TYPE OF INDUSTRY

科学技術・大学

情報通信研究機構

NICT 先端研究 ⑭

匿名認証における鍵失効技術

サイバーセキュリティ研究所・セキュリティ基盤研究室主任研究員 江村 恵太

10年4月北陸先端科学技術大学院大学（JAIST）情報科学研究科博士後期課程修了。博士（情報科学）。14年10月より情報通信研究機構（NICT）主任研究員、現在に至る。

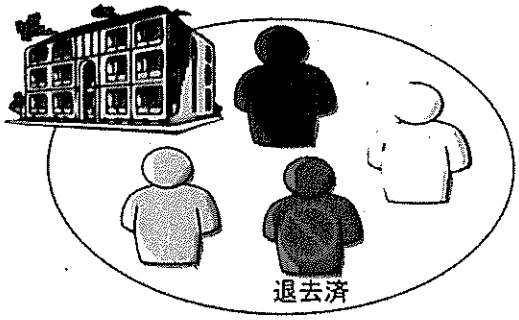
暗号というと普段なじみがない方が多いと思われるが、インターネットショッピングや高速道路での自動料金支払いシステムなどさまざまな場面で知らず知らずのうちに利用している技術である。暗号は他人が知らない秘密の鍵を用いることでその安全性が担保される。そのため鍵の使用期限が切れた場合や紛失してしまった場合には適切に鍵の機能を停止する必要があり、この鍵失効技術は暗号システムの実社会展開において必須である。しかし高機能な暗号技術を用いると鍵失効が難しい場合がある。一例として匿名性を持つ認証方式を紹介する。

例えばマンションのエントランスなどにおける入退出管理では、住人であることのみ匿名で確認できれば通常は十分で、どの住人かまで確認することは出来ているかどうかを直接確認することは、どの住人かを特定することにつながる。このように匿名で認証を行うことにつながり匿名性に矛盾する。もちろん誰かが退去したことで全住人に鍵を再配布するのは現実的ではなく、いかに匿名性を担保し、かつ適切に追跡可能性を実現するのかは匿名下での鍵失効において重要な課題といえる。

研究室ではこのような暗号の実社会展開に向けて、その機能性を失うことなく安全かつ効率的に鍵失効を行う技術の研究に取り組んでいる。その研究成果の一つとして、楕円曲線上定義される双線型写像およびゼロ知識証明と呼ばれる技術を利用することで、効率的かつ安全に匿名環境下での鍵失効を行う技術を開発している。

（火曜日に掲載）

マンション入退出管理システム



匿名認証：個人を特定せず、住人であることのみ確認

⇕ 対称的な要件

追跡可能性：元住人であるかどうか確認