氏名	TRAN, Duong Dinh
学位の種類	博士（情報科学）
学位記番号	博情第 512 号
学位授与年月日	令和 5 年 9 月 22 日
論文題目	Formal verification with algebraic techniques and its application
論文審査委員	緒方和博　北陸先端科学技術大学院大学　教授
	青木利晃　北陸先端科学技術大学院大学　教授
	石井大輔　北陸先端科学技術大学院大学　准教授
	土屋達弘　大阪大学　教授
	中村正樹　富山県立大学　教授

論文の内容の要旨

Formal verification has been extensively used to analyze various kinds of systems, such as verifying cryptographic protocols with security properties and mutual exclusion protocols with mutex properties. It is known as a unique approach in guaranteeing the absence of bugs (undesirable properties) in such systems. This approach formally describes the system under verification as a mathematical model using a dedicated language. The obtained result is called the formal specification of the system. Once the desired properties are specified with respect to the specification, formal verification that the system satisfies the properties can be conducted. There are two complementary approaches in formal verification: model checking and theorem proving. The former can be automatically conducted but cannot be used for systems that have an infinite number of states (infinite-state systems) in general due to the state explosion problem. The latter can deal with infinite-state systems but it requires human creativity, especially in lemma conjecture.

This thesis presents a formal verification approach with the employment of an algebraic specification language, namely CafeOBJ, equipped with an interactive theorem proving system, applied to verify the requirement properties of systems. We propose an approach and implement a supporting tool, namely IPSG, that can automatically generate formal proofs, the so-called proof scores, for formal verification of invariant properties. The algebraic specification language CafeOBJ is equipped with a rich specification syntax and many useful features for formal specifications of even complex systems, such as concurrent systems and distributed systems. It can be used as a powerful interactive theorem proving system, where humans can write a proof score to verify a desired property. However, writing proof scores is time- and effort-consuming, especially with complicated systems or specifications, and proof scores manually written are subject to human errors because they are user-defined, while CafeOBJ does not check their correctness. That is the reason motivating us to automate the proof score writing process and implement the tool. To demonstrate the efficiency and the practicability of the tool, experiments with various systems/protocols are conducted, ranging from a classical key distribution protocol to authentication protocols, from a real-time system to mutual exclusion protocols, and

from a distributed protocol to real cryptographic protocols currently in use.

In recent years, advanced research in the field of quantum computing and quantum information theory has brought a credible threat to cryptosystems currently in use. The most popular public-key (or asymmetric) primitives used today will no longer be secure under sufficient strong quantum computers because they can be efficiently broken by Shor's algorithm. That motivates cryptographers and security researchers to construct a new class of cryptographic protocols that are resistant to quantum attacks, called post-quantum cryptographic protocols (PQCPs), and verify the security of those PQCPs. Therefore, it would be very useful and meaningful to apply formal verification techniques to PQCP security analysis. This thesis presents two security verification case studies with: (1) the Hybrid Post-Quantum Transport Layer Security Protocol (PQ TLS) and (2) the Hybrid Post-Quantum Secure Shell Transport Layer Protocol (PQ SSH). PQ TLS has been proposed by Amazon Web Services (AWS) as a quantum-resistant version of the TLS 1.2 protocol, which is one of the most crucial and extensively used cryptographic protocols. PQ SSH has been proposed as a quantum-resistant version of the SSH Transport Layer protocol, where AWS is also one of the authors. We formally verify that the two protocols enjoy the desired security properties claimed in their design specifications, such as *session key secrecy* and *forward secrecy*, by using IPSG to generate their proof scores. The formal verifications are achieved under a threat model with the presence of an active attacker who can control the network, with respect to an unbounded number of protocol participants and protocol executions. The attacker can break the security of classical key exchange algorithms presuming by utilizing the power of large quantum computers. Moreover, the threat model also assumes the compromises of all secret types, such as ephemeral secret keys and long-term private keys of honest principals.

In the PQ SSH verification case study, in addition to the formal verification of three properties, we point out a counterexample showing that the protocol does not enjoy the *authentication* property, although what we found does not affect the confidentiality of session keys shared between honest participants. We then propose to slightly revise the protocol by adding the identifiers of the client and the server into the exchange hash. After revising the CafeOBJ formal specification accordingly, we can formally verify that the improved protocol enjoys the *authentication* property as well as the three other properties.

Keywords: formal verification, proof scores, post-quantum cryptographic protocols, algebraic language, IPSG.

論文審査の結果の要旨

証明スコア法はCafeOBJなどの代数仕様言語でプログラムを書くように証明を書くことが出来るという利便性を備える一方ヒューマンエラーの影響を受けるという弱点を併せ持つ。CafeOBJ 処理系が担当するのは証明の一部の計算（簡約）であり証明の正しさを確認するわけではないためである。この弱点を克服するため Invariant Proof Score Generator（IPSG）を開発した。構造帰納法を適用する変数を選択すると、構造帰納法による証明のための証明スコアを自動生成する。場合分けを行うことで、各々の部分場合（open-close 断片と呼ぶ）に対し、true か false かを CafeOBJ 処理系が返すようにまでする。true を返す open-close 断片は証明が完了しておりそれ以上何もする必要は無い。false を返す open-close 断片に対しては、補題を探し適用する必要がある。補題発見は定理証明においてもっとも知的な作業である。上述したように true か false かを CafeOBJ が返すまで場合分けを自動で行うことで、ひとがもっとも知的な補題発見に注力することを可能にする。
IPSG を用いて１０以上の事例に対し定理証明（形式検証）を実施している。それらの事例の２つは、ポスト量子ハイブリッド Transport Layer Security（PQ ハイブリッド TLS）とポスト量子ハイブリッド Secure Shell（PQ ハイブリッド SSH）である。量子コンピュータが実用化されショアのアルゴリズムがその上で実行されるようになると、整数の素因数分解などに安心・安全性を委ねている RSA などの暗号プリミティブは解読されてしまう。このため、量子コンピュータに耐性のあるポスト量子暗号が盛んに研究され、ポスト量子暗号を用いた上位のプロトコルが設計されている。PQ ハイブリッド TLS と PQ ハイブリッド SSH はそのようなプロトコルである。セキュリティプロトコルの形式検証では侵入者の存在を仮定する。Dolev-Yao の汎用侵入者がデファクトスタンダードとして用いられる。ネットワークを流れている情報を盗み見たり、他者に成りすましてメッセージを送ったりすることなどが出来ることを仮定する。Dolev-Yao の汎用侵入者が可能なことに加え、ショアのアルゴリズムで解読可能なものは解読可能であるという仮定も加えている。たとえば、楕円曲線ディフィー・ヘルマン鍵共有は解読可能になる。IPSG を用いて PQ ハイブリッド TLS がサーバとクライアント間で共有した秘密情報は第３者に漏れることは無いこと（秘匿性）、クライアントが対話している相手が意図したサーバであること（認証性）などの性質を満たすことを定理証明（形式検証）している。PQ ハイブリッド SSH に対して定理証明を試みている最中に認証性を満たさない反例を発見した。おそらく最初の発見者である。修正案を提案し、修正案が認証性および他の所望な性質を満たしていることを定理証明（形式検証）した。

証明スコア法の弱点を克服し定理証明におけるもっとも知的な作業である補題発見に注力することを可能とする IPSG を開発すると共に、IPSG を用いて PQ ハイブリッド TLS と PQ ハイブリッド SSH 含む１０以上の事例に対し定理証明（形式検証）を行い、PQ ハイブリッド SSH の反例を見つけ修正案を提案し修正案が所望の性質を満たすことを定理証明（形式検証）した。十二分に博士（情報科学）に値する研究成果である。