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　２９　年　　６　月　１１　日現在

機関番号：　８２６２６
研究種目：　若手研究(B)
研究期間：　2014～2016
課題番号：　２６７３００６８

研究課題名（和文）クラウドサービスに適した階層型計算委託に関する研究

研究課題名（英文）A Study on Hierarchical Delegation of Computation for Cloud Services

研究代表者
松田　隆宏（MATSUDA, Takahiro）

国立研究開発法人産業技術総合研究所・情報技術研究部門・研究員

研究者番号：６０７０９４９２

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：必ずしも信頼できない第三者よって行われた計算の結果の正しさ（計算時の不正）を検証できる暗号技術である検証可能計算委託技術の高効率化、柔軟化を目指した。研究を進める中で、暗号文の宛先変更（再暗号化）が可能な公開鍵暗号技術である代理人再暗号化技術に着目し、再暗号化手続きの検証が可能な方式や、準同型性を持つ方式などの成果を得た。

研究成果の概要（英文）：Verifiable delegation of computation is a cryptographic technology in which computation performed by a third party can later be verified. We studied how to make it more efficient and flexible. As our main work, we focused on proxy re-encryption, which is a cryptographic primitive in which the task of changing the destination of ciphertexts (i.e. re-encryption) can be delegated to a third party, and obtained several results on it. In particular, we proposed proxy re-encryption that supports the verifiability of the re-encryption procedure, and one that supports the homomorphic property.

研究分野：　暗号理論

キーワード：　暗号技術

１．研究開始当初の背景

近年、Amazon EC2 などの計算資源を販売する型のクラウドサービスのビジネスが盛んとなっている。この種のサービスの最大の利点は、自前で高価なハードウェアを用意すること無く、大規模な計算を実行可能であるという点である。しかし、計算が利用者の手を離れたサービス業者の計算資源上で行われるため、依頼先のサービス業者に、非常に強い信頼性を置かねばならないという問題がある。サービス提供者に置かねばならない信頼性レベルの高さは、利用者にサービス使用を躊躇させる原因となる。

その事態を解決するための技術の一つとして、「検証可能計算委託」という暗号技術がある。この暗号技術は、必ずしも信頼できないエンティティによって行われた、委託した計算の、「計算結果の正しさ」の検証(計算時の不正の検出)を行うことができる、という機能を持つ。しかし、従来の検証可能計算委託には、効率性と柔軟性、二つの面で課題がある。より具体的には、任意の関数の計算を委託可能な方式は、通信回数、計算コスト、通信量等などが、実利用不可能なほど非効率なものしか知られておらず、効率性に乏しい。また、委託したい計算の切り分けや再委託などが考えられておらず、柔軟性に乏しい。

これらの問題を解決した検証可能計算委託が実現できれば、クラウドサービス業者におかねばならない信頼性レベルを低減できるため、サービス利用者にとっての利用の障壁を低減することができることに加えて、計算資源販売型のクラウドサービスにおいて扱うことができる計算の種類の柔軟化につながり、クラウドサービス提供者・利用者双方に貢献できることが期待できる。

２．研究の目的

従来の検証可能計算の課題を解決し、クラウドサービスでの利用に適した、効率的で柔軟な操作が可能な検証可能計算技術の実現を目指す。より具体的には、計算を「階層的」に委託可能な検証可能計算技術について、その機能及び安全性要件やモデル、などの基礎理論の整備を行い、さらに効率的な構成を与えることを目指す。また、目的技術の構成のために有用な構成要素となり得る技術についても明らかにし、それらを含めた検証可能計算技術の理論基盤を構築することを目指す。ただし、一つの可能性として、そもそも理論的な効率の下界が存在し、効率的な構成自体が達成不可能な場合がある。従って、研究を進めるうえで効率的な構成が困難であると判明した場合には、構成の(不)可能性を明らかにすることや、計算可能な関数を限定することで、効率的な方式の構成を目指す。

３．研究の方法

目的の実現のために、本研究では大まかに分けて３つの段階に分けて研究を進める。段階１においては、階層型検証可能計算委託の機能要件及び安全性要件を整理し、厳密な安全性モデルの定式化を行う。段階２においては、実際に個別の計算問題の困難性に基づいて、暗号学的な安全性の証明可能な方式の構築を行う。段階３においては、段階２にで得られた方式の一般化、効率化を検討する。そして、基礎的な統計関数など簡素かつ有用ないくつかの関数について、提案した方式のプロトタイプ実装を行う。また、研究開始前の現時点では、段階２においてあらゆる関数について安全な階層型検証可能計算委託は不可能、という場合もあり得るため、段階２において困難に直面した場合は、不可能性の証明や、関数のクラスを意味のある範囲で制限し、そのクラスに対し安全な方式の検討を行う。

４．研究成果

初年度である平成 26 年度に前述の研究計画に基づいて研究を開始し、文献調査及び初期の検討を重ねた結果、まず個別の具体的な暗号学的な操作(計算)の委託技術である、代理人再暗号化（Proxy Re-Encryption）に着目して、定式化、方式構築、理論整備などに集中的に取り組んだ。代理人再暗号化技術とは、あるユーザ A 宛の暗号文を、A が委託を許した「代理人」が、別のユーザ B が復号できる暗号文へと変換(再暗号化)できる技術である。しかも再暗号化のプロセスにおいて、代理人に平文の情報は洩れない、という性質を持つ。この暗号要素技術は、クラウドストレージにおいて、暗号化したままでの他のユーザとのファイル共有などに利用できる。（実際、現在まで、複数の企業が、代理人再暗号化技術を用いた商用サービスを行っている。）従来の代理人再暗号化方式では、代理人が再暗号化の手続きを正しく行ったかどうかを、再暗号化された暗号文の受信者が検証できることは保証されていない。そこで、受信者が再暗号化前後の暗号文を基に、代理人によって再暗号化手続きが正しく行われたかどうかを検証することができる機能を有する代理人再暗号化の機能・安全性要件を定式化した。そして、同機能・安全性要件を満足する方式の構成法を示し、厳密な安全性証明も与えた。提案した検証可能代理再暗号化の構成は、公開鍵暗号や電子署名など、基礎的な暗号要素技術を構成要素とする一般的な構成となっているため、構成要素に具体的な計算問題の困難性に基づく方式を当てはめることにより、目的とする検証可能代理人再暗号化が直ちに得られる。この成果は、暗号研究分野において権威ある国際会議 CT-RSA 2015 において採録された。なお、本提案構成において考えている方式の委託計算、すなわち暗号文の再暗号化は一度のみであるが、構成要素に追加の性質を要求することで、本研究が最終的に目指す「階層的」な計算の委託(代理人再暗号化の文脈において

は複数回の再暗号化)が可能であると考えられる。実際にそれを厳密に証明することは、今後の課題である。

研究計画においては、当初は汎用的な計算クラスについての検証可能計算クラスについての方式を目指す予定であったが、実際には代理人再暗号化方式に関する成果が、理論的にも非常に高度なものになったこと、及び代理人再暗号化それ自体がクラウドサービスにおいて今後幅広い利用が期待される重要な暗号要素技術であることから、初年度から次年度にかけて、同技術に関する成果を深化する方向へと重点を置いて研究をすすめた。平成 26 年度には、検証可能代理人再暗号化方式に関する研究によって得られた代理再暗号化に関する知見に基づき、検証可能計算の構成に潜在的に有用な、新たな機能を有する代理再暗号化方式を提案した。より具体的には、代理人再暗号化における再暗号化後の暗号文上でのみ、暗号化したままで平文に対し演算を施すことができる性質を持つ「準同型代理再暗号化方式」を定式化し、効率的な方式の構成法を示した。さらに、既存研究によって、準同型暗号から検証可能計算委託への変換方法が知られており、この方法を提案方式に適用することで、従来方式が持たない柔軟性と安全性を両立する計算委託を可能な方式が可能であることを示した。この成果は、その前身となる成果を国内会議 SCIS 2016 において発表した。(本文書の執筆時点では、準同型型代理再暗号化方式に関する研究成果について、完全版を国際論文誌へ投稿準備を進めている。)

また、平成 27 年度においては、他に以下の様な成果を挙げた：汎用的な検証可能計算委託の実現の理論的(不)可能性について文献調査及び検討を進める中で、検証可能計算委託自体の実現可能性と密接に結びついている暗号技術である SNARG (Succinct Non-interactive Argument)の実現に必須とされる暗号学的仮定の、公開鍵暗号における応用を見出した。この成果は、暗号研究分野において権威ある国際会議 PKC 2016 において採録された。さらに、検証可能計算と深い「述語暗号」と呼ばれる高機能な公開鍵暗号の一種である時限機能付き暗号の構成法について示した成果が、国際論文誌 International Journal of Information Security に採録された。

平成 28 年度には、平成 26 年度に提案した検証可能代理人再暗号化方式の構成要素について再考を与えた。代理人再暗号化における代理人の不正検出には、暗号文の手続きの際に、暗号文の復号結果の正しさを第三者に検証可能な公開鍵暗号が必要であり、その様な公開鍵暗号技術は非対話型開示機能付き公開鍵暗号(Public Key Encryption with Non-interactive Opening、以下 PKENO)と呼ばれる。平成 28 年度には、この PKENO の個脳の拡張と新たな構成法を成果として得られ、これによって、さらに検証可能代理人再暗号化の構成の幅が広がったと考えられる。この成果は、国際会議 ISITA 2016 において発表した。

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 Yusuke Sakai Takahiro Matsuda, Goichiro Hanaoka. “Tag-KEM/DEM framework for public-key encryption with non-interactive opening,” Proceedings of 2016 International Symposium on Information Theory and its Applications (ISITA 2016), pp. 231-235, 2016. (査読有)

② Kohei Kasamatsu, Takahiro Matsuda, Keita Emura, Nuttapong Attrapadung, Goichiro Hanoaka, Hideki Imai. “Time-specific encryption from forward secure encryption: generic and direct constructions.” International Journal on Information Security, Vol. 15, No. 5, pp. 549-571, October 2016. (査読有)
DOI: 10.1007/s10207-015-0304-y

③ Takahiro Matsuda, Goichiro Hanaoka. “Trading Plaintext-Awareness for Simulatability to Achieve Chosen Ciphertext Security.” Public-Key Cryptography – PKC 2016, Vol. 9614 of Lecture Notes in Computer Science, pp. 3-34, Springer, 2016. (査読有)
DOI: 10.1007/978-3-662-49384-7

④ 川合豊，松田隆宏，小関義博，花岡悟一郎．“準同型暗号における安全な分析の制御について．”2016 年暗号と情報セキュリティシンポジウム(SCIS 2016)予稿集，4E2-2，2016．(査読無)

⑤ Satsuya Ohata, Yutaka Kawai, Takahiro Matsuda, Goichiro Hanaoka, Kanta Matsuura. “Re-Encryption Verifiability: How to Detect Malicious Activities of a Proxy in Proxy Re-Encryption.” Topics in Cryptology – CT-RSA 2015. Vol. 9048 of Lecture Notes in Computer Science, pp. 410-428, Springer, 2015. (査読有)
DOI: 10.1007/978-3-319-16715-2_22

〔学会発表〕（計 4 件）

① Yusuke Sakai, Takahiro Matsuda, Goichiro Hanaoka. “Tag-KEM/DEM framework for public-key encryption with non-interactive opening.” 2016 International Symposium on Information Theory and its Applications (ISITA 2016). 2016 年 10

月 31 日. Monterey (California, USA).

② Takahiro Matsuda, Goichiro Hanaoka. “Trading Plaintext-Awareness for Simulatability for Achieving Chosen Ciphertext Security.” 19th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2016). 2016 年 3 月 7 日. Taipei (Taiwan).

③ 川合豊, 松田隆宏, 平野貴人, 小関義博, 花岡悟一郎. “準同型暗号における安全な分析の制御について.” 2016 年暗号と情報セキュリティシンポジウム(SCIS 2016). 2016 年 1 月 22 日. ANA クラウンプラザホテル熊本ニュースカイ(熊本県熊本市).

④ Satsuya Ohata, Yutaka Kawai, Takahiro Matsuda, Goichiro Hanaoka, Kanta Matsuura. “Re-Encryption Verifiability: How to Detect Malicious Activities of a Proxy in Proxy Re-Encryption.” The Cryptographers’ Track at the RSA Conference 2015 (CT-RSA 2015). 2015 年 4 月 24 日. San Francisco (California, USA).

６．研究組織

(1)研究代表者

松田　隆宏（MATSUDA, Takahiro）
国立研究開発法人産業技術総合研究所・情報技術研究部門・研究員
研究者番号： 60709492