岡山大学

PRESS RELEASE

大学記者クラブ加盟各社　御中

平成 21 年 10 月 27 日
岡　山　大　学

楕円ペアリング暗号およびグループ署名を用いた実用的な「組織間匿名認証技術」の開発

概要：　本学工学部通信ネットワーク工学科の研究グループは、不正アクセスの防止とプライバシー保護を両立する「楕円ペアリング暗号およびグループ署名を用いた匿名認証」の実現のための代数計算ライブラリおよび認証プロトコルの実装を完了したと発表した。

本年度より、具体的な状況設定のもとで、実用的な匿名認証基盤の確立に向けた実証実験に着手する。これが成功すれば、組織間における認証基盤に対して、匿名認証技術を用いた新たな仕組みの導入となり、企業間や大学間など組織間でのインターネットを介した電子データの流通・活用が一気に進むことが期待される。

＜業績＞

岡山大学工学部通信ネットワーク工学科の研究グループは、不正アクセスの防止とプライバシー保護の両立を目的とした匿名認証の実現に向け、「楕円ペアリング暗号を用いたグループ署名」の研究・開発を進めている。この技術を用いることで、昨今問題となっている個人情報の漏洩を防ぐことができ、その上でインターネットなどを介した多様なサービスの提供が可能となる。同研究グループではこれまでに、その土台となる代数計算ライブラリの開発および具体的な認証プロトコルの実装について研究を進めてきた。そして本年度より、これまでに得られた研究成果をベースとして、具体的な状況設定のもとに、組織間での実用的な匿名認証技術の確立に向けた実証実験に着手する。

＜見込まれる効果＞

これが実現されれば、組織間における認証基盤に対して、匿名認証技術を用いた新たな仕組みの導入となり、見込まれる効果として(a)匿名認証によって個人情報・組織情報の漏洩を防ぐことができるのみならず、(b)組織間での相互認証により各組織の情報資源を有効に流通・活用でき、(c)電子決済や電子回覧などの効率化も図られることとなる。

＜お問い合わせ＞
岡山大学 工学部 通信ネットワーク工学科・事務
（電話番号）086-251-8255
（FAX番号） 086-251-8255