様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ４ 月 ２２ 日現在

機関番号：１４４０１
研究種目：研究活動スタート支援
研究期間：2014～2015
課題番号：２６８８００１２

研究課題名（和文）安全なインターネット経路構成技術に関する研究

研究課題名（英文）Research on Secure and Efficient Internet Routing Protocols

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）　　2,100,000円

研究成果の概要（和文）：インターネット経路の安全な制御に向けて、効率的に運用可能な電子署名を構築した。本研究の主な成果として、ネットワークの構成に応じた集約方法を検討することで、機器への負荷がネットワークの運用規模に依存しない方式を構成した。また、誤った署名が集約された場合であったとしても原因となる署名を特定可能な技術も提案している。これら一連の成果を実装評価することで、ネットワーク機器への負荷が従来技術の三分の一程度へ削減できることを示した。これらの成果は研究計画を通じて2件の査読付き国際論文誌、5件の国際会議論文として公開している。

研究成果の概要（英文）：Towards the security of the Internet routing, I proposed secure and efficient digital signature schemes. By considering how to aggregate signatures under network configurations, the data size of the proposed scheme is fixed with respect to the number of signers. Moreover, our scheme can identify invalid signatures even if any data is fault. We then showed that our scheme can decrease the network overhead by 30%. We published two international journals and five international conference papers in this research.

研究分野：情報セキュリティ

キーワード：インターネットセキュリティ　サイバーセキュリティ　電子署名　集約可能電子署名　暗号　BGP

１．研究開始当初の背景

インターネットを陰から支えている技術は IP アドレスとネットワークの対応関係を保証する経路制御技術である。この経路制御技術への攻撃として、偽の経路情報を広告することで被害者組織のネットワークを乗っ取り、アクセスを遮断する手法が近年多発している。有名な事例として YouTube のアクセスを遮断した YouTube ハイジャックや BitCoin の現金情報を偽のネットワークで盗用した BitCoin ハイジャックが知られている。

この問題に対し、経路制御への電子署名の導入が検討されている。電子署名はデータの正当性を保証できることから、経路制御の真贋保証が期待されている。その反面、電子署名の負荷は大きく、実際にはルータのメモリ肥大化とパケットサイズの増加によるネットワーク遅延という問題が発生する。このような背景から、本研究では運用負荷が無視できるほど小さい経路保証技術の確立を目指す。

２．研究の目的

本研究で目指す内容は（１）運用負荷が運用規模に対して定数オーダになる電子署名方式の提案とその安全性の証明、（２）提案した電子署名方式の実装評価の二点である。

（１）について、上述した暗号技術導入に寄る問題は従来の暗号技術がだいきぼ運用を考慮しておらず負荷が線形になることに大きく起因する。これに対し、負荷が定数オーダになる方式を提案することで、低コストでの運用が期待できる。また、提案方式の安全性について、現在の技術では計算困難な問題に基づいて「電子署名が偽造できない」ことを数学的に証明することで、どのような攻撃も起こり得ないことを保証する。

（２）について、（１）で提案した方式をコーディングし、その性能を評価する。また、提案方式がネットワークシステムに及ぼす影響について、仮想ネットワーク環境上で導入することで評価する。

２．研究の方法

本研究は三段階に分けて実施した。まず第一段階として、基盤となる方式の提案と安全性証明を行った。第二段階では提案方式の実装を行い、最終段階では仮想ネットワーク上での実験を行った。以下に、それぞれの詳細を説明する。

第一段階について、まず方式の要件定義と安全性定義について、チューリングマシンの概念にもとづいた要件定義を行った。また、その具体的な方式構成について、閉包性と準同型性を持つ関数を定義することで取り組んだ。閉包性はある集合において任意の値に関する演算結果が元の集合の要素に収まる性質であり、準同型性は関数の入力側と出側で演算の構造が維持される性質である。これにより、電子署名生成アルゴリズムの出力が演算を通じて集約されることで負荷が削減できる。この提案方式の安全性の証明については、ある計算困難な問題の計算困難性仮定に基づいて、提案方式を破る敵が存在した場合、計算困難な問題が解けるアルゴリズムができることを示した。これは難しい問題が解けるという矛盾を包括するため、前提となる敵の存在が誤りであることを意味する。この安全性証明の完了までを提案方式の構成作業とした。

第二段階について、暗号技術を構成する基本的な関数や代数計算法に関する既存のライブラリを併用しつつ、提案方式を実装した。また、その実計算時間について ECDSA など実際に利用されている暗号アルゴリズムと計算時間を比較することで評価した。

最終段階では既存のネットワークシミュレータソフトウェアに第二段階の実装物を導入し実験することで、ルータのメモリ量およびスループットを評価した。

３．研究成果

本研究の成果としては、2 件の査読付き国際論文誌の採録、7 件の査読付き国際会議での発表、4 件の国内研究会での発表、1 件の国内権威的学会における受賞を挙げている。

第一段階の成果としては、電子署名を集約できる方式について、双線形写像と呼ばれる二入力一出力からなる準同型性を持つ関数を通じた構成（学会発表 1*), 2),11*）に相当）と束ね準同型写像と呼ばれる全射関数を通じた構成（雑誌論文 1)および学会発表 4*)に相当）について、それぞれ提案した。双線形写像は暗号分野では近年注目を集めている関数であり、この関数を通じて効率の面から性能に優れた方式を提案している。とくにスタンダードモデルと呼ばれる現実的な仮定のもとで安全性を証明可能な方式を構成した。一方、束ね準同型関数は効率面では双線形写像からなる方式には劣るものの、情報理論的安全性という無限の計算能力を持つ敵に対しても署名の偽造を防ぐ方式を持つ。これは考える限り最高の安全性を持つことを意味する。これらの方式の安全性はそれぞれ CDH 仮定と素因数分解と呼ばれる最も計算困難な問題に基づくことも数学的に証明している。

第二段階の成果として、提案方式の実装を通じ、提案方式の速度を評価した（学会発表 3), 6*), 7*)に相当）。なお、効率の面から双線形写像に基づく方式のみ実装している。計算機環境に依存する話であるため具体的な速度数値は割愛するが、RSA や ECDSA といった既存の汎用暗号技術と比べて、概ね倍程度の速度低下が見られた。一方で、本研究の動機でもあったメモリサイズは削減が期待できる兆候が得られていた。

最終段階の成果として、実装物をシミュレーションしたところ、新たに二つの問題点が

浮上した。一つ目は誤った情報が集約済みの署名に挿入された場合にすべての電子署名が不当な情報として扱われること、もう一点は経路の形状によっては署名が正しく集約できないことである。前者の問題に対しては、集約済みの署名を複数用意することで、集約された署名の中からどの署名が誤っているか特定できる手法を新たに提案した（学会発表 8)に相当)。これは集約済みの署名と検証失敗の原因となる署名の連立方程式を構成するという発想に基づいている。この構成においても、署名のデータサイズは運用規模に対して定数オーダであるため、効率的な運用が期待できる。一方、後者の問題については、署名の集約方法とネットワーク構造の因果関係を明らかにすることで、電子署名が正しく集約される規則性を明らかにした（雑誌論文 2)に相当)。これら一連の成果を通じて提案方式の有用性を評価したところ、従来の電子署名つきの経路制御技術と比べて、提案方式により負荷を七割削減できることを確認した。

なお、一連の研究を通じた副次的な成果として機器自体の認証を行う鍵交換方式（学会発表 5*)に相当）や、電子署名をより幅広い組み込み機器に利用したアプリケーション（学会発表 8*)に相当）を提案している。また、経路制御技術の新たな側面としてインターネット以外のレイヤのプロトコルも部分的に議論している（学会発表 9),10)に相当。）

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　２件）

1) Nobuaki Kitajima, Naoto Yanai, Takashi Nishide, Goichiro Hanaoka, Eji Okamoto, "Fail-Stop Signatures for Multiple-Signers: Definitions, Constructions, and Their Extensions," Journal of Information Processing, Vol.24, No.2, pp.275-291, 2016 年 2 月.
2) Naoto Yanai, Masahiro Mambo, Kazuma Tanaka, Takashi Nishide, Eiji Okamoto, "Another Look at Aggregate Signatures: Their Capability and Security on Network Graphs," Proc. of The Seventh International Conference on Trusted Systems, Series of Lecture Notes in Computer Science, Vol. 9565, pp.30-46, 2016 年 3 月.

〔学会発表〕（計１１件）

以下では査読付きを* で記す。

1*) Naoto YANAI, Masahiro MAMBO, and Eiji OKAMOTO, “A CDH-Ordered Multisignature Scheme in the Standard Model with Better Efficiency,” Proc. of International Symposium on Information Theory and its Application (ISITA) 2014, pp.236-240 2014 年 10 月.
2) Naoto YANAI, Masahiro MAMNO, and Eiji OKAMOTO, “Ordered Multisignatures Made Shorter”, 第 37 回情報理論とその応用シンポジウム (SITA 2014), pp.72-77, 2014 年 12 月.
3) 村中 謙太, 矢内 直人, 岡村 真吾, 藤原 融, “多人数署名の実装と評価”, 電子情報通信学会技術研究報告, ICSS2014-78, Vol.114, No.489, pp.91-96, 2015 年 3 月.
4*) Nobuaki Kitajima, Naoto Yanai, Takashi Nishide, Goichiro Hanaoka and Eiji Okamoto, "Constructions of Fail-Stop Signatures for Multi-Signer Setting", Proc. of the 10th Asia Joint Conference on Information Security (AsiaJCIS 2015), pp.112-123, 2015 年 5 月.
5*)Yukou Kobayashi, Naoto Yanai, Kazuki Yoneyama, Takashi Nishide, Goichiro Hanaoka, Kwangjo Kim, Eiji Okamoto, "Gateway Threshold Password-based Authenticated Key Exchange Secure against Undetectable On-line Dictionary Attack", Proc. of the 12th International Conference on Security and Cryptography (SECRYPT 2015), pp.39-52, 2015 年 7 月.
6*) Kenta Muranaka, Naoto Yanai, Shingo Okamura and Toru Fujiwara, "Secure Routing Protocols for Sensor Networks: Construction with Signature Schemes for Multiple Signers", Proc. of The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2015), pp.1329--1336, 2015 年 8 月.
7*) Kenta Muranaka, Naoto Yanai, Shingo Okamura, Toru Fujiwara, "Toward Secure Routing Protocols for Sensor Networks," The 10th International Workshop on Security (IWSEC2015), poster, 2015 年 8 月.
8*) Hikaru Kishimoto, Shingo Okamura, Naoto Yanai, "Secure Payment Protocol for Charging Information over SmartGrid," The 10th International Workshop on Security (IWSEC2015), poster, 2015 年 8 月.
8) 田中 和磨, 矢内 直人, 岡田 雅之, 金山 直樹, 西出 隆志, 岡本 栄司, "BGPSEC におけるアグリゲート署名の導入," コンピュータセキュリティシンポジウム 2015 (CSS2015), pp.815-822, 2015 年 10 月.（CSS2015 優秀論文賞受賞）
9) 村中 謙太、矢内 直人、岡村 真吾、藤原 融, "多人数署名を用いた Secure-DSR の提案", 2016 年暗号と情報セキュリティシンポジウム, 2E2-1, 2016 年 1 月.
10) 矢内 直人, "経路制御の定式化に向けて：DSR の構成", 2016 年暗号と情報セキュ

リティシンポジウム 2016, 3F1-2, 2016 年 1 月.
11*)Tomoya Iwasaki, Naoto Yanai, Masaki Inamura, Keiichi Iwamura, "Tightly-Secure Identity-Based Structured Aggregate Signature Scheme under the computational Diffie-Hellman Assumption," The 30th IEEE International Conference on Advanced Information Networking and Applications (AINA-2016), pp.669-676, 2016 年 3 月.
〔図書〕（計　0件）

〔産業財産権〕
○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
藤原研究室
http://www-infosec.ist.osaka-u.ac.jp/index.html

Naoto Yanai
http://www-infosec.ist.osaka-u.ac.jp/~yanai/

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
該当なし

(3)連携研究者
該当なし