【13】

氏名	中西 透（なかにし とおる）
博士の専攻分野の名称	博士（工学）
学位記番号	第 15753 号
学位授与年月日	平成12年10月24日
学位授与の要件	学位規則第4条第1項該当 基礎工学研究科物理系専攻
学位論文名	Anonymous Digital Signatures and Their Applications to Bidding and Voting without Any Trusted Third Party （匿名ディジタル署名の提案と信頼機関を利用しない入札・投票への応用）
論文審査委員	（主査） 教授 藤原 融 （副査） 教授 柏原 敏伸　教授 村田 正幸

論文内容の要旨

入札及び投票をネットワーク上で実現することが期待されており、暗号技術を用いて、通信の安全性、参加者の公平性、匿名性を満す匿名入札プロトコル及び匿名投票プロトコルの開発が研究されている。小さいコミュニティでは信頼できる機関の設立が困難であり、信頼できる機関を利用しないいくつかの匿名入札プロトコル及び匿名投票プロトコルが提案されている。しかし、これらのプロトコルでは、匿名の参加者が他の参加者の応札内容や投票内容を知った後で参加を取り止めることが可能である。このため、落札価格の不正操作や、投票の途中棄権が起こる可能性がある。

本論文では、いくつかの匿名ディジタル署名を提案し、それらを利用することにより従来法の問題点を解決した匿名入札プロトコル及び匿名投票プロトコルを提案する。匿名ディジタル署名では、署名のみが与えられてもその署名者を特定できない、しかし、署名者のすべての候補と通信を行うことにより、その署名者を特定可能である。したがって、応札内容や投票内容にこの署名を付加することにより、匿名の途中棄権者を特定することが可能となる。

まず、署名の匿名性の定式化を行い、一方向性置換が存在するという仮定の下で、匿名ディジタル署名である匿名否認不可署名及びリンク可能グループ署名が構成可能であることを示す。また、離散対数問題が困難であるという仮定の下で、これらの署名を効率的に構成する。そして、匿名入札プロトコル及び匿名投票プロトコルに必要とされる性質を示し、匿名否認不可署名を用いた匿名入札プロトコルとリンク可能グループ署名を用いた匿名投票プロトコルを構成する。さらには、構成したプロトコルが必要とされる性質を満すことを示す。

論文審査の結果の要旨

本論文では、いくつかの匿名ディジタル署名を提案し、それらを入札・投票プロトコルに応用している。

匿名ディジタル署名に関しては、新たに匿名否認不可署名及びリンク可能グループ署名の概念を導入している。これらはそれぞれ、従来提案されている否認不可署名及びグループ署名を拡張したものである。まず、署名の匿名性の定式化を行い、一方向性置換の存在仮定の下で、理論的な実現方式を提案している。これにより、匿名否認不可署名及びリンク可能グループ署名が、特定の数論上の仮定ではなく、かなり一般的な仮定の下で実現できることがわかっ

た。また、離散対数問題が困難であるというよく用いられる仮定の下で、より効率的な実現方式も提案している。

次に、匿名否認不可署名を用いた入札プロトコルとリンク可能グループ署名を用いた投票プロトコルが提案されている。提案プロトコルでは、匿名性が満されている。匿名性は、参加者のプライバシ保護とともに、入札では談合の防止にも役立つ。これは、談合をもちかける対象者を限定するための情報となりうる応札者名や応札者と応札価格との対応関係が秘匿されるからである。また、提案プロトコルでは、第三者の信頼機関が各プロトコルに参加する必要がないため、第三者への依存度が小さい。このことは、信頼機関を設立することが困難な小さいコミュニティでの利用において、有効である。従来提案されていた信頼機関を利用しない匿名入札・投票プロトコルでは、他の参加者の応札内容・投票内容を知った後で、参加を取り止めることが可能であった。本論文では、このことが落札価格の不正操作や投票の途中棄権をもたらすことを示し、従来法の問題点を指摘している。本論文のプロトコルでは、匿名ディジタル署名を利用することにより、正当な参加者の匿名性を満しながら、不正が発生したときにはその不正者を特定することが可能となっている。このことは不正行為の抑止効果があり、従来法の問題点が解決されている。

以上のように、本論文で提案されたプロトコルを用いることにより、第三者への依存度を軽減した匿名入札・投票サービスが実現可能となる。これは社会活動のコンピュータネットワーク上での実現に大きく寄与しており、本論文は博士（工学）の学位論文として価値があるものと認められる。