VCG と同様の方法で掲載順位を決定するため，と同じ社会的余剰が得られる．しかしながら，主催者の収入は，理論的には GSP よりも低い値しか得られない．一方，例 1，2，3 にて，GSP，VCG，提案プロトコルにおける，収入の期待値を求めた．結果，提案プロトコルの方が VCG よりも良い収入を得ることができている．従って，提案プロトコルの方が VCG と比較して，より良い期待収入を得ることができるかの検証も必要であると考える．そこで，計算機実験を用いて，GSP，VCG，提案プロトコルで得られる期待収入の比較を行う．

クリック率は，(C1) 一様分布と (C2) 文献[5]と同様に実証データを参考にしたものの2つの状況で実験を行う．実証データに基づくクリック率は，具体的には，減少率を α としたとき，最上位のクリック率 $C_{k,1}$ に対して $C_{k,1} = C_{k+1,1} + C_{k+1,1}\alpha^k/(1+\alpha+\cdots+\alpha^k)$

とし，$C_{k,j}$ $(j \geqq 2)$ は，$C_{k,j} = C_{k,1}\alpha^{j-1}$ とする．本実験では $C_{1,1} = 1$，$\alpha = 0.5$ とする．また，入札額 v_i は，(V1) 一様分布と (V2) ベキ乗分布 $(y = 100v_i^{-r})$ の 2 種類の実験を行う．べき乗分布における y は v_i 以上の値をとりうる確率をあらわす．ベキ分布を適用することにより，低い入札額が多い一方で，高い入札額が少ない状況をモデル化している．本実験では $r = 1.22$ とした．さらに，最低入札額は 0，品質は全ての入札者について $q_i = 1$ とする．この問題設定において，各 100 インスタンスを実行した結果を表 1，2，3 に示す．VCG，提案プロトコルの項目は，GSP での期待収入に対する VCG と提案プロトコルの期待収入の比率を示す．

表 1 は，CTR を (C1)，評価値を (V1) に設定した場合の結果を示す．提案プロトコルの方が VCG よりも平均的に収入が高い．しかしながら，掲載数が 3，入札者数が 5 の場合，31 インスタンスで VCG での収入の方が高い場合がある．表 2 は，CTR を (C2)，評価値を (V2) に設定した場合の結果を示す．全てのパラメータ設定において 10%以上も提案プロトコルの方が平均的に収入が多く，規模が大きい掲載数が 10，入札者数が 100 の場合，提案プロトコルは 97 %に達している．表 3 は，CTR を (C2)，評価値を (V1) に設定した場合の結果を示す．この設定でも，提案プロトコルの方が VCG よりも平均的に収入が高い．評価値が一様分布であるため，入札数が多いほど，入札額を降順に並べた場合の隣接する 2 つの入札額の差分が少なくなるため，GSP と比較して得られる収入の比率は提案プロトコルは 99 %まで達することができる．これら計算機実験により，提案プロトコルは，平均的に VCG よりも良い収入が得られ，入札者数が多くなればなるほど，GSP との差が減少し，ほぼ同等の結果が得られることがわかった．

7. おわりに

本論文では，入札額を秘匿したまま，オークション結果を決定できる，セキュアなキーワード広告オークションプロトコルの提案を行った．まず，我々は，入札額を秘匿したまま，既存の GSP や VCG を利用してオークション結果を求めても，主催者は支払額から入札額を知ることができることを指摘した．従って，支払額から入札額が漏洩しにくいオークションプロトコルを提案し，それを実現する暗号プロトコルを提案した．提案プロトコルは GSP をベースにしており，実用性は高いと考えられる．さらに，計算機実験により，新しいプロトコルの期待収入は，既存の GSP と比較してほぼ同等の結果が得られることを示した．

今後の課題としては，支払額の計算を難しくすることなく，入札額に関する情報が全く漏洩しない，よりセキュアなキーワード広告オークションを提案することがある．

文　献

[1] P. Cramton, Y. Shoham and R. Steinberg Eds.: "Combinatorial Auctions", MIT Press (2006).

[2] 横尾："オークション理論の基礎", 東京電機大学出版会 (2006).

[3] G. Aggarwal, A. Goel and R. Motwani: "Truthful auctions for pricing search keywords", Proceedings of the 7th ACM conference on Electronic commerce (EC'06), pp. 1–7 (2006).

[4] B. Edelman, M. Ostrovsky and M. Schwarz: "Internet advertising and the generalized second price auction: Selling billions of dollars worth of keywords", American Economic Review, 97, pp. 242–259 (2007).

[5] 櫻井, 岩崎, 横尾："適切な掲載数を決定するキーワード広告オークションの提案", コンピュータソフトウェア (ソフトウェア科学会論文誌),「ソフトウェアエージェント とその応用」特集号, (2008). to appear.

[6] H. R. Varian: "Position auctions", International Journal of Industrial Organization, 25, 6, pp. 1163–1178 (2007).

[7] M. Abe and K. Suzuki: "M+1-st price auction using homomorphic encryption", Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems, pp. 115–124 (2002).

[8] M. Naor, B. Pinkas and R. Sumner: "Privacy preserving auctions and mechanism design", In Proceedings of the 1st ACM Conference on Electronic Commerce, pp. 129–139 (1999).

[9] K. Chida and K. Takahashi: "Privacy Preserving Computations without Public Key Cryptographic Operation", Proceedings of the 3rd International Workshop on Security (IWSEC2008), (2008).

[10] K. Suzuki and M. Yokoo: "Secure generalized vickrey auction using homomorphic encryption", Proceedings of the 7th International Financial Cryptography Conference (FC-03), pp. 239–249 (2003).

[11] M. Yokoo and K. Suzuki: "Secure generalized vickrey auction without third-party servers", Proceedings of the 8th International Financial Cryptography Conference (FC-04), pp. 132–146 (2004).

[12] V. Krishna: "Auction Theory", Academic Press (2002).

[13] A. Yao: "How to Generate and Exchange Secrets", Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS-86), pp. 162–167 (1986).