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

平成　３０　年　　６　月　１１　日現在

機関番号：　１４４０１
研究種目：　若手研究(B)
研究期間：　2016～2017
課題番号：　１６Ｋ１６０６５

研究課題名（和文）安全なIoT ネットワークの経路制御に関する研究

研究課題名（英文）A Study on Routing Security for IoT Networks

研究代表者
矢内　直人（Yanai, Naoto）

大阪大学・情報科学研究科・助教

研究者番号：３０７３７８９６

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：IoT 機器間において安全かつ効率的にネットワークを構成できるよう、負荷の低い署名方式を構成した。とくにIDベース署名と呼ばれる任意の文字列を公開鍵として用いる電子署名方式で構成することで、各デバイスがID情報やMACアドレスなどを用いる方式において、従来の方式よりも短い鍵の長さで高い安全性を持つ方式や、鍵が危殆化したときに鍵を更新できるような方式を構成した。さらに電子署名を持つ際のネットワークの安全性の解析方法や、ラズベリーパイ上での実装実験も行うことで、より実利用に近いプロトコルレベルでの検討も行った。これらの成果は学術論文誌7編、査読付き国際会議7編として公開している。

研究成果の概要（英文）：To construct networks securely and efficiently for IoT devices, we proposed several digital signature schemes with low costs. In particular, for ID-based signatures which allow any user to utilize its own ID information or MAC address as a public key, we proposed more secure scheme even for a shorter key length and a key-updatable scheme if a secret key is revealed. Next, we proposed a security analysis method for networks with digital signatures. We also conducted experiments the above results on Raspberry-Pi to confirm the performance. We published these results as seven academic articles and seven international conference proceedings.

研究分野：　情報セキュリティ

キーワード：　ルーティングセキュリティ　暗号　電子署名　セキュアルーティング　IoT

１．研究開始当初の背景

本研究の着想および背景は署名者自身による攻撃を防ぐ送信者・受信者間で合意が必要な電子署名方式とその集約方法を示すことで、IoT ネットワークにおける不正な機器接続の防止を効率的に実現するような経路制御プロトコルの設計にあった。

研究が進むにつれ、各機器が与えられた平文に対し単一の署名しか生成できない限り、何らかの攻撃が発生したとしても迅速にその発生源を特定できると考え、そのような機能を安全に実現する方式の設計と、その実装実験に内容を移していった。

２．研究の目的

本研究の大目的は上述した機能の実現であるが、その目的に向けて特に以下の三つの観点について明らかにすることを目的とした。

まず一点目は方式レベルの検討として、電子署名の安全性をどのように保証するかである。IoT 機器では計算能力の制限や、攻撃者による機器解析を通じた秘密情報の漏えいなどがあり得る。これらを考慮したうえでなお、安全性を保証する方式の設計を目指す。

二点目は電子署名を導入した経路制御において、実際に安全性をどのように解析するのか、方法論を確立する点である。電子署名の利用による経路制御に関する従来の安全性議論は直観的な枠組み（フォークロア）を出ておらず、数理的に示したような成果は知る限り存在しない。これは実際に安全性を解析できるような手法が検討されていないためである。このため、この安全性の解析方法自体も明らかにする。

最後に、設計した方式について何らかの IoT 機器を用いて実験することで、その有効性を検証する。暗号技術はしばしば負荷が高く、導入が厳しい状況をあり得るため、実装実験を通じて実現性を検討する。

３．研究の方法

以下に、前節で述べた三つの目的に対する研究方法をそれぞれ説明する。

３－１．方式レベルの検討

決定性 ID ベース署名と呼ばれる電子署名方式において、署名の集約方法を検討した。これは各機器が任意の文字列を公開鍵として使えること、また、与えられた平文に対し署名が一意に定まるという性質を持つ。とくにこの ID ベース署名方式において従来の方式より短い鍵を用いても同等の安全性を持つ方式を構成することで、小計算能力の機器でも利用できるようにする。

また、IoT 機器から署名生成用の鍵が漏えいした際に対し、秘密鍵を動的に更新する鍵更新機能を導入する。

上述したいずれの方式においても、署名の集約機能を損なうことがない様に構成する。また、方式が破れないことを数学的な証明を通じて示す。

３－２．経路制御の安全性解析手法

高い水準の安全性を保証するには計算論的モデルにおいてチューリングマシンを仮定した議論が望ましい。ここでいうチューリングマシンとは、ある機械に対して入力と対応する出力の組のみを定義し、その機械の内部処理を考慮しない計算機科学の概念である。このチューリングマシンによる解析を通じて、ある入出力を利用できるような攻撃者に対して、その攻撃者がどのような処理をしていたとしても攻撃ができないことを保証できる。このチューリングマシンを通じた安全性の議論を通じて、電子署名が偽造不可能であるならば経路制御が安全にできることを示す。

３－３．IoT 機器を用いた実装実験

性能評価と提案プロトコルの実現性を評価するために、IoT 機器上での実装実験を行った。IoT 機器としてはラズベリーパイを用いた。ラズベリーパイは SD カードにプログラムを書き込み、搭載することで任意のプログラムを利用することが可能である。各経路制御プロトコルのプログラムを搭載したラズベリーパイを複数台並べることで、ラズベリーパイ間の通信を通じて実験が可能となる。

４．研究成果

以下に前節で述べた三つの項目に関する成果をそれぞれ以下に述べる。

４－１．方式レベルの検討

決定性 ID ベース署名について、緊密な帰着と呼ばれる最高水準の安全性を示した。ここでいう緊密な帰着とは、方式の安全性が安全性の前提となる数学的な仮定と等価であることを意味しており、暗号理論における最高の安全性といえる。この緊密な帰着の達成により、従来の方式よりも短い鍵で同等程度の安全性を満たすことができる。とくにこの緊密な帰着を達成する方式について、その実現方法を明らかにすることで、特定の条件を満たす構成になっていれば緊密な帰着を満たせることを示した。また、多人数設定において、緊密な帰着を実現したまま署名を集約する構成およびその実現方法も明らかにしている。

また、鍵が危殆化した際にも安全性を保証できるよう、鍵を更新できる方式を構成した。一般には鍵の更新は署名の代数構造を書き換えるため、集約機能に差し障る可能性がある。この問題を、署名の代数構造に準同型性を持たせることで解決している。直観的には鍵を更新した場合であっても代数構造は変わらないため、集約機能を維持することが可能となる。

上述した一連の成果は学術論文誌 3 編、査読付き国際論文誌 3 編、国内研究会 1 編として公開している。

４－２．経路制御の安全性解析手法

チューリングマシンの概念を適用した攻撃者に対する安全性と、その証明方法を検討した。安全性の定義としては、他の機器に対し署名を要求・受け取ることができる能力を想定し、また、そのやりとりの後に攻撃者自身が自分で署名を偽造することができる科を検討する安全性である。

また、その際に経路制御に利用された電子署名が安全なものである限り安全性を保証できるような方法論を検討した。

上述した成果は査読付き国際会議 1 編として公開している。

４－３．IoT 機器を用いた実装実験

ラズベリーパイ上に設計した電子署名と経路制御プロトコルを実装し、評価した。その結果、RSA 署名など従来の署名方式を利用した場合と比べてラウンドトリップタイムやパケットロスの削減ができることを示した。これは従来の技術と比べて署名長が短くなったことが大きく起因しているものと予想している。

上述した成果は査読付き国際会議 2 編、国内研究会 1 編として公開している。

４－４．その他の成果

上述した問題とは厳密には異なるが、本機関を通じて得た電子署名方式について、応用技術を検討することで、IoT 向けアプリケーションを何点か新たに提案している。

詳細は割愛するが、この成果は査読付き論文誌 2 編、査読付き国際会議 2 編を公開している。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　５件）

1. 田中 和磨, 矢内 直人, 岡田 雅之, 西出 隆志, 岡本 栄司, “APAT: BGPSEC におけるアグリゲート署名の導入”, 情報処理学会論文誌, 58 巻 2 号, pp.544-556, 情報処理学会, 2017 年 2 月.
2. Naoto Yanai, Tomoya Iwasaki, Masaki Inamura, Keiichi Iwamura, “Provably Secure Structured Signature Schemes with Tighter Reductions”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E100-A, No.9, pp.1870-1881, September 2017.
3. Naoto Yanai, Toru Fujiwara, “Tighter Reductions for Deterministic Identity-Based Signatures”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E101-A, No.1, pp.64-76, January 2018.
4. Thi Ngoc Diep Pham, Chai Kiat Yeo, Naoto Yanai, Toru Fujiwara, “Detecting Flooding Attack and Accommodating Burst Traffic in Delay Tolerant Networks”, IEEE Transactions on Vehicular Technology, Vol.67, No.1, pp.795-808, January 2018. (IF 4.066)
5. Naoto Yanai, “Meeting Tight Security for Multisignatures in the Plain Public Key Model”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E101-A, No.9, September 2018. (accepted.)

〔学会発表〕（計１３件）

1. Kazuma Tanaka, Naoto Yanai, Masayuki Okada, Takashi Nishide, Eiji Okamoto, “APAT: An Application of Aggregate Signatures to BGPSEC,” The 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2016), Fast Abstract, June 2016.
2. Kenta Muranaka, Naoto Yanai, Shingo Okamura, Toru Fujiwara, “ISDSR : Secure DSR with ID-based Sequential Aggregate Signature,” In Proc. of the 13th International Joint Conference on e-business and Telecommunications (ICETE 2016), Vol. 4, SECRYPT, pp. 376-387, July 2016.
3. 村中 謙太, 矢内 直人, 岡村真吾, 藤原 融, “ISDSR: ID ベースシーケンシャルアグリゲート署名の Dynamic Source Routing への適用,” コンピュータセキュリティシンポジウム 2016 (CSS 2016), pp.594-601, 2016 年 10 月.
4. 岸本 光, 矢内 直人, 岡村真吾, 藤原融, “スマートグリッドにおけるグループ署名を用いた利用者認証プロトコル,” コンピュータセキュリティシンポジウム 2016 (CSS 2016), pp.850-857, 2016 年 10 月.
5. Naoto Yanai, "Towards Provable Security of Dynamic Source Routing Protocol and Its Applications," Proc. of ER 2016 Workshops, AHA, MoBiD, MORE-BI, MReBA, QMMQ, SCME, and WM2SP, LNCS 9975, pp.231-239 November 2016.
6. Naoto Yanai, “On the Tightness of Deterministic Identity-Based Signatures”, Proc. of The Fourth International Symposium on Computing and Networking (CANDAR 2016), pp.168-173, November 2016.
7. Naoto Yanai, Toru Fujiwara, “A New Proof Technique for Tight Security Reductions on Deterministic Identity-Based Signatures”, 第 39 回

情報理論とその応用シンポジウム (SITA 2016), 8.2.2, pp.466-471, 2016 年 12 月.

8. 岸本 光, 矢内 直人, 岡村 真吾, “スマートグリッドにおける利用者認証プロトコルの導入に向けた性能評価,” 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 1C2-5, 2017 年 1 月.
9. Hikaru Kishimoto, Naoto Yanai, Shingo Okamura, “An Anonymous Authentication Protocol for Smart Grid,” Proc. of the 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA 2017), pp.62-67, IEEE, March 2017.
10. Naoto Yanai, “Tightly Secure Identity-Based Multisignatures,” 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW 2017), pp.253-254, IEEE, June 2017.
11. 小島 英春, 矢内 直人, “無線センサネットワークにおける経路保証プロトコルの実現に向けて”, 第 13 回ネットワークソフトウェア(NWS)研究会, 2017 年 6 月.
12. Hideharu Kojima, Naoto Yanai, “Performance Evaluation for The Signature Algorithm of ISDSR on Raspberry Pi”, Proc. of 10th International Workshop on Autonomous Self-Organizing Networks (ASON 2017), co-located in The Fifth International Symposium on Computing and Networking (CANDAR 2017), IEEE, November 2017 (accepted).
13. Nobuaki Kitajima, Naoto Yanai, Takashi Nishide, “Identity-Based Key-Insulated Aggregate Signatures, Revisited”, Proc. of The 13th International Conference on Information Security and Cryptology (Inscrypt 2017), November 2017 (accepted).

〔図書〕（計　0件）

〔産業財産権〕該当なし

○出願状況（計　0件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究代表者

矢内　直人　　（YANAI, Naoto）
大阪大学・大学院情報科学研究科・助教
研究者番号：30737896

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：

(4)研究協力者

（　　）