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　 ６ 月　 １ 日現在

機関番号：１３３０２
研究種目：若手研究(B)
研究期間：2013～2015
課題番号：２５７３００８３

研究課題名（和文）準同型認証子による効率の良いデータ認証手法に関する研究

研究課題名（英文）Research on efficient data authentication techniques using a homomorphic authentication code

研究代表者

面　和成（Omote, Kazumasa）

北陸先端科学技術大学院大学・情報科学研究科・准教授

研究者番号：５０４１７５０７

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：本研究では，信頼できないクラウドストレージにおいて，ネットワーク符号及び準同型認証子を適用することによってデータの修復を安全かつ効率的に可能とするデータ認証手法を提案した．本方式では，秘密鍵が異なる複数のクラウド利用者にも対応できる新たな準同型認証子を構築しただけでなく，データ所有者を介することなく健全なサーバのみでデータの修復が可能となる直接的修復（direct repair）機能を実現している．さらに，提案した準同型認証子をうまく適用することによって，データの直接修復かつ動的処理を可能とする現実的なセキュアクラウドシステムやデータの公平な売買システムの構築も行った．

研究成果の概要（英文）：In this research, we proposed the data authentication schemes which enabled data repair securely and efficiently by using network coding and homomorphic authentication code in untrusted storages. In these schemes, we constructed a new homomorphic authentication code which was able to deal with the different private keys for plural users, and we also achieved "direct repair" function of data which enables data repair by healthy servers without data owner. Furthermore, by using our proposed homomorphic authentication code, we constructed a practical secure cloud system which satisfied both direct repair and dynamic operations of data and we also constructed a fair trade system of data.

研究分野：情報セキュリティ

キーワード：データ認証　準同型性　認証子　ネットワーク符号　セキュアクラウドストレージ

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．一般的に，認証子は効率よく計算でき，また，上記のようなデータの完全性を保護できることから，データ認証プロトコルを実現するための重要な要素技術となっている．さらに，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．準同型認証子とは，例えば 2 つのデータ m1 と m2 から m1+m2 を演算する場合，それぞれの認証子 MAC1 と MAC2 から MAC1+MAC2 を演算することによって，(m1+m2) の認証子を秘密鍵なしに計算できるという性質を持つ認証子である．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．特に，分散ストレージシステム，センサネットワーク等，膨大なデータを演算する計算機器におけるデータ認証技術として近年注目を浴びている．しかしながら，準同型認証子には，ユビキタス環境等の先進的な環境に適用する際，(i) 異なる秘密鍵で生成された準同型認証子同士を演算できない，(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．

上記問題を解決するために，本研究ではデータ認証手法を確立し，かつ，その新たな応用について研究を進めていくものである．本研究において提案する準同型認証子の新しい構成法は，秘密鍵が異なる複数の利用者にも対応した現実的なものである．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，今後ますます重要になってくるユビキタス環境におけるデータ認証プロトコルとしても注目を浴びている．しかしながら，それらのプロトコルは単一の秘密鍵でしか認証子同士を演算できず，準同型認証子の現実的かつ効率的な構成法については，未だに十分な研究がなされているとは言えない．そのため，仮に効率のよいデータ認証手法を従来の準同型認証子で実現できたとしても，秘密鍵の種類数だけ認証子を保存しなければならず大きなコストが必要となってくる．これは，分散ストレージシステムやセンサネットワークといった利用者や端末が膨大であるシステムにとって望ましい状況ではない．

２．研究の目的

本研究では，以下の研究課題について研究開発を行う．

(1) 準同型認証子による現実的で効率の良いデータ認証手法（研究課題 1）

(2) 準同型認証子によるデータ認証手法の応用（研究課題 2）

[研究課題 1]

通常の準同型認証子を用いたデータ認証手法においては，単一の秘密鍵だけが使用されるに過ぎない．一方，本研究で提案する準同型認証子においては，秘密鍵が異なる複数の利用者にも対応しようとするものである．このような高度な準同型認証子を使用することで，分散ストレージシステムやセンサネットワーク等におけるデータ認証において，複数の秘密鍵を用いている認証子同士の演算が可能となる．

[研究課題 2]

準同型認証子は様々なデータ認証プロトコルの要素技術となるが，従来研究における準同型認証子は単一の秘密鍵を使用する場合にしか対応していない．そこで，準同型認証子のさらなる可能性を探るため，従来の準同型認証子の応用だけでなく，今回提案する新たな準同型認証子の応用についても研究開発を行う．特に，分散ストレージシステムやセンサネットワーク等に準同型認証子／提案準同型認証子を適用することを検討する．

本研究では，具体的なストレージシステムモデル（複数の信頼されるデータ所有者と複数の信頼できないストレージが存在するモデル）を想定し，準同型認証子による現実的で効率の良いデータ認証手法として PoR（Proof of Retrievability）方式の構築を目指す．PoR 方式は，ストレージサーバ上のデータの完全性を検証することに加えて，完全性の検証に成功した箇所の部分データ（符号語）の取出しが保証される方式である．ここでは，誤り訂正符号(error-correcting codes)や消失符号(erasure codes)を用いて符号化されたデータがストレージに保存される．なお，PoR 方式で用いられる準同型認証子としては，複数の秘密鍵を扱える新たな準同型認証子を構築する．

PoR に関する研究はこれまでに数多くなされてきているが，そこで用いられている準同型認証子は，秘密鍵が同一のものであり，異なる複数の利用者に対応したものはなかった．さらに，データ修復の際，準同型認証子の再計算が必要になり，データ所有者は膨大な認証子の再計算を行う必要があるという課題もあった．そこで本研究では，秘密鍵が異なる複数の利用者にも対応でき，かつ，データ修復の祭に準同型認証子の再計算が不要となり，認証子のままで直接的な修復処理(direct repair)が可能となる方式を提案する．より具体的には，以下のを満たす PoR 方式を提案する．

(1) 直接的修復：データ修復の際にデータ所有者が膨大な認証子の再計算を行う必要がなく，古い認証子から新しい認証子を直接的に生成できる性質．

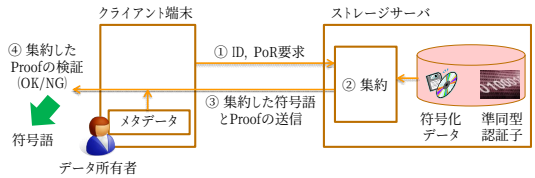

図 1 PoR 方式

(2) 複数ユーザ対応：複数のデータ所有者がそれぞれ異なる秘密鍵を持ち，かつ，準同型認証子による準同型演算が行えるということ．
(3) 共通鍵暗号ベース：演算が軽量な共通鍵暗号をベースとした準同型認証子．

さらに，提案方式の各フェーズにおける演算処理を実装評価することで効率性の評価を行う．

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．

(1) ストレージサーバには膨大なデータが保存されている．
(2) 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．

より具体的には，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．

(1) 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
(2) 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
(3) 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．

本研究では，複数の秘密鍵を扱える既存の準同型認証子である InterMAC に対して，秘密鍵が異なる複数のクラウド利用者に向けた改良を実施した．InterMAC はネットワーク通信において完全性検証を行うものであり，これを今回提案するストレージシステムに直接的に利用することはできず，利用するには鍵の非対称性が必要であった．そこで，InterMAC を改良することによって対称鍵で使われる InterMAC に鍵の非対称性を与えることに成功した．また，データ修復の際，通常の認証子では認証子の再計算が必要になるが，提案準同型認証子では認証子の再計算が不要となり，認証子のままで直接的な修復処理(direct repair)が可能となる．これにより，データ所有者は膨大な認証子の再計算を行う必要がなく，認証子から次の認証子を直接構成できる．本研究では，複数ユーザにおいてこの性質を世界で始めて実現した．

以下に提案した PoR 方式の具体的な 3 つのフェーズを記載する．

[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．

[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．

[サーバ復旧フェーズ]
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．

各プロトコルの実装評価では，チェックフェーズ及びサーバ復旧フェーズが効率的であることを確認した．まず実験環境は次の通

りであり，クライアント／サーバのスペック：Core i5 (2.4GHz), RAM 4GB, Win7(64bits), 実装言語：Python 2.7.3，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：10，復旧に必要なブロック数：20 である．図 2，3，4 では，符号化フェーズ，チェックフェーズ，及びサーバ復旧フェーズにおける各演算処理時間をデータサイズの増加と共にグラフで示した．符号化処理はデータサイズに対して線形になるが，これは最初の一度のみの処理なので大きな問題はない．これに対して，頻繁に行われるチェックフェーズにおける処理時間はスポットチェックのためデータサイズに対してほぼ一定となっており，1 回のチャレンジアンドレスポンスの演算処理は 1 秒未満で実施可能であることを確認した．

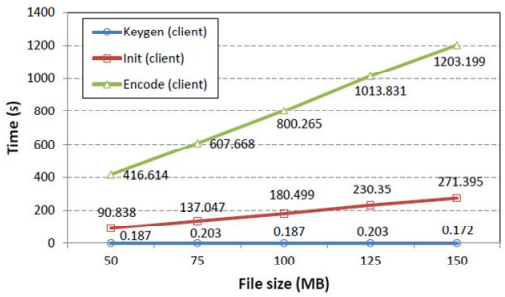

図 2 符号化フェーズにおける演算処理時間

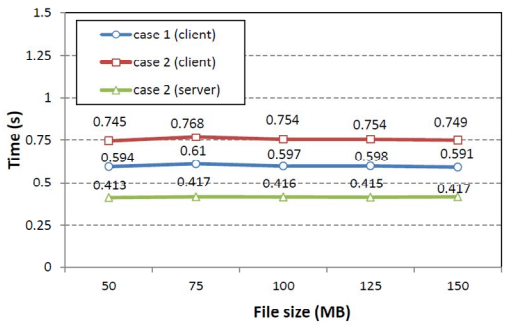

図 3：チェックフェーズ（チャレンジ・レスポンス処理）における演算処理時間

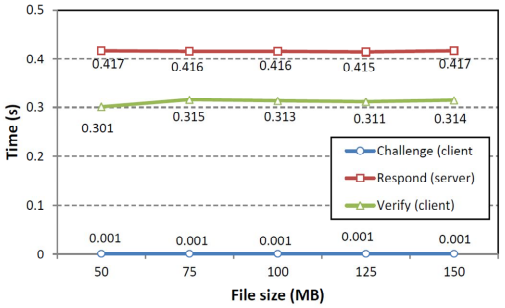

図 4：サーバ復旧フェーズにおける演算処理時間

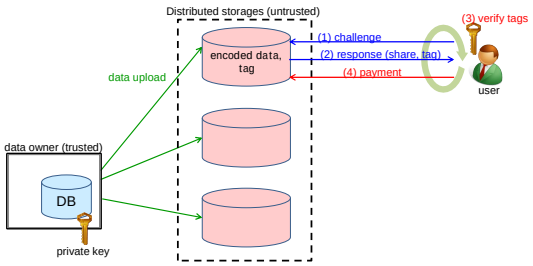

図 5：データ利用者と分散ストレージサーバ間の公平なデータ売買方式

データ利用者と分散ストレージサーバ間で公平にデータを売買する方式の実現に向けて PoR の応用手法を机上検討した（図 5 参照）．データ利用者にデータを売る際に，(a) 分散ストレージサーバが偽のデータを提供するリスクと (b) データ利用者が対価を支払わないというリスクが考えられる．本提案手法では，PoR の完全性と機密性を上手く利用することにより，データ利用者がデータを秘匿したままそのデータがデータ所有者のものであることを確認しながら，データの対価を支払うことができる．

4．研究成果

平成 25 年度は，具体的なクラウドシステムモデルを定義し，ネットワーク符号及び準同型認証子を用いることでデータの修復を効率的に可能とするデータ認証手法を提案した[j3,c5]．平成 26 年度は，秘密鍵が異なる複数のクラウド利用者にも対応できる新たな準同型認証子を構築した[j5,c4]．これは，秘密鍵が異なる複数の利用者に対応できるだけでなく，データ修復時における新たな機能である「direct repair」（直接的修復）を初めて実現する斬新なものであった．データ修復の際，通常の認証子では認証子の再計算が必要になるが，提案方式では認証子の再計算が不要となり認証子のままで「direct repair」が可能となる．平成 27 年度は，構築した新たな準同型認証子をセキュアクラウドシステムに応用した[j1,c1,c2,c3]．具体的には，提案した準同型認証子をうまく適用することによってデータの直接修復かつ動的処理を可能とするより現実的なセキュアクラウドシステム[j1,c1,c3]，及び提案した準同型認証子を用いた公平なデータ売買システム[c2]を提案した．さらに，センサネットワークや匿名通信におけるデータ認証手法に関する研究も実施した[j2,j4]．

5．主な発表論文等

〔雑誌論文〕（計 5 件）

[j1] Kazumasa Omote and Tran Phuong Thao, "D2-POR: Direct Repair and Dynamic Operations in Network Coding-based Proof of Retrievability", IEICE Transactions on

Information and Systems, vol. E99-D, no. 4, pp. 816-829, 2016.【査読有り】
[j2] Keita Emura, Akira Kanaoka, Satoshi Ohta, Kazumasa Omote and Takeshi Takahashi, "Secure and Anonymous Communication Technique: Formal Model and its Prototype Implementation", IEEE Transactions on Emerging Topics in Computing, Volume 4, Issue 1, pp.88-101, 2016.【査読有り】
[j3] Kazumasa Omote and Tran Phuong Thao, "ND-POR: A POR based on Network Coding and Dispersal Coding", IEICE Transactions on Information and Systems, vol. E98-D, no. 8, pp.1465-1476, 2015.【査読有り】
[j4] Atsuko Miyaji and Kazumasa Omote, "Self-healing wireless sensor networks", Concurrency and Computation: Practice and Experience, Volume 27, Issue 10, pp.2547-2568, 2015.【査読有り】
[j5] Kazumasa Omote and Tran Phuong Thao, "MD-POR: Multi-source and Direct Repair for Network Coding-based Proof of Retrievability", International Journal of Distributed Sensor Networks (IJDSN) vol. 2015, article ID: 586720, pp.1-15, 2015.【査読有り】

〔学会発表〕（計５件）
[c1] Kazumasa Omote and Tran Phuong Thao, "DD-POR: Dynamic Operations and Direct Repair in Network Coding-based Proof of Retrievability", The 21st Annual International Computing and Combinatorics Conference (COCOON 2015), LNCS, vol.9198, Springer-Verlag, pp.713-730, Bejing, China, August 4-6, 2015.【査読有り】
[c2] Kazumasa Omote and Tran Phuong Thao, "POR-2P: Network Coding-based POR for Data Provision-Payment System", The 10th International Conference on Risks and Security of Internet and Systems (CRISIS 2015), Springer-Verlag, Mytilene, Greece, July 20-22, 2015.【査読有り】
[c3] Kazumasa Omote and Tran Phuong Thao, "SW-SSS: Slepian-Wolf Coding-based Secret Sharing Scheme", The 8th Conference on Computational Intelligence in Security for Information Systems (CISIS 2015), Advances in Intelligent Systems and Computing, vol. 369, Springer-Verlag, pp.347-365, Burgos, Spain, June 15-17, 2015.【査読有り】
[c4] Kazumasa Omote and Tran Thao Phoung, "MDNC: Multi-source and Direct Repair in Network Coding-based Proof of Retrievability Scheme", The 15th International Workshop on Information Security Applications (WISA 2014), pp.177-188, Jeju Island, Korea, August 25-27, 2014.【査読有り】
[c5] Kazumasa Omote and Tran Thao Phoung, "A new Efficient and Secure POR Scheme Based on Network Coding", The 28th IEEE InternationalConference on Advanced Information Networking and Applications (AINA 2014), IEEE, pp.98-105, Victoria, Canada, May 13-16, 2014.【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.jaist.ac.jp/is/labs/omote-lab/index.html

６．研究組織
(1)研究代表
面 和成（OMOTE KAZUMASA）
北陸先端科学技術大学院大学・情報科学研究科・准教授
研究者番号：５０４１７５０７

(2)研究分担者
なし

(3)連携研究者
なし