SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

ProVerif による検索可能暗号の形式的安全性検証について
Formal Verification of Security for Searchable Symmetric Encryption using ProVerif

鈴木孝誠 * 山本博章* 三重野武彦†
Kosei Suzuki Hiroaki Yamamoto Takehiko Mieno

荒井研一†† 岡崎裕之* 布田裕一†††
Kenichi Arai Hiroyuki Okazaki Yuichi Futa

キーワード 形式的安全性検証、検索可能暗号、ProVerif

あらまし

情報セキュリティにおいて、暗号プロコトルの安全性を形式的に検証する技術は、安全性を担保する上で重要な技術である。その中で、ProVerif は暗号プロトコルの安全性を自動的に検証するためのツールの一つであり、広く研究されている。

安全性を考慮した検索技術として、検索可能暗号が広く研究されている。検索可能暗号は、クライアントとサーバで構成され､保存フェーズと検索フェーズからなる。保存フェーズでは、クライアントが自身のデータを暗号化してサーバに保存する。検索フェーズでは、クライアントが暗号化した検索キーワードをサーバに送り、サーバは暗号化キーワードと暗号化データを用いて検索を行う。その後、サーバは検索結果をクライアントに返す。このようにクライアント・サーバ間の暗号プロトコルとして記述できる。検索可能暗号の安全性は、実システムと漏洩情報だけを使って構成される理想システムとの識別不能性で証明されるが、形式検証ツールを用いた安全性の解析を見かけない。

本研究では、ProVerif を用いて検索可能暗号の安全性の形式的な検証を試みる。特に、基本的な手法として知られているカートモラの手法について検証する。

参考文献

[1] B.Blanchet(Project leader), “ProVerif: Cryptographic protocol veri-fier in the formal model.” Available at http://prosecco.gforge.inria.fr/personal/bblanche/proverif/.

[2] R. Curtmola et.al., Searchable symmetric encryption: Improved definitions and efficient construction, J. of Computer Security, pp.895—934, 2011

* 信州大学
† エプソンアヴァシス（株）
†† 長崎大学
††† 東京工科大学