ブロックチェーンを利用した電力取引情報のプライバシーを保護する手法の提案

ZHUOWEI DENG[1,a)]　金子 晃介[2,b)]　櫻井 幸一[1,c)]

概要：バーチャルパワープラント (VPP) による電力配信の仕組みにブロックチェーン技術を基盤としたスマートコントラクトを導入することで，生成した電力と仮想通貨の当事者間での取引が実現できるようになる．しかしながら，ブロックチェーンに保存されたデータはユーザーの誰にでも閲覧可能であり，電力取引に関する情報が悪用される懸念がある．ユーザーのプライバシーを保護するための方法として，ブロックチェーンにデータのメタデータなどを保存し，実際のデータは秘密鍵を利用して暗号化した上で別のデータベースに保存する方法が提案されている．この方法では，ユーザーのデータを閲覧したい場合は，当該ユーザーに許可を得て公開鍵を受け取り，データベース内の当該ユーザーのデータを復号する．しかしながら，この手法では，電力取引の内容を分析したい研究者などは，データの分析にあたり，各ユーザーから公開鍵の受け渡しの許可を得るなどの複雑の認証手順を踏まなくてはいけない．そこで本論文では，ブロックチェーン技術においてプライバシーを保護し，且つデータ分析にあたる認証手順を解消するために，秘密分散法を基盤とした秘密計算を導入する．本手法は，ユーザーが電力の取引情報を自己管理できる且つユーザーからの認証手順を必要とせずに，研究者がユーザーの情報を暗号化したままで分析可能になる VPP システムを提案する．

キーワード：バーチャルパワープラント，ブロックチェーン，仮想通貨，プライバシー，秘密分散法，秘密計算

Proposal of Privacy Protection of Electricity Transactions Information on Blockchain

ZHUOWEI DENG[1,a)]　KOSUKE KANEKO[2,b)]　KOUICHI SAKURAI[1,c)]

Abstract: By implementing smart contract based on blockchain technology into a power distribution mechanism of Virtual Power Plant (VPP), users can generate electricity by themselves and use cryptocurrency to trade on electricity. Since data saved in blockchain can be read by all users, private information is possible to be used in malicious ways. Therefore, in order to protect privacy of users from malicious users, a method of writing metadata, etc. into blockchain and saving original data encrypted by secret key into a new database has been proposed. In this approach, anyone who wants to read the data has to ask for permission from users and get the public key to decrypt the data. However, researchers who want to analyze the transaction data need to get certification which may lead to complicated procedures. In this paper, to protect the privacy in blockchain and cancel the certification in data analyses, secure multiparty computation based on secret sharing will be implemented. By means of that, we will propose a VPP system that users can manage their own information and researchers can analyze data without decryption.

Keywords: virtual power plant, blockchain, cryptocurrency, privacy, secret sharing, secure multiparty computation

1. はじめに

現代社会において，あらゆる分野でデジタル化が急激に進んでおり，様々な先端テクノロジーが人々の日常生活を次の段階へ運ぼうとしている．その中でも，近年大きな発展を遂げている技術は，2008 年にサトシ・ナカモトが提出した仮想通貨ビットコイン [1] によって生まれた分散型台帳，ブロックチェーン [2] である．

ブロックチェーンの特性である改竄耐性により，書き込まれたデータを改竄することがほぼ不可能になる．また，分散型特性により，中央集権機関の手を借りずに各ブロックの管理を行うことができる．

そこで，分散型システムがもたらすメリットを日常生活に実現したいと考えた我々は，従来の中央集権管理の電力システムに存在する改善の可能性に気づき，ブロックチェーン技術をスマートシティの電力システム，いわゆるバーチャルパワープラント [3] に応用できるかどうかについて検討を始めた．ブロックチェーンの特性を活かせれば，エリアごとに各家庭は自分で電力を生成し，仮想通貨を通して電力の取引や交換などを行うことが可能であると考えられる．

しかしながら，ブロックチェーンによる分散型システムには，問題点が生じる．なぜなら，ブロックチェーンに保存される内容は登録されたユーザーの誰にでも閲覧可能であるため，その情報が悪用される懸念が存在している．ユーザーのプライバシーを保護するための方法として，一つはゲートウェイを用いてブロックチェーンに保存された情報へのアクセスを管理すること [4]．もう一つとしては，ブロックチェーンにデータのメタデータなどだけを保存し，実際のデータは秘密鍵を利用して暗号化した上で別のデータベースに保存する手法が提案されている [5]．[5] の手法では，ユーザーのデータを閲覧したい場合は，当該ユーザーに許可を得て公開鍵を受け取り，データベース内の当該ユーザーのデータを復号する手順になる．しかし，この手法では，電力取引の内容を分析したい研究者などは，データの分析にあたり，各ユーザーから公開鍵の受け渡しの許可を得るなどの複雑の認証手順を踏まなくてはいけない．そこで我々は，ブロックチェーン技術においてプライバシーを保護し，且つデータ分析にあたる認証手順を解消するため，秘密分散法を基盤とした秘密計算を導入する．本論文では，ユーザーが電力の取引情報を自己管理できる且つユーザーからの認証手順を必要とせずに，研究者がユーザーの情報を暗号化したままで分析可能になる VPP システムを提案する．

[1] 九州大学 大学院システム情報科学府
Department of Informatics Graduate School of Information and Electrical Engineering, Kyushu University
[2] 九州大学 サイバーセキュリティセンター
Cybersecurity Center,Kyushu University
[a)] deng.zhuowei.984@s.kyushu-u.ac.jp
[b)] kaneko.kosuke.437@m.kyushu-u.ac.jp
[c)] sakurai@inf.kyushu-u.ac.jp

2. 関連研究

2.1 分散型システム

従来の電力システムは，中央集権管理で，人々が信頼できる電力会社と電力使用の契約を行い，使用した電力に対し，相応の金額を払う仕組みである．しかし今後は，スマートシティの発展と共に，あらゆるものが分散型で自己管理になる傾向があると見られる．

分散型管理システムを実現できれば得られるメリットとしては，いくつかある [6]．一つとしては，システムが分散しているため，一台一台にかける負担が少なくなる．その上，たとえ部分的に故障しても，全体に及ぼす影響が少ない．従来の中央集権管理システムと比較すれば，需要に応じて個々の端末から変えられるので，その柔軟性は明らかに高くなる．中央コンピューターに比べれば，個々の端末に必要な費用も低い．

2.2 バーチャルパワープラント

分散型管理を組み込む電力システムは，バーチャルパワープラント (VPP) と呼ばれている．バーチャルパワープラントは，環境の需給バランスをコントロールするため，大規模発電所の代わりに，数多くの小規模発電設備を情報理論で管理し，一つの発電所のように機能されることを示している [6].

2.2.1 アドバンテージ

そのようなシステムが持ち合わせるアドバンテージは，主に四つがある [6][7].

1）利便性
2）需給バランス
3）再生エネルギーの導入
4）電力需要の負荷標準化
5）電力損失の最小化

「利便性」においては，ユーザーは自分で電力を生成し，使用することにより，自家の消費量と合わせて調整することができる．「需給バランス」には，各地域には消費する電力量はそれぞれ異なるので，中央型電力システムは常にそれに合わせて需給バンラスを保たなければならないと同時に，施設を運行管理するコストも少なくない．VPP による新たなシステムがあらゆる要素に応じて各自自分のエリアに需給バランスを取ることが可能になる．「再生エネルギーの導入」に関して，現在世界各地でもエネルギーがますます必要とされている．生成不安定な自然エネルギーを集めて，余る量を持つユーザーと足りないと感じるユーザーの取引によって再生エネルギーを活用できると考えられる．「電力需要の負荷標準化」は，電力使用量がピークになる時期に，供給を保てるために常にピークの使用量に

達する負荷を負わなければならないが，ピークではない時期にコストの上昇と稼働率の低下が問題になっている背景で，VPP システムであればその負荷を調整することができると考えられる．「電力損失の最小化」は，電力伝送距離が比較的に長い中央管理機関がその過程でより多くのエネルギーを損失しやすい現状に対して、エリアごとに動作する小規模発電設備の方がその損失を最小化することが可能だと示している．

2.3 データレイクを利用したプライバシー保護

バーチャルパワープラント (VPP) にブロックチェーンを応用したいとすれば，上文で紹介したように，ブロックチェーンに保存されるデータは登録されたユーザーの誰にでも閲覧可能であるため，その情報が悪用される恐れがある．ユーザーのプライバシーを保護するため，更なる手法を講じなければならない．そこで，Linn ら [5] がデータレイクという別のデータベースを応用する手法を提案した．

データレイクは元々ヘルスケア領域で提案された手法である．ブロックチェーンを用いて，ヘルスケアデータを保存することで，最新の医療情報を効率的に共有することができるが，上記の理由から，元々敏感である医療情報が悪用される可能性がある．情報を提供してくれるユーザーに対して，プライバシーの侵害になりかねない．

Linn らは，ヘルスケアデータそのものをデータレイクに保存し，ブロックチェーンにデータのメタデータなどだけを書き込む方法を考えた．

ユーザー自身で個人データの管理を行うべきという思想を基に，ユーザーは各自公開鍵認証を持ち，自分のデータに対し，秘密鍵を用いて暗号化し，デジタル署名を加えてデータをブロックチェーンとデータレイクの 2 つの場所に保存する．それぞれとしては，ブロックチェーンで各ブロックに保存されるデータは，データレイクの中にある一人のユーザーの全てのヘルスケアデータのカタログになる．一方，データそのものはデータレイクという別のデータベースに保存される．この全体を一つの図書館に例えるとすれば，一冊一冊の本には各のユーザーの全データが書かれていて，本の目次は各ブロックに記録されている．

2.3.1 トランザクション

さらに，各ブロックにあるトランザクションは，下記の五つの情報が含まれている．

1）ユーザーに対する識別子
2）ヘルスケアデータへのリンク
3）トランザクションが生成された時間
4）データのタイプ
5）メタデータ

「ユーザーに対する識別子」は，ユーザーが本人だと認証する手段である．「ヘルスケアデータへのリンク」は，暗号化された状態で，これを復号化したら得たリンクの先にはユーザーがアクセスしたいデータがある．「トランザクションが生成された時間」は，いつ頃の情報によってデータの参考価値にも影響が出ると考えられる．そして，「データのタイプ」と「メタデータ」も含まれている．この二つは，データへのアクセスにさらなる利便性を提供するタッグとして活用できる．

以上をベースに，ユーザー自身でデータのアクセスを管理することができる．ユーザー自身は全てのデータをアクセスすることができると共に，他のユーザーに書き及び読みの権限を与えることと，それを排除することもできる．当然、これまでのアクセス歴を閲覧することが可能である．

2.3.2 アドバンテージ

この手法において，ブロックチェーンを用いるアドバンテージは主に三つある．1 つ目は，ユーザー自身の管理により，ユーザーのプライバシーが保護される．2 つ目は，普通のデータベースより，ブロックチェーンは様々な分野からのユーザーに対し，簡単に情報を共有する環境を提供できる．世界範囲から情報を集めると，情報の一般性も保障される．3 つ目は，ブロックチェーンがもたらす分散型管理によって，システムが部分的に故障しても，全体に及ぼす影響も大きくならない．そのため，システム全体が長く持続できる．

2.3.3 問題点

しかしながら，Linn らの手法は，データを全てデータレイクに保存しているため，データレイクのセキュリティやプライバシーに対する保護を強化する必要がある．また，電力取引情報を分析したい研究者にとって，鍵の受け渡しの許可を得るためには，複雑な手続きを踏まなくてはいけない．そこで，我々は秘密分散法を基盤とした秘密計算をデータレイクに加えようと考えた．

3. 秘密計算と秘密分散法

3.1 秘密計算

従来，データの安全性を保障するため，データを暗号化することにより，秘密が守られる．また，暗号化されたデータに対し，分析や計算したいとなれば，その暗号文を一度復号化しなければならない．しかし，その復号化の過程で，データが平文になり，悪意を持つ人に秘密を漏洩する可能性が高くなる．そこで，秘密計算という概念が現れ，データを暗号化されたままの状態で計算できる仕組みを実現した．

その秘密計算の中にも，大きく三つのタイプ [8] に分かれている．

3.1.1 準同型暗号

準同型暗号とは，準同型性を有する暗号方式である [9]．つまり，暗号文状態のままで平文の加算や乗算をできるようになる．

鍵生成関数はペアーとなる公開鍵 pk と秘密鍵 sk を生成

する．Enc は暗号化アルゴリズムで，Dec は復号化アルゴリズムと仮定し，平文の a と b を暗号化アルゴリズムで暗号化し，$Enc(a)$ と $Enc(b)$ を得る．

そこで，もし $a+b$ を計算したいとすれば，今までのように $Enc(a)$ と $Enc(b)$ を復号化する必要がなくなる．暗号文 $Enc(a)$ と $Enc(b)$ を加算し，復号化してから $a+b$ の答えが得られる (1)．

$$Dec(Enc(a)+Enc(b))=a+b \tag{1}$$

3.1.2 Garbled Circuit

Garbled Circuit とは，第三者の介入を入らずに，二人のユーザーはお互いの入力，x と y を知らずとも，共同で $f(x,y)$ を計算できるような暗号化プロトコルのことである．

Gkikas[10] が紹介した Yao[11] が提案したアルゴリズムについて，論理回路 OR ゲートを例として説明する．OR ゲートには，二つの入力ワイヤと一つの出力ワイヤがある．それぞれ x，y と z を命名する．

それをベースに，ユーザー A が各ワイヤに対し，それぞれ 0 と 1 に関連している二つのランダム値を生成する．x にとっては k_x^0 と k_x^1 が生成され，y と z には同じ原理で生成される．

生成された k_x^0，k_x^1，k_y^0，k_y^1，k_z^0，k_z^1 を暗号化するための鍵と見なし，k_z^0，k_z^1 を入力ワイヤの鍵を持って暗号化し，Garbled Computation Table(GCT)[10] を作成する．

ユーザー B はユーザー A にもらった鍵で GCT の一部の情報だけを復元することができ，その結果を再び A に送り返す．

以上をベースに、関数 f で秘密計算を行う際，論理回路を関数 f のように立ち上げば良い．サーバ側 (B) は元のデータ x を知らずに $f(x)$ を計算することができ，またその結果をプロキシ側 (A) に送る．

3.1.3 秘密分散

秘密分散とは，データをいくつかの断片に分散し，アルゴリズムによって決められた断片を揃わない限り，データを復元することができない仕組みのことである．また，その断片はシェアと呼ばれている [8]．

その原理は多項式の演算に基づいている．$k-1$ 次の多項式には，閾値 k 組の値が対応して確定できれば，多項式を決定することができる．例として，一次関数 $(k-1=1)$ の方程式 $y=ax+b$ の中に，a と b の数値を決めたいとなれば，少なくとも二つの座標 $(x1,y1)$，$(x2,y2)$ が必要になる．

言い換えれば，$k-1$ 次の多項式には，k 組の値が持ち合わせないとなれば，その正体を見分けすることができない．同様，秘密情報に Shamir[12] に提案された (k,n) 閾値秘密分散法を用いると，データは $n(n>k)$ 部分のシェアに分かれ，少なくとも k 個のシェアを集めないと秘密情報の復元ができなくなる．

その秘密分散を基盤とした秘密計算は，以下のような過程で示す [8]．

（1）ユーザーは自分のデータ x を分散し，各サーバ S_i にシェアの x_i を送る．

（2）秘密計算に用いる関数 f を全てのサーバに送る．

（3）各サーバ S_i はそれぞれのシェアを基に，関数 f を用いて計算し，$f(x_i)$ を得られる．

（4）各サーバ S_i は計算結果 $f(x_i)$ を集結する，

（5）集結された $f(x_i)$ から $f(x)$ を復元する．

3.2 秘密分散法

上文に紹介したように，我々はデータベースに対する保護を強化したい上に，研究者にとって複雑な手順を踏まずに分析を行える環境を構築したいため，秘密計算を応用することになった．しかしながら，秘密計算の三つのタイプの中，準同型暗号 [13] と Garbled Circuit には鍵による復号作業が存在し，我々の考えと一致しないため，応用することが難しいと見られる．

従って，セキュリティとプライバシーを保護しつつ，且つ鍵の受け渡し手順が不要な秘密分散法は適切だと考え至った．

4. VPP システムの提案

本論文では，同じエリアに所属するユーザー同士が生成した電力を基に，当事者間での仮想通貨による取引などを行うことができる VPP システムを提案する．ユーザーが VPP システムで電力取引を行えるため，自身や家族に関する情報を登録しなければならない．ブロックチェーンにそのような情報を書き込むには，システム上の全てのユーザーに情報を見られることになり，プライバシーの懸念が存在しかねない．以下は，提案する VPP システムにおける電力取引の手順，システムに存在する情報またその情報に対する保護策について説明する．

4.1 電力取引の手順

提案する VPP システムにおいて，同じエリアに在住するユーザーを対象に一つのブロックチェーンネットワークを構築する．各ユーザーは電力の提供側と需要側のどちらの一方，またはその両方になれる．同エリアで，ユーザーはブロックチェーンに書き込まれた情報を基に，電力の取引先を探すことができる．合意が達成した後に取引が成立することになる．

4.2 VPP に保存される情報

ユーザーは取引を行うため，または電力の使用にあたり，どのような情報を登録するべきか，どのような情報が保存されるか，以下のように示す．

1）ユーザー本名
2）具体的な住所
3）電話番号またはメールアドレスのような連絡先
4）リアルタイムで提供している電力価格と電力容量
5）使われていた電力量またはその時間帯

「ユーザー本名」に関して，実際の電力取引を行う際に，実名化する必要があると考えられる．仮想通貨で想定されている取引とはいえ，実際の金銭問題や責任問題などのトラブルが発生した時に，実名化されてないと問題が深刻になりかねない．

「具体的な住所」には，ユーザー同士実名を了承したとしても，果たしてこのユーザーは実在しているかどうかは，まだ曖昧な部分が残っていて，それを疑問と抱いたユーザーのため，住所による確認は提供されるべきかと考えられる．

「電話番号またはメールアドレスによる連絡先」について，取引がスムーズに進行されるための手段である．住所が登録されているとはいえ，取引をする度に尋ねるには需要側にとって不便であり，提供側にとっても望ましい手段だと言い難い．最初の一回だけ対面で相談できれば，次回以降の取引は連絡だけで済ませる．

「リアルタイムで提供している電力価格と電力容量」はユーザーが取引先を選択するため，必要不可欠な情報である．

「使われていた電力量またはその時間帯」はトランザクション情報の一部として自動的に記録されるものであり，また使用者自身がどのように電力を消費しているのかを知る手段である．

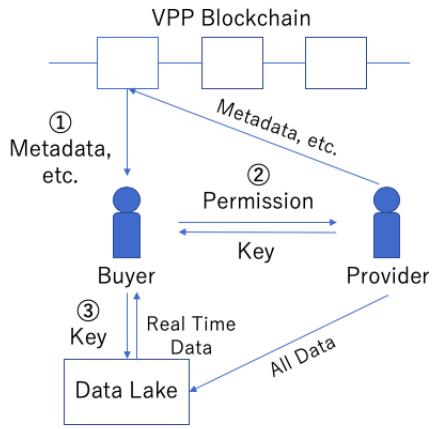

図 1　電力取引手順 (Linn らの手法を基に)

4.3　保護すべき VPP 情報

上文で紹介したように，VPP システムに直接ブロックチェーンを応用すると，電力取引情報が悪用される懸念があり，ユーザー自身が危険に晒される可能性が存在している．

本名，住所または連絡先などの個人情報による危険性は当然であるが，使われている電力量とその時間帯によっては，ユーザーの 1 日のスケジュールが推定されることが可能で，それによってユーザーとその家族にはプライバシーが侵害されかねない上に，身の安全すら保証できなくなる．

そのような懸念を防ぐため，我々はデータレイク [5] による手法を VPP システムに応用すると考えた．これにより，以上で示した実際のデータは別のデータベースに移ることになり，ブロックチェーンに書き込まれるのはメタデータなどの情報だけで，以下のように示す．

1）ユーザー id
2）所在エリア
3）メールアドレス
4）平均的な電力容量と価格

図 1 で，ユーザー (Buyer) は最初にこのような情報を目にし，取引を申し込みたいとなれば，メールアドレスで電力提供側 (Provider) に連絡し，対面で許可を得て，もらった鍵を使い，データベースに保存された暗号化された情報を復号化し，リアルタイム的な情報を基に取引を行うことができる．

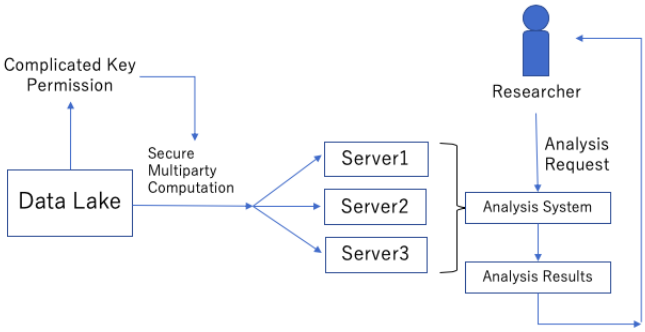

図 2　VPP 上の秘密計算

4.4　VPP 上の秘密計算

しかし，上記手法において，情報を閲覧するため，ユーザー本人から許可を貰わなければならない．電力消費などの情報を分析に用いたいと考えてる研究者にとって，鍵の受け渡しなどの手順を踏まなくてはいけない．データ分析にさらなる利便性を提供しつつ，データ自体を秘密として保護したいと思い，暗号化したままで演算可能で且つ鍵の受け渡しを必要としない秘密分散法を基盤とした秘密計算をデータレイクに応用すると考えた．

秘密分散法により，実際のデータはいくつかのサーバに分散され，充分の数のシェアを揃わないと復元できないようになっている．図 2 のように，研究者 (Researcher) たちはデータそのものを触れずに，システムに演算の項目を依頼すれば，サーバが自力で結果を出し，研究者たちに届く

	id	name	area	address	mail_ad	elect_amount_kwh	ect_price_yenperkv
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	mCvdH	C3	jrXusbdzmB, iHXIF	mCvdH@vpp.com	591	17
2	2	mvmN4	C2	jTuvGix6QT, ZI9...	mvmN4@vpp.com	629	21
3	3	dRmkj	C4	Z0qh14FXfw, 65...	dRmkj@vpp.com	806	61
4	4	tKrKe	C1	InyL2wbgk7, P6...	tKrKe@vpp.com	1033	19
5	5	DrzTJ	C5	c7dR6pMADy, ix...	DrzTJ@vpp.com	240	62
6	6	RmV9k	C6	6uOVJKC0uX, 3...	RmV9k@vpp.com	1389	97

図 3 VPP データベース (暗号化される以前)

仕組みも可能になる．

では，実際の VPP システムに応用すればどうなるのかについて，まず我々は Python 環境で SQLite のデータベースを作成し，ランダム関数を用いてユーザーの情報を生成した．我々はユーザー id，ユーザー本名，所在地域，家庭住所，メールアドレス，リアルタイムの電力容量または電力価格を仮定し，図 3 のように，暗号化または分散化される以前のデータベースを示す．

秘密分散による秘密計算を用いて，以上の情報は分散され，暗号化される．これにより，ユーザーのプライバシーが保護される．更にその中，分析に用いられる部分は電力容量や電力価格などだと考えられる．

以上を基に，例として，研究者は以下のような分析項目に注目する可能性がある．

1）エリアごとに，各時期における平均電力価格と平均電力容量

2）エリアごとに，各時期における電力需要と供給

3）システム全体の上記パラメーター

4）天気，気温などの様々な要素による電力価格や容量の変動

このような分析を行うことにより，研究者は VPP システムにおける各エリア今後の運営に，さらに的確なアドバイスを提供することができ，先の研究にも大量な分析可能なデータを蓄えることが可能になる．

また，研究者たちは鍵の受け渡しなどの手順を経由しせず，データ自体も触れていないとはいえ，データ所有者のユーザーたちにインセンティブを提供する必要があると考えられる．当システムとしては，データ利用の代わりに，電力取引に用いられる仮想通貨の分配が望ましい．

4.5 セキュリティ性

4.5.1 四則演算の組み合わせ

神宮ら [14] が提案した秘密分散による秘密計算の手法の中，s と a はそれぞれ秘密情報と乱数として扱われている．高速演算を実現するため，乗算では一時的秘密情報 as を復元することになる．また，加算により，a が一時的に知られることが可能である．加算と乗算の組み合わせ計算になれば，秘密情報が漏洩される懸念が存在している．そのため，常に a などの乱数を新しく生成して秘密分散情報を更新しなければならなくなる．既に負担が高い演算機能を負っている以上，高速演算の代わりに更新作業が増えることが全体的にプラスとは言い難い．

4.5.2 大量演算

上記は高速演算を実現するため，解決しなければならない問題点ではあるが，他の演算手法においても，実は似たような危険性が秘めていると考えられる．なぜなら，秘密計算が実装された以上，日々大量な演算が行われることになり，その大量の演算結果を集中すれば，元のデータを逆算できる可能性も存在しかねない．簡単な例として，次の二つの演算が行われるようでしたら：

$$x + y = a \tag{2}$$

$$2x + y = b \tag{3}$$

得た結果 a と b だけを基に，x をわかるようになる恐れがある．実際の演算ではそのように簡単に暴かれることがないと考えられるが，大量な演算結果が積み重ねば危険性もまた増していく．

それは秘密計算の全体において解決すべき問題点であり，本提案においても，今後さらなる検討が必要である．

5. まとめ

ブロックチェーン技術を基盤としたバーチャルパワープラント (VPP) システムは，ブロックチェーンの分散型特性などにより，ユーザーの自己管理を実現しようとしている．本論文では，それをベースに，秘密分散による秘密計算を応用してプライバシーを保護し且つデータ分析に利便性を提供できる手法を提案し，セキュリティに潜む問題点について分析した．

参考文献

[1] Nakamoto, Satoshi.: *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf(2008).

[2] Archana Prashanth Joshi, Meng Han, Yan Wang.: *A survey on security and privacy issues of blockchain technology*, Mathematical Foundations of Computing, 1(2): 121-147(2018).
[3] Jonas Schlund, Lorenz Ammon, Reinhard German.: *ETHome: Open-source blockchain based energy community controller*, In e-Energy ' 18: International Conference on Future Energy Systems, June 12–15, 2018, Karl- sruhe, Germany. ACM, New York, NY, USA, 5 pages.(2018).
[4] Yue Xiao, Wang Huiju, Jin Dawei, Li Mingqiang, Jiang Wei.: *Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control*, Journal of medical systems. 40. 218. 10.1007/s10916-016-0574-6.(2016).
[5] L. A. Linn and M. B. Koo.: *Blockchain for health data and its potential use in health IT and health care related research*, ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST(2016).
[6] 楽エネ：VPP（バーチャルパワープラント）とは？新たなエネルギー資源を，入手先 ⟨https://rakuene-shop.jp/columns/3509-2/⟩ (2019.11.19).
[7] Jordan Murkin, Ruzanna Chitchyan, Alastair Byrne.: *Enabling peer-to-peer electricity trading*, 4th International Conference on ICT for Sustainability(2016).
[8] Kikuchi Ryo, Ikarashi Dai.: *Progress of Secure Computation: Basic Constructions and Dedicated Algorithms*, Fundamentals Review Vol.12 No.1 pp.12-20(2018).
[9] フリー百科事典『ウィキペディア』: 準同型暗号，入手先 ⟨https://ja.wikipedia.org/wiki/準同型暗号⟩(2019.05.08).
[10] Konstantinos Gkikas: Yao's Garbled Circuit, 入手先 ⟨https://homepages.cwi.nl/ schaffne/courses/crypto/2014/presentations/Kostis_Yao.pdf⟩ (2014.10.23).
[11] A. C. Yao.: *Protocols for Secure Computation*, Comm. ACM, Vol. 22, No.11, pp.612-613(1979).
[12] Shamir, A.: *How to share a secret*, In Proceedings of the 23rd IEEE Symposium on the Foundations of Computer Science, pages 160-164(1982).
[13] 林卓也: 準同型暗号を用いた秘密計算とその応用, システム/制御/情報, Vol.63, No.2, pp. 64-70(2019).
[14] 神宮武志，岩村恵市: 除算を含む四則演算に適用可能な秘密分散法を用いた秘匿計算手法の提案, IPSJ SIG Technical Report Vol.2015-CSEC-70 No.8 Vol.2015-SPT-14 No.8(2015).