Keywords you should know. 第159回

知っておきたいキーワード

秘密計算

Ahmad Akmal Aminuddin †

† 東京理科大学 工学部 情報工学科
"Secure Computation" by Ahmad Akmal Aminuddin (Department of Information and Computer Technology, Tokyo University of Science, Tokyo)
キーワード：秘密計算，マルチパーティ計算，秘密分散，プライバシー保護，情報セキュリティ

まえがき

Society 5.0とは，さまざまな知識と情報が共有される社会であり，モノのインターネット（IoT: Internet of Things）をはじめとする，さまざまな情報収集技術により収集した大量のデータを使いこなして，リアルタイムでの自動健康診断や病気の早期発見など，今までにない新たな価値のあるサービスを生み出し，質の高い豊かで安心な生活を実現するデータ駆動社会である．しかし，収集したデータには，秘密情報の漏洩やプライバシーの侵害などの課題が存在する．また，欧州連合（EU: European Union）の一般データ保護規制（GDPR: General Data Protection Regulation）や日本の改正個人情報保護法などの法整備からも，秘密情報を保護しながらデータを活用できる技術がより重要視されていることが見て取れる．この課題に対して，自由なデータ流通と機密情報保護を両立できる秘密計算技術が注目されている．本稿では，なぜ秘密計算が必要なのかから説明し，秘密計算の原理，歴史，実現する手法を紹介する．また，平均年収を求める問題を例とし，秘密計算の仕組みを説明し，最後に，応用例を紹介する．

秘密計算が必要な理由

情報の機密性を保護できる技術として，暗号という手法は昔から知られている．暗号とは，元となる意味がある秘密情報に対して，異なる意味を持つ暗号化した情報に変換し，解読できない状態にすることである．この処理を暗号化といい，元の情報に戻す処理を復号という（図1）．

暗号技術を利用し，ゲノムや個人の年収情報など，さまざまな機密性の高い情報を安全に保管・収集することができる．しかし，集めたデータを解析し，何かの新しい知見を得るには，暗号化した情報を一旦元の情報に復号してから解析を行う必要があるため，秘密情報が漏洩する可能性がある．

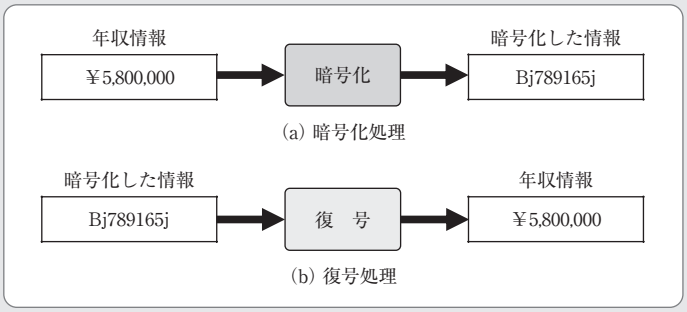

図1　従来暗号技術の暗号化と復号処理

秘密計算の概念とモデル

秘密計算とは，データを秘匿したまま計算を行う技術であり，1980年代に基礎的な秘密計算方式が提案されてから，現在まで，日本国内外において盛んに研究されている．秘密計算を導入することで，暗号化したデータを秘匿したまま計算を行う秘密計算処理が可能となるため，完全に信頼できない環境下でも，生データと同じ精度で分析を行うことができる上に，暗号化したデータは復号しないため秘密情報漏洩のリスクを回避できる．

近年では，データの保存をクラウドサーバに委託するビジネスモデルが注目される．本稿では，秘密情報所有者（クライアント）がクラウドサーバに情報をアウトソーシングし，計算資源や解析のノウハウを持つサーバは，収集したデータをもとに，秘密計算を用いて，安全に解析を行い，最終結果だけを秘密計算を依頼したクライアント（例えば，研究者や企業など）に返すというクライアント・サーバモデルを想定する（図2）．

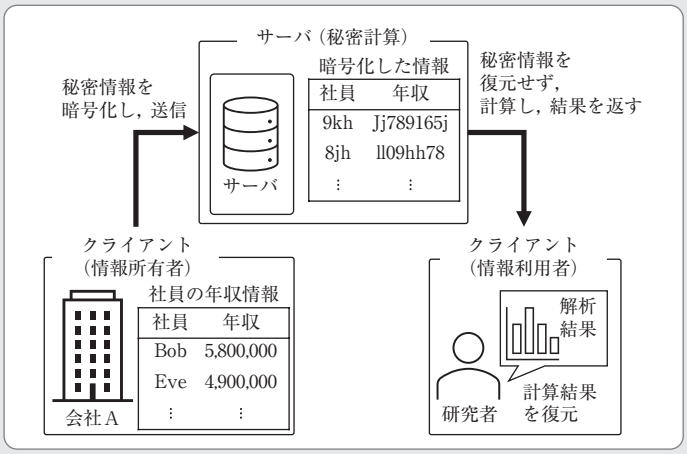

図2　クライアント・サーバモデル

秘密計算の歴史と実現する手法

(1) 秘匿回路（Garbled Circuit）

1982年に，Yaoは，2者間の金持ち比べ問題（お互いの財産を秘密にしたまま，どちらがお金を持っているかを知る問題）に対して，初めての秘匿回路を用いた秘密計算法を提案したが，秘匿回路の作成処理には時間がかかるという課題がある．

(2) 秘密分散（Secret Sharing）

1988年に，Ben-Orらは，高速な計算ができる秘密分散を用いた秘密計算法を提案した．秘密分散は，高速な処理を実現できるが，独立して管理される複数サーバ間の通信が必要であるため，高速な通信網で繋がれている複数台（乗算が必要な場合，3台以上）のサーバが必要という課題がある．

(3) 準同型暗号（Homomorphic Encryption）

1台のサーバでも秘密計算が実現できる方法として，準同型暗号が知られている．2009年に，Gentryは，乗算の回数に制限がない，加算と乗算を任意にできる完全準同型暗号を提案したが，秘密分散と比べて，計算量が格段に多く，計算に多大な時間がかかるという課題がある．その後，実世界の応用を重視した秘密計算法も多数提案されているが，その詳細は省略する．

(4) 信頼できる実行環境（TEE: Trusted Execution Environment）

最近登場した技術であるTEEとは，プロセッサ内に加えられた機能で，オペレーティングシステムから独立した，デバイスのメモリー上に構築される信頼できる実行環境のことである．秘密計算は，信頼領域内で処理されるため，秘密分散を用いた場合と比較し，複数サーバ間の通信を必要とせず実現できるが，サイドチャネル攻撃（ハードウェアを物理的に観測し，内部の情報を得る攻撃）に弱いという課題がある．

秘密分散を用いた秘密計算

クライアント・サーバモデルにおける秘密分散を用いた秘密計算の仕組みを解説する．

(1) 秘密分散について

秘密分散とは，ある秘密情報を複数の異なる値（シェアと呼ぶ）に変換し，複数の独立に管理されているサーバに保管する手法である．秘密分散法の例としては，(k, n) 閾値秘密分散や，加法型秘密分散など（ISO/IEC19592-2:2017）があるが，ここでは，最も理解しやすい加法型秘密分散を紹介する．

加法型秘密分散は，満場一致法を採用した秘密分散法であり，n 台のサーバが保持する n 個のシェアをすべて集めないと，元の秘密情報を復元できないという性質を持つ（分散と復元は，Algorithm 1，2を参照）．以降では，サーバ S_i が保持する，秘密情報 s に対するシェアを $[s]_i$ とし，$i = 1, ..., n$ が各サーバの識別子であり，公開される情報とする．また，以降の説明では，秘密情報などを整数とするが，通常の場合，秘密情報や，シェアなどは，有限体 $\mathbb{Z}/p\mathbb{Z}$ 上の元であり，すべての計算は $\mathbb{Z}/p\mathbb{Z}$ 上で実現される（p は素数とする）．

☞

Algorithm 1：分散処理

①$n-1$個の乱数$a_1, \ldots, a_{n-1}$を選んで，$n-1$台サーバのシェア$[s]_1 = a_1, \ldots, [s]_{n-1} = a_{n-1}$とする．

②式(1)でn番目のシェア$[s]_n$を計算する．

$$[s]_n = s - \sum_{j=1}^{n-1} [s]_j \qquad (1)$$

Algorithm 2：復元処理

①n台のサーバからn個のシェアを集めて，式(2)より秘密情報sを復元する．

$$s = [s]_1 + [s]_2 + \cdots + [s]_n = \sum_{i=1}^{n} [s]_i \qquad (2)$$

(2) 秘密計算の手順

Aliceは，秘密計算を行う$n=2$台のサーバS_1, S_2を用いて，会社Aで働いているBob, Charlie, Dave, EveとFredの平均年収を求めたい場合を考える(図3)．

(a) 分散処理

クライアントは分散処理を実行し，年収情報を$n=2$台のサーバに分散する．例えば，Bobの年収$b=480$万円に対して，$n-1=$一つランダムな値，$[b]_1=283$を選んで，S_1に送り，$[b]_2 = 480-283=197$を計算し，S_2に送る．残りの年収に対しても同じ処理を実行すると，各サーバは，図3に示すようなシェアを保持する．

(b) 秘密計算処理

各サーバは，送られてきたシェアを用いて，秘密計算処理(この場合，平均値を計算)を実行し，結果をAliceに返す．例えば，S_1は，保持しているシェアの平均値，$[avg]_1 = (283+303+272+377+145)/5 = 276$を計算し，Aliceに渡す．$S_2$も同様に，$[avg]_2 = 244$を計算し，Aliceに渡す．

(c) 復元処理

Aliceは，送られてきたシェアを足し合わせて，各社員の年収を知らなくても，その平均年収，$avg = 276+244 = 520$万円を求めることができる．

(3) 秘密分散を用いた秘密計算の課題

秘密分散を用いた加算，定数との乗算は簡単に実現できるが，例えば，$n=2$の場合，加法型秘密分散法で分散された秘密情報b, cの乗算結果bcを求めるには，以下の計算が必要にある．

$$\begin{aligned} bc &= ([b]_1 + [b]_2)([c]_1 + [c]_2) \\ &= ([b]_1[c]_1 + [b]_2[c]_2) \\ &\quad + ([b]_1[c]_2 + [b]_2[c]_1) \end{aligned}$$

加算処理と異なり，単純に各サーバが保持しているシェア同士の演算だけでは実現できず，サーバ間の通信，シェア数の増加などの問題が生じ，全体の処理速度へ影響を与える．このように，乗算処理を効率的に行うことは，秘密計算を実用化する前に解決しなければならない課題となる．(k, n)閾値秘密分散を用いた乗算処理も同様な課題がある．この課題の対策法として，補助乱数を導入した秘密計算[1]や，著者が提案したTUS方式[2]などがあげられる．本稿では，これ以上言及しないが，興味のある方は，この機会に，各論文を参照されたい．

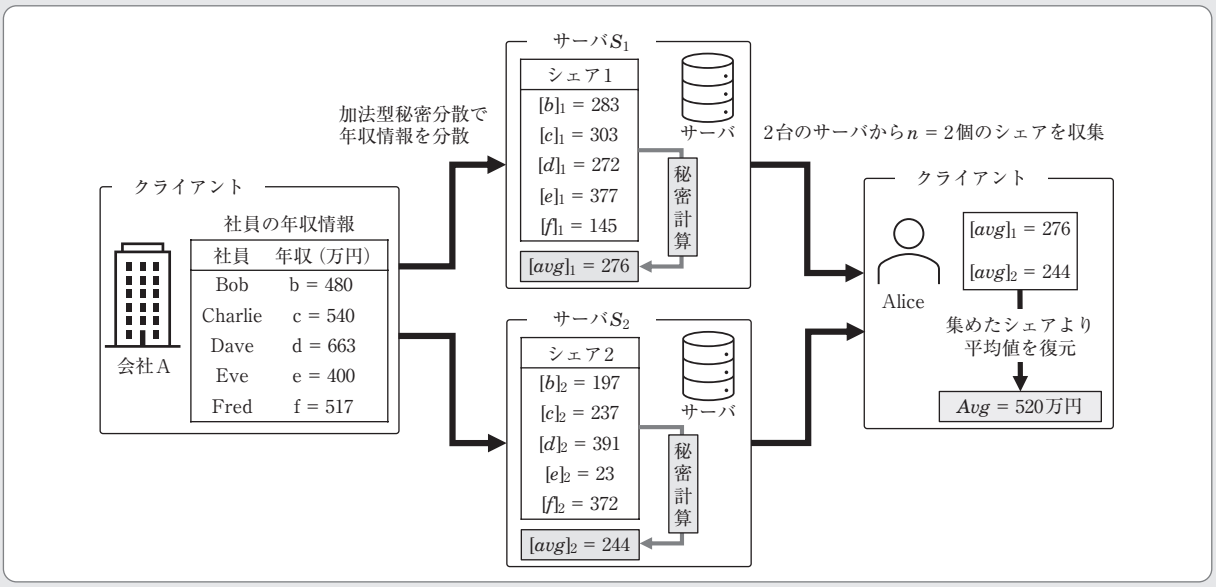

図3　加法型秘密分散を用いた秘密計算の例

秘密計算の応用例

秘密計算の最も有名な活用事例は，2008年の甜菜オークションである．デンマーク唯一の甜菜加工会社であるDanisco社，農家連合と研究機関の三者間で，秘密計算を用いて，農家の入札情報を秘匿したまま，セキュアなオークションが実施された[3]．また，2019年には，NECと大阪大学の共同研究において，秘密計算を利用し，ゲノム情報を保護しながら，安全に解析できるようにした[4]．この他にも，創薬における予測モデルの構築や，患者の情報を保護したまま炎症性腸疾患に関する観察研究なども，近年，盛んに行われる．さらに，Dropboxなどのクラウドストレージサービスの普及とともに，秘密計算を利用し，保管されている暗号化したデータを復号せずに検索ができる秘匿検索技術も盛んに研究されている[5]．

むすび

ここ数年，秘密計算の定義化（ISO/IEC4922-1:2023）や秘密計算を実現する方式の定式化（ISO/IEC4922-2:2024）の活動が進んでいる．また，Cybernetica社のSharemind，NTTのMEVALなど，秘密計算のサービス・ライブラリーも多数提案されている．さらに，近年では，AI（人工知能）を用いた画像認識などの活用も普及し，AIによる個人，または，機密性の高いデータの解析においても，秘密計算技術は不可欠である．このことから秘密計算は，今後のさらなる展開やさまざまな分野への活用が期待される技術であると考えられる．

（2024年7月24日受付）

参 考 文 献

1) T. Araki, J. Furukawa, Y. Lindell, A. Nof and K. Ohara: "High-throughput semi-honest secure three-party computation with an honest majority", in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), pp.805-817 (2016)
2) K. Iwamura and A. Kamal: "Communication-efficient secure computation of encrypted inputs using (k, n) threshold secret sharing", IEEE Access, 11, pp.51166-51184 (2023)
3) P. Bogetoft, et al.: "Secure multiparty computation goes live", in: Dingledine, R., Golle, P. (eds) Financial Cryptography and Data Security (FC 2009), LNCS, 5628, pp.325-343 (2009)
4) NEC：“NEC・大阪大学，複数機関が保有するゲノム情報をプライバシー侵害リスクを抑えて解析できることを実証 ～データを暗号化したまま解析できる秘密計算で実現～”，2019年7月23日，https://jpn.nec.com/press/201907/20190723_03.html（参照：2024年7月13日）
5) A. Kamal and K. Iwamura: "Searchable encryption using secret sharing scheme that realizes direct search of encrypted documents and disjunctive search of multiple keywords", Journal of Information Security and Applications, 59, p.102824 (2021)

Ahmad Akmal Aminuddin（アフマド アクマル アミヌディン）

2022年，東京理科大学大学院工学研究科電気工学専攻博士後期課程修了．同年，同大学工学部情報工学科助教となり，現在に至る．情報の秘匿性を保護しながら情報の利活用ができる技術である秘密計算およびその応用である秘匿検索に関する研究に従事．博士（工学）．

キーワード募集中

この企画で解説して欲しいキーワードを会員の皆様から募集します．ホームページ（https://www.ite.or.jp/）の会員の声より入力可能です．また電子メール（ite@ite.or.jp），FAX（03-3432-4675）等でも受け付けますので，是非，編集部までお寄せください．

（編集委員会）