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 １３ 日現在

機関番号：１２１０２
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１８３

研究課題名（和文）多彩な機能を有する準同型認証子およびデータ軽量認証手法に関する研究

研究課題名（英文）Research on homomorphic authentication code with various functions and lightweight data authentication techniques

研究代表者

面　和成（Omote, Kazumasa）

筑波大学・システム情報系・准教授

研究者番号：５０４１７５０７

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究では，クラウドストレージにおいて，ネットワーク符号ベースの取り出し可能性証明（POR)に基づいた軽量なデータの監査及び修復を実現する手法を提案した．その中で，クライアントがデータの修復手続きから解放される“直接修復”の仕組みを新たに提供すると共に，データの監査を行う第三者監査機関（TPA）を導入する．TPAは，クライアントの代わりにクラウドサーバに保存されているデータの可用性と完全性を共通鍵暗号ベースで検証する第三者機関であり，クライアントはデータ監査プロセスから解放される．さらに，データの動的処理（データの更新・挿入・追加・削除）が可能なPOR方式を提案した．

研究成果の学術的意義や社会的意義
データ同士の演算が必要なデータ認証プロトコルにおいては，認証子同士の演算を可能にする準同型認証子が重要な暗号要素技術となっている．例えば，クラウドシステムにおける効率的なデータ認証プロトコルを構築する際，データの変更に伴って認証子も変更する必要があるため，準同型認証子を適用することは非常に有効である．本研究では，利用者の手を離れて認証子同士の演算を行うようなクラウドストレージにおいて，準同型認証子を応用することによって，データの認証のみならずデータの修復までを実現するPOR方式を新たに提案した．

研究成果の概要（英文）：In this research, we proposed a network-coding-based Proof Of Retrievability (POR) scheme, which achieved a lightweight data auditing and data repairing in a cloud storage. In particular, we support direct repair mechanism in which the client can be free from the data repair process. Simultaneously, we also support the task of allowing a third party auditor (TPA), on behalf of the client, to verify the availability and integrity of the data stored in the cloud servers without the need of an asymmetric-key setting. The client is thus also free from the data audit process. Furthermore, we proposed a new network-coding-based POR scheme which can deal with dynamic operations such as modification, insertion and deletion.

研究分野：情報セキュリティ

キーワード：セキュアクラウドストレージ　ネットワーク符号　メッセージ認証子(MAC)　準同型MAC

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

メッセージ認証子（以降では単に認証子と呼ぶ）とは，メッセージ／データが改ざんされていないこと（完全性）を保証する暗号技術である．認証子は認証すべきデータと秘密鍵から計算され，これにより同じ秘密鍵を持つ者のみがデータの改ざんを検出できる．そのような認証子の重要な拡張として，準同型認証子があげられる．準同型認証子は，秘密鍵を知ることなく，データの正当な変更に伴って認証子も変更できることから，利用者の手を離れてデータ同士及び認証子同士の演算を行うようなデータ認証プロトコルにおいて重要な技術である．さらに本技術は，効率よく計算できるため，分散ストレージシステム等，利用者の手を離れて膨大なデータを演算することが求められる近年のユビキタスシステムにおける軽量なデータ認証技術としても重要な技術となっている．しかしながら，準同型認証子には，(i)秘密鍵を持つ特定の者しか検証できない等の限定的な構成のため，異なる秘密鍵での演算や第三者検証といった多彩な機能を実現できない，(ii)準同型認証子における応用上の考察は未だに不十分である，といった問題点がある．

準同型認証子は，単なるデータ認証プロトコルとして利用されるだけでなく，特に，分散ストレージシステムやセンサネットワーク等，ユビキタス環境における軽量なデータ認証技術として注目を浴びている．しかしながら，これらのプロトコルは，異なる秘密鍵での演算や第三者検証といった準同型認証子の多彩な機能を有する構成法について，未だに十分な研究がなされているとは言えない．また，準同型認証子は公開鍵暗号技術の１つである準同型署名と比較して非常に軽量であり，機能を充実させることにより準同型署名の代替技術となり得るため，本研究による多彩な機能を有する準同型認証子を開発することはそれ自体極めて重要である．

以上より，多彩な機能を有する準同型認証子，及び先進的なユビキタス環境における多彩な機能を有するデータ軽量認証手法を提供する本研究の実施は，極めて重要なものである．

２．研究の目的

本研究では，分散ストレージシステムにおいて，準同型認証子を用いて単にデータの認証を行う（完全性を満たす）だけでなく，データの修復を可能とする（可用性を満たす）PoR 方式（詳細は後述する）の提案を行う．つまり，多彩な機能を有する準同型認証子，及び先進的なユビキタス環境における多彩な機能を有するデータ軽量認証手法の研究開発を行うものである．より具体的には，サーバに保存されているデータが利用可能であり，かつ改ざんされていないことをチェックするために，証明可能データ保有（Provable Data Possession; PDP）[1]や取り出し可能性証明（Proof of Retrievability; PoR）[2,3]が提案されている．PDP ではサーバが保存しているクライアントデータの完全性を保証するのに対して，PoR では完全性が保証されたクライアントデータのシェアを得ることができるため，データの取り出し可能性を保証できる．したがって，PoR は PDP よりも機能性が高いプロトコルであると考えられる．

以前の科研費若手 B の研究（課題番号：25730083）においても，POR 方式の提案を行ってきた．しかしながら，TPA にデータの認証チェックを委託する公開監査において，(1) チャレンジ＆レスポンスに制限がある，(2) TPA は各サーバに対して全ての符号ブロックをチェックしなければならない，という深刻な問題が残っていた．これらの問題は，多彩な機能を有するデータ軽量認証手法を実現する上で大きな課題である．そこで本研究では，これらの問題を解決すべく，軽量なデータ監査及びデータ修復を持つ共通鍵暗号ベースかつネットワーク符号ベースの POR 方式を提案することを目的とする．提案方式における主な貢献は次の 3 つである．

- 直接修復機能および公開監査機能を持つ POR 方式の提案
  - 直接修復：サーバが攻撃されたとき，健全なサーバはクライアントに頼ることなく新しいサーバに自身の符号ブロックと準同型認証子を直接与える．それから，新しいサーバは与えられた符号ブロックをチェックでき，新しい符号ブロックとその準同型認証子を計算できる．したがって，クライアントは修復プロセスから解放される．
  - 公開監査：TPA は，クライアントの秘密鍵を知ることなしにクライアントの代わりにサーバのデータを定期的にチェックできる．このとき，TPA は spot-checking 手法を用いるため，効率的にデータをチェックできる．その結果，クライアントはサーバチェックの負荷から解放される．
  - チャレンジ・レスポンス：POR の適切なチャレンジレンスポンス方式に従う．
- 安全性評価
  - 不正なストレージサーバ，あるいは不正な TPA からの現実的な攻撃を想定し，その形式化を行い，理論的な安全性証明を実施した．
- 性能評価
  - 4 つのフェーズを実装し，ファイルブロックサイズとファイルブロック数をパラメータとして性能の比較評価を実施した．

さらに，直接修復，公開監査およびチャレンジ・レスポンスを満たしつつ，データの動的処理（データの更新・挿入・追加・削除）の実現可能性を検討した．

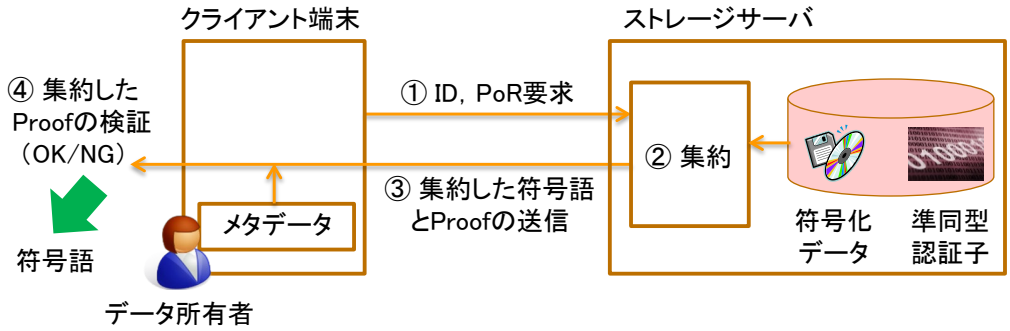


図 1 POR 方式

３．研究の方法

PoR 方式は，基本的にはストレージサーバのデータの完全性を検証するものであり，以下の前提をもつ．

- ストレージサーバには膨大なデータが保存されている．
- データが暗号化されているかどうかは気にしなくてよい．

また，想定する脅威として以下を考える．

(1) 膨大なデータが保存されているストレージサーバは，安全性と信頼性の両面で信用されていない．
(2) ストレージサーバ上のデータの全てまたは一部が消滅したとしても，ストレージサーバはデータ所有者に対してデータを持っていることを証明しようとする．
(3) ストレージサーバは，ほとんど使用していないデータを削除することによって新たな容量を確保しようとする．
(4) ストレージサーバは，データ紛失事故（管理ミス，ハードウェア故障，攻撃等）を隠す．

PoR では，上記の前提及び脅威のもとで，データ所有者はストレージサーバが符号語とその認証子を忠実に保存しているかを効率的かつ安全に検証する．このとき，ストレージサーバに符号化データとその認証子が共に保存されている．そして，データ所持の証明（Proof）を効率的に検証するために，少量のメタデータを用いたチャレンジ･レスポンスプロトコルを用いる．より具体的には，チャレンジに含まれる複数のブロックアドレス対して，ストレージサーバは符号語と認証子を集約してレスポンスとしてデータ所有者に返信する．

PoR 方式の概要を図 1 に示す．データ所有者は，ランダムチャレンジとして ID と PoR 要求をストレージサーバへ送信する．ストレージサーバは，受信した PoR 要求に対して符号化データとその認証子からデータ所持の証明（Proof）を集約して生成し，データ所有者の端末にレスポンスとして集約した符号語と集約した Proof を送信する．データ所有者は，メタデータを用いて Proof を検証し，OK であれば Proof を受理して該当の符号語を取得し，NG であれば Proof を棄却して該当の符号語を捨てる．

本方式では，データがネットワーク符号で符号化され分散ストレージサーバに保存され，データ所有者と分散ストレージサーバがセキュアチャネルで接続され，分散保存されたデータに対して可用性，完全性，機密性の全てを満たす．

- 可用性では最大 t 台未満の分散ストレージサーバが消失したとしてもサーバの符号語データの復旧が可能である
- 完全性ではチャレンジ＆レスポンス（スポットチェック）により準同型認証子によるデータの効率的な定期チェックを実施する
- 機密性では最大 t 台未満の分散ストレージが結託したとしても元のデータに関して何も分からない．

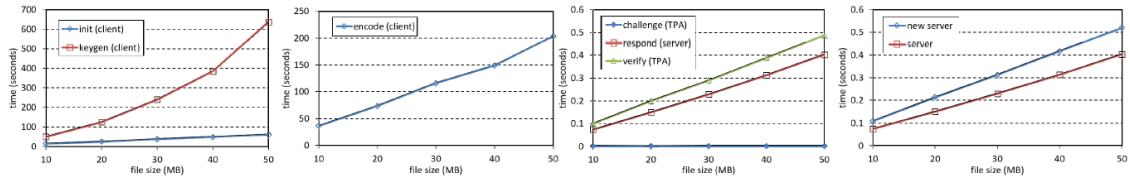
提案した PoR 方式の具体的な 4 つのフェーズを以下に記載する．

(1) 初期化・鍵生成フェーズ：データ所有者が，分散ストレージ用と TPA 用の鍵を生成する．
(2) 符号化フェーズ：データ所有者が自身のデータを符号化し，さらにその符号化データの認証子を計算して，ストレージサーバに保存する．
(3) チェックフェーズ：データ所有者は自身のデータの正当性や消失有無の確認のために，チャレンジ＆レスポンス方式で定期的に保存データのチェックを行う．
(4) 修復フェーズ：あるサーバが乗っ取られる，或いはあるサーバのデータが改ざんされてしまった場合，残りの健全なサーバのデータを用いて復旧を行う．

理論的な安全性評価では，TPA がユーザの秘密鍵を推測する攻撃，及びサーバによるリプレイ攻撃，汚染攻撃及び認証子偽造攻撃を形式化し，それらの攻撃が成功する確率を導出し，それらの確率が無視できるほど小さいことを証明した．

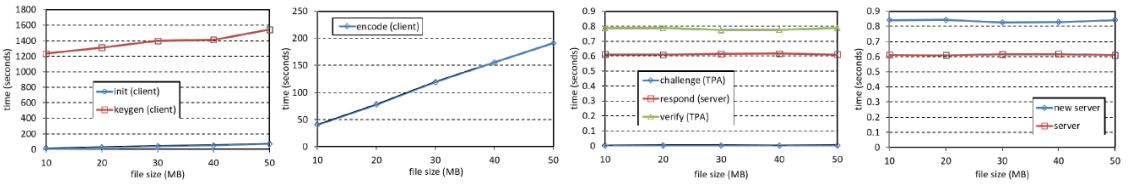
実装による性能評価では，4 つのフェーズにおいて，ファイルに関するパラメータの設定基準を明らかにするために性能評価を実施し，ファイルブロックサイズとファイルブロック数を

パラメータとする 2 つのケースについて比較評価を行った．実験環境は，クライアント／サーバのスペック：MacBook Pro，Intel Core i5 (2.7GHz)，RAM 16GB，実装言語：Python 2.7.11，セキュリティパラメータ：q=256bits，サーバ数：10，チェックブロック数：5 である．図 2 は，ファイルブロック数が固定でファイルブロックサイズが可変であるケース 1 の性能評価結果を示しており，図 3 は，ファイルブロックサイズが固定でファイルブロック数が可変であるケース 2 の性能評価結果を示している．また，図 4 は，ケース 1 とケース 2 の性能の比較結果である．その結果，与えられたあるデータ量に対して，ブロックサイズを固定してファイルブロック数を増やす方が効率的であることが実験的に明らかになった．実際には，チェックフェーズや修復フェーズが，初期化・鍵生成フェーズや符号化フェーズに比べて頻繁に行われることに留意すべきである．



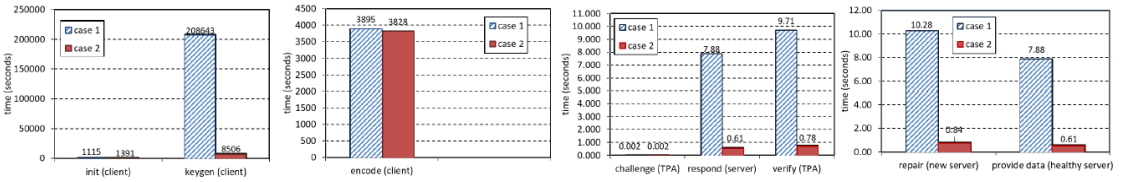
(a) Init, Keygen　(b) Encode　(c) Check　(d) Repair

図 2　ケース 1:ファイルブロック数が固定でファイルブロックサイズが可変のときの性能評価



(a) Init, Keygen　(b) Encode　(c) Check　(d) Repair

図 3　ケース 2:ファイルブロックサイズが固定でファイルブロック数が可変のときの性能評価



(a) Init, Keygen　(b) Encode　(c) Check　(d) Repair

図 4　ファイルサイズを 1GB に固定した場合のケース 1 とケース 2 の性能比較

４．研究成果

データ同士の演算が必要なデータ認証プロトコルにおいては，認証子同士の演算を可能にする準同型認証子が重要な暗号要素技術となっている．例えば，クラウドシステムにおける効率的なデータ認証プロトコルを構築する際，データの変更に伴って認証子も変更する必要があるため，準同型認証子を適用することは非常に有効である．本研究では，利用者の手を離れて認証子同士の演算を行うような先進的なユビキタス環境（ネットワークコーディング等を利用したセキュア分散ストレージシステム，センサネットワーク）における準同型認証子を用いた，機能が多彩で効率の良いデータ認証手法の研究を 3 年間取り組んできた．その結果，研究成果として雑誌論文 1 本[j1]，国際会議論文 6 本[c1, c2, c4, c6-c8]，及び国内研究会 2 本[c3, c5]が公表された．

平成 28 年度は，セキュア分散ストレージシステムを主な対象とし，Cater-Wagman MAC によって第三者検証可能な準同型認証子（VHMAC）の基本構成を提案した（国際会議論文 1 本）．さらに，マルウェア対策やプライバシを考慮したデータ認証手法に関する研究を実施した（雑誌論文 1 本，国際会議論文 2 本）．平成 29 年度は，VHMAC におけるデータの動的処理（データの更新・挿入・追加・削除）の検討を行うとともに，マルウェア対策を考慮したデータ認証手法に関する研究を実施した（国際会議論文 1 本，国内研究会 1 本）．平成 30 年度は，データの動的処理が可能なセキュア分散ストレージシステムの提案を行うとともに，マルウェア対策やブロックチェーンを考慮したデータ認証手法に関する研究を実施した（国際会議論文 2 本，国内研究会 1 本）．データの動的処理については，動的処理内容に応じて VHMAC を安全かつ効率的に

変換する手法を明らかにし，さらにネットワークコーディングを行う対象データの最適な範囲が不明であるという実運用上の課題を明らかにした．

＜引用文献＞
[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, “Provable Data Possession at Untrusted Stores”, ACM CCS’07, pp.598-609, 2007.
[2] A. Juels and B. Kaliski, “PORs. Proofs of retrievability for large files”, CCS’07, pp.584-597, 2007.
[3] H. Shacham and B. Waters, “Compact Proofs of Retrievability”, ASIACRYPT’08, pp.90-107, 2008.

５．主な発表論文等
〔雑誌論文〕（計１件）
[j1] Naoto Kawaguchi and Kazumasa Omote, “Malware Function Estimation using API in Initial Behavior”, IEICE Transactions on Fundamentals, Vol.E100-A, No.1, pp.167-175, January 2017. 【査読有り】

〔学会発表〕（計８件）
[c1] Masatsugu Oya and Kazumasa Omote, “Early Detection of Remote Access Trojan by Software Network Behavior”, The 14th International Conference on Information Security and Cryptology (Inscrypt 2018), LNCS, Vol.11449, Springer-Verlag, pp.658-671, 2018. 【査読有り】
[c2] Mitsuyoshi Imamura and Kazumasa Omote, “Network Deployments of Bitcoin Peers and Malicious Nodes based on Darknet Sensor”, The 19th World Conference on Information Security (WISA 2018), LNCS, Vol.11402, Springer-Verlag, pp.117-128, 2018. 【査読有り】
[c3] 渡邊竣，トラン フンタオ，面和成，「ネットワーク符号を基盤としたセキュアクラウドストレージにおけるデータ動的処理の検討」，IEICE Japan Tech. Rep.，ISEC 2018-9，pp.51-57，2018 年 5 月．
[c4] Genki Osada, Kazumasa Omote and Takashi Nishide, “Network Intrusion Detection based on Semi-Supervised Variational Auto-Encoder”, The 22nd European Symposium on Research in Computer Security (ESORICS 2017), LNCS, Vol.10493, Springer-Verlag, pp.344-361, 2017. 【査読有り】
[c5] トランフンタオ，面和成，「軽量なセキュアクラウドストレージのための Proof Of Retrievability」，IEICE Japan Tech. Rep.，ISEC 2017-38，pp.281-288，2017 年 7 月．
[c6] Tran Phuong Thao and Kazumasa Omote, “ELAR: Extremely Lightweight Auditing and Repairing for Cloud Security”, The 31st Annual Computer Security Applications Conference (ACSAC 2016), pp.40-51, 2016. 【査読有り】
[c7] Daichi Adachi and Kazumasa Omote, “A Host-Based Detection Method of Remote Access Trojan in the Early Stage”, The 12th International Conference on Information Security Practice and Experience (ISPEC 2016), LNCS, Vol.10060, Springer-Verlag, pp.110-121, 2016. 【査読有り】
[c8] Yosuke Ishikuro and Kazumasa Omote, “Privacy-Preserving Profile Matching Protocol Considering Conditions”, The 10th International Conference on Network and System Security (NSS 2016), LNCS, Vol.9955, Springer-Verlag, pp.171-183, 2016. 【査読有り】

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）
○取得状況（計０件）

〔その他〕
ホームページ等
http://www.risk.tsukuba.ac.jp/omote-lab/omote/

６．研究組織

(1)研究分担者
なし

(2)研究協力者
なし

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。