SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

TTP を用いて 1 台のサーバで構成可能な秘密分散法による秘匿計算
Secrecy Computation using Secret Sharing Scheme Configurable on a Single Server using Trusted Third Party

岩村 恵市 * 白井 洸多 * 稲村 勝樹 †
Keiichi Iwamura Kota Shirai Masaki Inamura

キーワード 秘匿計算，秘密分散，$n < k$，マルチパーティ計算，情報理論的安全性，高速処理

あらまし

AI（Artificial Intelligence）などで解析してフィジカル空間にフィードバックさせる時に用いられるビッグデータについて，これらのデータの中には個人情報や機密情報が含まれることも多く，プライバシー保護や機密保護を考慮しながらデータの利活用を行う仕組みが必要とされる．秘匿計算を行う手法は大きく分けると，準同型暗号を用いる方式と，秘密分散法を用いる方式があるが，IoT（Internet of Things）デバイスなどから収集された膨大なビッグデータを AI などで処理するためには，計算量が軽い秘密分散法が適していると言える．

秘密分散法の特徴は，分散した n 個の分散値から k 個の分散値を集めれば元の秘密情報を復元できるが，k 個未満の分散値からは秘密情報に関する情報を一切得ることができないということである．ここで，もしサーバが同一の組織などで管理された場合，k 個の分散値が集まり秘密情報は漏洩することになる．

また，従来の秘密分散法を用いた秘匿計算においては，秘匿加算は容易に実現できるが，秘匿乗算を行う際に問題が生じることが知られている．例えば，Shamir によって提案された (k, n) 閾値秘密分散法では，秘匿乗算を行うと多項式の次数が $k-1$ から $2k-2$ に変化してしまうので，秘密情報を復元するために必要となる分散値の数が k 個から $2k-1$ 個に変化してしまうという問題がある．

それに対して我々のグループでは，TTP（Trusted Third Party）を想定することによって，$k \leq n < 2k-1$ においても情報理論的安全性をもつ秘匿計算法（TUS 方式）を提案してきた．その中で最新の成果では

1. 秘匿計算結果に 0 を含まない，
2. 各サーバが復元する乱数は固定される，
3. 攻撃者が知らない乱数とそれを構成する乱数の分散値を各サーバが持つ，

の条件のうち，1 と 2 を解決し，3 を TTP によって実現する方式となっている．一方で，この TUS 方式を含めた TTP や信頼できるサーバを含む既存の秘密分散法による秘匿計算の研究において，秘匿計算から通信を排除したり，サーバ台数を削減したりすることを目的とした秘密分散の議論をされていない．

本論文では，TTP を最大限に活用して，n を分散数とし N をサーバ数とした場合，$N < k$ においても実行できる秘密分散法による秘匿計算法を提案する．提案方式は秘密情報を乱数で暗号化して秘密分散による秘匿計算を行うため，鍵に当たる乱数が安全に管理されていれば，サーバが保持する情報が全て漏洩しても秘密情報は漏洩しない．また，提案方式は最小 1 台のサーバで秘密分散による秘匿計算を実行できる．これにより，サーバ間の通信は不要となるため，秘密分散法による秘匿計算において問題となるサーバ間通信による遅延が発生せず，非常に高速な秘匿計算を実現することができる．また，同一機関がサーバを管理できるようになる．

* 東京理科大学大学院工学研究科電気工学専攻，
〒 125–8585 東京都葛飾区新宿 6–3–1.
Dept. of Electrical Engineering, Graduate School of Engineering, Tokyo university of Science, 6–3–1 Niijuku, Katsushika-ku, Tokyo, 125–8585, Japan.
iwamura@ee.kagu.tus.ac.jp
† 広島市立大学大学院情報科学研究科情報工学専攻，
〒 731–3194 広島県広島市安佐南区大塚東 3–4–1.
Dept. of Computer and Network Engineering, Graduate School of Information Sciences, Hiroshima City University, 3–4–1 Ozuka-Higashi, Asaminami-ku, Hiroshima, 731–3194, Japan.