様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 １４ 日現在

機関番号：８２６２６
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２８３４

研究課題名（和文）短い秘密情報に基づいた認証技術と鍵管理技術に関する研究開発

研究課題名（英文）Research on authentication and key management techniques based on weak secrets

研究代表者
辛　星漢（SHIN, SeongHan）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：２０４４３１９５

交付決定額（研究期間全体）：（直接経費）　　6,500,000円

研究成果の概要（和文）：本研究課題では、日本の提案方式 AugPAKE と SKI mechanism をそれぞれ国際標準団体 ISO/IEC で標準規格化した。具体的には、AugPAKE が含まれている国際標準 ISO/IEC 11770-4 (2nd edition)が平成29年11月に出版され、また SKI mechanism が含まれている国際標準 ISO/IEC 20009-4 (1st edition)が平成29年8月に出版された。そして、既存の匿名パスワード認証方式における問題点を明確した上で、よりよい効率と安全性証明を有する新たな方式を提案した論文などが国際論文誌へ掲載された。

研究成果の学術的意義や社会的意義
本研究成果の学術的や社会的意義はパスワード認証方式、鍵管理方式そして匿名パスワード認証方式の暗号理論的な安全性解析と実装上の問題解決を行うことで ISO/IEC の国際標準化過程に大きな影響を及ぼすことである。また、厳密な安全性証明ができる新たな方式を設計するとともに、常に実用化を念頭においてより効率で様々な攻撃を想定してそれらの攻撃に安全な方式を設計することである。これらの研究成果は学術的にも大きな貢献になると予測されるし、本研究の成果はすでに標準化した国際標準化団体において既存の認証・鍵管理方式を見直す切っ掛けになることを期待している。

研究成果の概要（英文）：In this project, we have conducted standardization activities on our authentication scheme (AugPAKE) and anonymous authentication scheme (SKI mechanism) in ISO/IEC. In 2017, two international standards ISO/IEC 11770-4 (2nd edition) and ISO/IEC 20009-4 (1st edition) were officially published where AugPAKE was included in the former standard and SKI mechanism was in the latter standard. Also, we published several papers where we pointed out several problems in the previous (anonymous) password authentication schemes and proposed much more efficient and/or secure schemes.

研究分野：情報セキュリティ

キーワード：暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

安全・安心できるネットワーク社会を支えるには暗号技術は必要不可欠である。近年、国際標準化過程にある暗号技術に関してより多くの研究が行われている。その一例として、国際標準団体 IETF (Internet Engineering Task Force)が標準化を推進している暗号プロトコル TLS 1.3 に関して、今年の10月に行われた ACM CCS 2015で TLS 1.3のハンドシェイクプロトコルに暗号理論的に安全性証明をした論文や TLS 1.3の脆弱性を示す安全性解析をした論文などが発表された。本研究では、現在国際標準団体 ISO/IEC の ISO/IEC 11770-4と ISO/IEC 20009-4でそれぞれ国際標準規格化が進んでいる弱い秘密情報に基づいた鍵管理技術と匿名認証技術に焦点を当てる。

暗号技術の中で、盗聴・なりすまし・通信データの改ざんなどを行うアクティブな攻撃者に対しても目に見えない相手を正しく認証しながら安全な通信路を確立する認証付き鍵共有方式 (Authenticated Key Exchange: AKE)は欠かせない要素技術のひとつである。実際に認証付き鍵共有方式は SSL/TLS, SSH, IPsec などで頻繁に使われている。認証付き鍵共有方式では相手を認証するために様々な秘密情報（例えば、公開鍵証明書の公開鍵とペアになる秘密鍵、共通鍵、パスワードあるいはそれらの組み合わせなど）を用いている。その中でパスワードだけを秘密情報として用いるパスワード認証付き鍵共有方式（ここでは、簡単に“パスワード認証方式”と呼ぶ)はユーザへの利便性や実世界で広く導入されているなどの利点から長い間盛んに研究が行われている。しかしながら、ユーザが覚えているパスワードの情報量はもともと少ないためオフライン全数探索攻撃が多くのパスワード認証方式において有効になっている。

現在、EKE (Encrypted Key Exchange)を始めとする多数のパスワード認証方式 (Password-Authenticated Key Exchange: PAKE)が IEEE 1363.2, ISO/IEC 11770-4, IETF, ITU-T などの国際標準団体で標準化されて（または、されつつで）ある。特に、ISO/IEC 11770-4はパスワード認証方式（Balanced/Augmented PAKE）以外にもパスワードを用いた遠隔サーバとのやり取りでユーザの長い秘密鍵を復元するパスワード認証付鍵回復方式(Password-Authenticated Key Retrieval: PAKR）を含めており、今のところ標準規格の改定により J-PAKE と AugPAKE が議論されている。

パスワード認証方式はアクティブな攻撃者に対して安全性を保障しているが､相手側に認証を受けるために最初にユーザのアイデンティティー(識別子)を送らなければならない｡そのため、攻撃者は通信路を盗聴するだけでどのユーザがどのサービスを利用しているかなど追跡ができてしまう。匿名パスワード認証方式（Anonymous PAKE）はパスワード認証方式の安全性にユーザの匿名性を保障するものである。現在、ISO/IEC 20009-4では SKI mechanism を含めて四つの方式が議論されている。

本研究では上記のように国際標準化が進んでいる ISO/IEC 11770-4と20009-4関連のパスワード認証技術、（パスワード）鍵管理技術、匿名パスワード認証技術に焦点を合わせて行う。これまで本研究の代表者はさまざまな認証付き鍵共有方式について研究を取り組んでおり、AugPAKE と SKI mechanism は日本の提案方式としてそれぞれ ISO/IEC 11770-4と20009-4に含まれている。本研究の主なモチベーションは日本の提案方式 AugPAKE と SKI mechanism を標準規格化することだが､そのためにも関連方式や周辺方式の暗号理論的な安全性解析や提案方式の実装上の問題解決などの研究開発は必ず必要であると考えられる。

２．研究の目的

本研究では、日本の提案方式 AugPAKE と SKI mechanism をそれぞれ ISO/IEC 11770-4と

20009-4で標準規格化するとともにパスワード認証方式、（パスワード）鍵管理方式、匿名パスワード認証方式を徹底的に分析した上、より効率がよくてかつ厳密な安全性証明ができる新しいパスワード認証方式、鍵管理方式及び匿名パスワード認証方式を提案する。

３．研究の方法

本研究の目的を達成するためには（1）新しいパスワード認証方式、鍵管理方式及び匿名パスワード認証方式の研究開発、（2）AugPAKE と SKI mechanism の参照実装・管理、（3）国際標準団体での標準化活動という三つの項目について研究開発を行う。「新しいパスワード認証方式、鍵管理方式及び匿名パスワード認証方式の研究開発」は本研究で一番重要な基礎研究課題であり、具体的には（匿名）パスワード認証方式と鍵管理方式の動向調査と分析、コア技術の追求、それをベースにもっとも効率がよくてかつ厳密な安全性証明ができる新しいパスワード認証方式、鍵管理方式及び匿名パスワード認証方式を提案することである。「参照実装・管理」では AugPAKE と SKI mechanism を外注により参照実装を実施し、それをベースに ISO/IEC JTC 1/SC 27 会議の標準化スケジュールに従って国際標準化活動を行う。

４．研究成果

平成28年4月に開かれた ISO/IEC JTC 1/SC 27タンパ会議では ISO/IEC 11770-4の1st CD (Committee Draft)を議論し、1st DIS (Draft International Standard)へ進むことが決議された。そして、平成28年10月に開かれた ISO/IEC JTC 1/SC 27アブダビ会議では ISO/IEC 11770-4の1st DIS と ISO/IEC 20009-4の1st DIS がそれぞれ議論され、二つとも1st FDIS (Final DIS)へ進むことが決議された。平成29年4月に開かれた ISO/IEC JTC 1/SC 27ハミルトン会議では AugPAKE が含まれている ISO/IEC 11770-4 FDIS と SKI mechanism が含まれている ISO/IEC 20009-4 FDIS がそれぞれ国際標準 IS (International Standard)として発行されることが決議された。その後、AugPAKE（IS では AKAM3と命名される）が含まれている国際標準 ISO/IEC 11770-4:2017-11 (2nd edition)が11月に出版され、また SKI mechanism が含まれている国際標準 ISO/IEC 20009-4:2017-08 (1st edition)が8月に出版された（その他①とその他②）。

また、既存の匿名パスワード認証方式における問題点を明確した上で、よりよい効率と安全性証明を有する新たな方式を提案した論文が国際論文誌へ掲載された（雑誌論文②）。そして、既存の匿名パスワード認証方式における攻撃と対策を示した論文が国際論文誌へ掲載された（雑誌論文①）。その他に、パスワード認証と IBS を使う方式の安全性解析と新たな方式を提案した論文（学会発表①）と、LRP-AKE の厳密な安全性証明と性能評価を議論した論文（学会発表②）をそれぞれ国際学会で発表した。

５．主な発表論文等

〔雑誌論文〕（計２件）

① SeongHan Shin, Kazukuni Kobara, How to Preserve User Anonymity in Password-Based Anonymous Authentication Scheme, IEICE Transactions on Information and Systems, 査読有, E101-D, 2018 年, 803-807, DOI 10.1587/transinf.2017EDL8183

② SeongHan Shin, Kazukuni Kobara, Simple Anonymous Password-Based Authenticated Key Exchange (SAPAKE), Reconsidered, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 査読有, E100-A, 2017, 639-652, DOI 10.1587/transfun.E100.A.1

〔学会発表〕（計１４件）

① SeongHan Shin, Secure Hybrid Authentication Protocols against Malicious Key Generation Center, ISITA2018（国際学会）, 2018 年

② SeongHan Shin, Two-factor Authentication LRP-AKE, Revisited, CSCI-ISOT 2018（国際学会）, 2018年

③ SeongHan Shin, Current Research Activity on Authentication Techniques, WAIS 2019（国際学会）, 2019年

④ SeongHan Shin, On the Security Proof and Performance Evaluation of LRP-AKE, SITA 2018, 2018年

⑤ SeongHan Shin, Kazukuni Kobara, Chia-Chuan Chuang, Weicheng Huang, How to Provide MQTT with Security, and Its Application (Poster), 12th International Workshop on Security (IWSEC 2017)（国際学会）, 2017年

⑥ SeongHan Shin, Kazukuni Kobara, A Secure MQTT Framework from PUF-based Key Establishment, The 2017 International Symposium on Internet of Things & Internet of Everything (CSCI-ISOT 2017)（国際学会）, 2017年

⑦ SeongHan Shin, Kazukuni Kobara, Reducing the Power of Key Generation Center in Hybrid Password Authentication Protocol, Computer Security Symposium 2017 (CSS 2017), 2017年

⑧ SeongHan Shin, Kazukuni Kobara, Security Analysis of Password-Authenticated Key Retrieval, The Seventh Symposium on Biometrics, Recognition and Authentication (SBRA 2017)（招待講演）, 2017年

⑨ SeongHan Shin, Kazukuni Kobara, PUF-based MQTT, 2018 Symposium on Cryptography and Information Security (SCIS 2018), 2018年

⑩ SeongHan Shin, Kazukuni Kobara, Chia-Chuan Chuang, Weicheng Huang, A Security Framework for MQTT, IEEE International Workshop on Cyber-Physical Systems Security (CPS-Sec)（国際学会）, 2016年

⑪ SeongHan Shin, Kazukuni Kobara, A Secure Anonymous Password-based Authentication Protocol with Control of Authentication Numbers, 2016 International Symposium on Information Theory and its Applications (ISITA2016)（国際学会）, 2016年

⑫ Tadanori Teruya, Yoshiki Aoki, Jun Sakuma, Fairy Ring: Ubiquitous Secure Multiparty Computation Framework for Smartphone Applications, 2016 International Symposium on Information Theory and its Applications (ISITA2016)（国際学会）, 2016年

⑬ SeongHan Shin, Kazukuni Kobara, How to Fix Client Anonymity in Anonymous Password-based Authentication, Computer Security Symposium 2016 (CSS 2016), 2016年

⑭ SeongHan Shin, Kazukuni Kobara, Chia-Chuan Chuang, Weicheng Huang, How to Provide MQTT with Security, 2017 Symposium on Cryptography and Information Security (SCIS 2017), 2017年

〔その他〕

① 国際標準規格, ISO/IEC 11770-4:2017-11 (2nd edition)

② 国際標準規格, ISO/IEC 20009-4:2017-08 (1st edition)

６．研究組織

(1)研究分担者

研究分担者氏名：照屋　唯紀

ローマ字氏名：(TERUYA, Tadanori)

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：情報・人間工学領域

職名：研究員

研究者番号（8 桁）：20636972

研究分担者氏名：松田　隆宏

ローマ字氏名：(MATSUDA, Takahiro)

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：情報・人間工学領域

職名：主任研究員

研究者番号（8 桁）：60709492

研究分担者氏名：山田　翔太

ローマ字氏名：(YAMADA, Shota)

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：情報・人間工学領域

職名：研究員

研究者番号（8 桁）：70750834

研究分担者氏名：村上　隆夫

ローマ字氏名：(MURAKAMI, Takao)

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：情報・人間工学領域

職名：主任研究員

研究者番号（8 桁）：80587981