データ流通とセキュリティ技術

Information Security for Data Distribution and Sharing

岡本　龍明

NTT Research, Inc.

E-mail: tatsuaki.okamoto@gmail.com

1　はじめに

ネットワーク上では膨大なデータが蓄積･流通され、様々な形で活用されるようになってきた。このことは科学の進展やビジネスに大きく貢献する一方、プライバシー保護が大きな問題となる。プライバシー保護に関しては、日本では個人情報保護法がありヨーロッパでは一般データ保護規則（GDPR) があるなど、それぞれの国や地域で異なった規定が定められており、データ流通においてはそれらの規定を遵守する必要が生じる。一方、ネットワークでは信頼性の低い情報や偽情報があふれており、正しい情報の流通を妨げているという問題がある。

本稿では、このようなデータ流通におけるプライバシーや信頼性を守るための技術について紹介する。まずプライバシーを保護する技術として、秘密計算（もしくは、多者計算）と関数型暗号を紹介する。さらに信頼性を保証する技術として、ブロックチェーンを紹介する。

2　秘密計算

秘密計算は、各利用者の保有するプライバシー情報を秘密にしたまま、それら情報に関する適当な関数（さまざまな統計量や各種関数）を計算するものである。この機能を実現する方法として、秘密分散方式を利用する方法、ガーブルド（暗号化）回路を用いる方法、完全準同型暗号を用いる方法などがある。

3　関数型暗号

関数型暗号は、暗号化したデータを単に復号するのではなくて、そのデータをある関数に入力して計算した値として復号するものである。秘密計算と同様に、関数型暗号も、プライバシーデータを秘密にしたまま、利用者が必要とする情報（統計値や関数計算値）のみを取り出すことが可能となる。

4　ブロックチェーン

ネットワーク上で蓄積、流通するデータの信頼性を高める（保証する）技術がブロックチェーンである。この技術の特徴は、データに対する信頼性を付与するために特定の権威者によるお墨付きを与えるものではなく、非中央集権的な形で（多くの参加者が協力して）データの正しさに対するお墨付きを与えるものである。さらに、ゼロ知識証明などの技術を用いることで、プライバシーを保護することも可能となる。

5　おわりに

秘密計算は 1980 年代から研究されてきた分野であるが、その効率や実用性を高める技術は最近の研究により大きく進展している。関数型暗号やブロックチェーンはいずれも 2010 年頃から研究されるようになった新しい分野であるが、データ流通のプライバシーや信頼性を保証する技術として研究・実用化が大きく進展している。

© 2021年 応用物理学会