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　１９　日現在

機関番号：　３２６６０
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６４２０３７３

研究課題名（和文）個人制御可能な秘匿計算手法に関する研究

研究課題名（英文）Research on an individual controllable secrecy computation

研究代表者
岩村　惠市（Iwamura, Keiichi）

東京理科大学・工学部電気工学科・教授

研究者番号：１０４３４０２８

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：スマホ等でも大量の情報を高速処理可能で、大量の情報を個人が管理・制御できる秘匿計算技術を確立した。特に、①実装による非対称型秘密分散法の有効性実証に関して、ライフログシステムを構築し、イノベーション・ジャパン2015とコンピュータセキュリティシンポジウム2015においてデモ展示を行った。また、②非対称型秘密分散法に適した秘匿計算の提案に関してその成果を論文誌に2件発表し、さらに、国際会議に7件発表した。また、1件の特許を出願した。また、③EXORを用いた非対称型秘密分散法の新たな応用に関してセンサネットワークと秘匿検索に対する応用を、論文誌に1件及び国際会議に3発表した。

研究成果の概要（英文）：The secrecy calculation technology in which a lot of information could be processed also for a smart phone high-speed, and an individual could manage and control a lot of information was established.In order to prove the validity of the asymmetrical secret sharing scheme by mounting, the life log system was built and demonstration exhibition was performed in innovation Japan 2015 and the computer security symposium 2015.About the proposal of secrecy calculation suitable for an asymmetrical secret sharing scheme, method, we published two paper to a paper magazine, made an international conference announcement of seven affairs, and performed a patent application.The application to a sensor network and secrecy search was announced to the paper magazine three times about new application of the asymmetrical secret sharing scheme using XOR at one affair and an international conference.

研究分野：　情報セキュリティ

キーワード：　秘密分散　秘匿計算　個人制御

１．研究開始当初の背景

ビッグデータの有効利用のため，ネット上に存在する大量のデータを分析・利用しようという研究が近年盛んに行われている．しかし，ネット上に存在する有用な情報の多くは，個人情報であることが多く，プライバシー保護とビッグデータ活用の両立が大きな課題となっている．

一方，近年プライバシー(権)とは個人が自分に関する情報を制御できる権利と定義される．よって，個人が自分の情報を制御・管理しながら，個人が同意した場合にのみその情報の分析・利用ができる仕組みが構築できれば，プライバシー保護とビッグデータ活用の両立が可能になり，ビッグデータ統合利活用が推進される．

そのため，プライバシー保護とビッグデータ活用を両立する技術として，秘匿計算に関する研究が最近盛んに行われている．秘匿計算とは情報を秘匿しながら，演算を行う技術である．これによって，プライバシーに関する情報を秘匿しながら，大量の情報を用いて統計演算を行えば，ビッグデータを有効に活用することができる．この秘匿計算手法は大きく，準同型暗号を用いる手法と秘密分散を用いる手法に分けられる．準同型暗号を用いる手法は一般的に計算量が多く処理が重いため，大量の情報を処理する場合には多くの処理時間が必要である．一方，秘密分散を用いる手法は一般的に処理が軽い．しかし，秘密分散は１つの秘密情報がｎ個に分散されるため，分散値を個人が管理することは難しい．

そこで，以下の要件を持つ秘匿計算技術の研究が必要になる．これによって個人が直接秘匿計算に参加でき，かつ個人の同意がなければ秘匿計算を行えない，すなわちプライバシー保護とビッグデータ活用の両立する技術が確立できる．

Ⅰ．スマホ等でも大量の情報を高速処理可能な軽量な秘匿計算技術
Ⅱ．大量の情報を個人が管理・制御できる秘匿計算技術

２．研究の目的

以下の３つを実現する．

① 実装による非対称型秘密分散法の有効性実証

研究代表者は既に非対称型秘密分散法と呼ぶ個人が秘密情報を管理可能な秘匿手法を提案している．しかし，その実用性検証は行われていなかった．そこで，この手法をスマホに実装し，スマホは１つの情報を管理するだけで，大量の情報の分散処理(秘匿化)及び復元処理が高速に実現できる，すなわち上記Ⅰ，Ⅱが実現できることを実証する．

② 非対称型秘密分散法に適した秘匿計算の提案

非対称型秘密分散法はShamirの(k,n)秘密分散法を基本としているため，秘匿加算は容易に行える．しかし，秘匿乗算や秘匿除算,秘匿比較演算などは研究課題を含む．よって，非対称型秘密分散に適した秘匿計算法を研究し，さらに①に示すスマホに実装して，秘匿計算に対しても上記Ⅰ，Ⅱが実現できることを示す．

③ EXOR を用いた非対称型秘密分散法の新たな応用

今まで提案している非対称型秘密分散には Shamir の(k,n)秘密分散法（以降，Shamir 法）の他に，EXOR を用いる秘密分散法[4]（以降，EXOR 法）がある．EXOR 法は秘匿計算には不適であるが，Shamir 法より処理が軽い．よって，EXOR 法をセンサネットワークなどに実装し，今まで秘密分散が使われていない分野への応用を検討し，利用のすそ野を広げる．

３．研究の方法

【平成２６年度】

前記①に示す実装による非対称型秘密分散法の有効性実証を行う．特に，スマホを用いたライフログシステムの構築を行う．また，②の非対称型秘密分散法に適した秘匿計算について研究を進める．

【平成２７年度】

平成２７年度は②についての研究を中心に行う．さらに，①で構築したスマホを用いたライフログシステムへの実装を行う．

【平成２８年度以降】

前記③に示すセンサネットワーク等への具体的応用を検討する．センサネットワークは次世代インフラの一つと考えられているが，セキュリティ対策が課題である．また，センサネットワーク以外の応用を検討し，確立する．

４．研究成果

前記①については、ライフログシステムを構築し、下記[その他]に示すように、イノベーション・ジャパン 2015 とコンピュータセキュリティシンポジウム 2015 においてデモ展示を行った。

また、②についてはその成果を下記[雑誌論文]の 1,3 に示すように論文誌（査読あり）に発表し、さらに、下記[学会発表]の 1,2,4-7,9 に示すように国際会議（査読あり）にも発表した。また、[産業財産権]に示すように１件の特許を出願した。

また、③についてはセンサネットワークに対する応用を、下記[雑誌論文]の 2 に示すように論文誌（査読あり）及び下記[学会発表]の 3 に示すように国際会議（査読あり）に発表した。また、秘匿検索に対する応用を検討し、[学会発表]の 8,10 に示すよう国際会議発表（査読あり）を行った。

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　3　件）

1. 神宮武志, 青井健, ムハンマド カマル アフマド アクマル アミヌディン, 岩村惠市:“秘密分散法を用いた次数変化のない秘匿計算手法”, 情報処理学会, 第 59 巻第 3 号, pp.1038-1049, Mar.2018.（査読有り）
2. 岩村 惠市, 須賀 祐治, 後藤 慎一, 金田 北洋：“クラスタツリー型センサネットワークに適した秘密分散法とそれを用いた鍵共有法”, 情報処理学会論文誌, Vol.57, No.10, pp.2236-2249, Oct.2016.（査読有り）
3. 渡辺泰平, 金田北洋, 岩村惠市, “サーバ台数の変化が生じない(k,n)しきい値秘密分散法に基づく乗算手法”, 電子情報通信学会論文誌 D, Vol.J98-D, No.3, pp.428-436, Mar.2015.（査読有り）

〔学会発表〕（計　11　件）

1. Kyohei Tokita, Keiichi Iwamura: "Fast Secure Computation Based on a Secret Sharing Scheme for n < 2k - 1," IEEE Fourth Conference On Mobile And Secure Services, pp.32-36, Miami USA, Feb.24-25 2018.
2. Kentaro Tsujishita, Keiichi Iwamura: "Password-Protected Secret Sharing Scheme with the Same Threshold in Distribution and Restoration," IEEE Fourth Conference On Mobile And Secure Services, pp.48-52, Miami USA, Feb.24-25 2018.
3. Ahmad Akmal Aminuddin Mohd Kamal, Keiichi Iwamura, Hyunho Kang: "Searchable Encryption of Image based on Secret Sharing Scheme ," Proceedings of APSIPA Annual Summit and Conference 2017, pp.1-9, Kuala Lumpur, Malaysia, Dec.12-15 2017.
4. 鴇田 恭平・岩村 惠市：“XOR 法の拡張による効率的な秘匿計算の実現”, コンピュータセキュリティシンポジウム 2017, 2E2-3, Oct.23-25 2017
5. Ahmad Akmal Aminuddin Mohd Kamal and Keiichi Iwamura：“Conditionally Secure Multiparty Computation using Secret Sharing Scheme for n<2k-1”, The fifteenth International Conference on Privacy, Security and Trust (PST2017), pp.1-6, Calgary, Canada, Aug.28-30 2017.
6. Naoto Kaneko, Keiichi Iwamura: "Improvement of Communication Traffic and Security of Proactive Secret Sharing Schemes and Combination Proactive Secret Sharing Scheme with an Asymmetric Secret Sharing Scheme", The 13-th International Symposium on Frontiers of Information Systems and Network Applications (FINA 2017), FINA-S1(3), pp.13-18, Taipei Taiwan, Mar.27-29 2017.
7. Ken Aoi, Takeshi Shingu, Keiichi Iwamura: "Security Evaluation on Secret Computation without Changing the Polynomial Degree",The 13-th International Symposium on Frontiers of Information Systems and Network Applications (FINA 2017). FINA-S3(2), pp.56-61, Taipei Taiwan, Mar.27-29 2017.
8. Naoto Kaneko, Keiichi Iwamura：“Proactive Secret Sharing Scheme Suitable for Asymmetric Secret Sharing Scheme,” The 5th IEEE Global Conference on Consumer Electronics (GCCE 2016), pp.429-430, Kyoto, Japan, Oct.11-14, 2016.
9. Taihei Watanabe, Keiichi Iwamura, Kitahiro Kaneda:" Secrecy Multiplication Based on a (k,n)-Threshold Secret-Sharing Scheme Using Only k Servers”, The 6th FTRA International Conference on Computer Science and its Applications (CSA2014), pp107-112, Guam, December.2014.
10. Takeshi Shingu, Keiichi Iwamura and Kitahiro Kaneda: "Secrecy Computation without Changing Polynomial Degree in Shamir's (K, N) Secret Sharing Scheme," ICETE 8th Data communication networks (DCNET 2016), pp.89-94, Lisbon, Portugal, 26-28 July, 2016(Student Best Paper Award).
11. Shinichi Goto, Keiichi Iwamura, Yuji Suga and Kitahiro Kaneda: "Secret Sharing Scheme and Key Sharing Scheme Suitable for Clustered Sensor Networks," 14th International Conference on Wireless Networks and Mobile Systems (WINSYS2016), pp.172-180, Lisbon, Portugal, 26-28 July, 2016.

〔産業財産権〕
○出願状況（計　1　件）

名称：秘密分散を用いた秘匿演算システムに関する計算装置
発明者：岩村惠市
権利者：東京理科大学
種類：特許
番号：特願 2015-25825
出願年月日：平成 27 年 2 月 12 日
国内外の別：国内

〔その他〕
1. イノベーション・ジャパン 2015 におけるデモ展示「ビッグデータの有効活用とプライバシー保護を実現する個人制御可能な秘匿計算システム」
2. コンピュータセキュリティシンポジウム 2015 におけるデモ展示「膨大なデータを個人制御可能な秘密分散を用いた秘匿計算システム」

６．研究組織
(1)研究代表者
岩村惠市（IWAMURA, Keiichi）
東京理科大学・工学部・教授
研究者番号：10434028