準同型暗号を用いてプライバシ保護を可能としたスマートグリッドの電力量削減プロトコルの提案

川嶋 遼祐 †　　稲葉 宏幸 †

† 京都工芸繊維大学 大学院工芸科学研究科
606-8585 京都府京都市左京区松ケ崎橋上町 1
kawashima08@sec.is.kit.ac.jp, inaba@kit.ac.jp

あらまし スマートグリッドで定期的に蓄積される電力利用情報には，需要家のプライバシ情報が含まれているため，暗号化技術等により保護する必要がある．その際，電力制御や課金サービスを行うために，加算が必要であるので，加法性準同型暗号を用いて保護を行う手法が考えられている．スマートグリッドでは，ひっ迫状況時には需要家の電気機器を制御し，事前に決められた分だけ電力を抑制できるが，これだけではこの状況を脱せない可能性がある．本論文では，ひっ迫状況時に需要家側に一定割合の削減目標を提示し，削減要請を行う電力量削減プロトコルを提案する．また，供給側は削減目標を達成した需要家に対してサービスを行うため，加法性準同型暗号の性質を用いて暗号化したデータ間での比較を行う．

A Proposal on Electricity Reducing Protocol with Privacy Protection for Smart Grid Using Homomorphic Encryption

Ryousuke Kawashima†　　Hiroyuki Inaba†

†Kyoto Institute of Technology
1 Hashigami-cho, Matsugasaki, Sakyo-ku, Kyoto-shi, Kyoto 606-8585,JAPAN
kawashima08@sec.is.kit.ac.jp, inaba@kit.ac.jp

Abstract The periodical electricity usage information measured by a smart meter is necessary to be protected by encryption technology because it contains customer privacy. So it is thought out a privacy protection scheme using additive homomorphic encryption. In the smart grid, when the electricity consumption is too high, it is repressed by controlling customer appliances in advance decided range. However, in case the electricity supply cannot catch up with the consumption, additional reducing method is required. In this paper, we propose the electricity reducing protocol, which is reduced by presenting the fixed reducing rate. And the supplier serves for the customers if they achieve the rate. In order to realize the protocol, they need to compare the encrypted data using homomorphic encryption property.

1　はじめに

現在，資源の有効利用や省エネルギー促進の観点から，次世代電力網としてスマートグリッドが注目されている．スマートグリッドでは，電力需要家の電力利用情報は，通信機能を有する電力計であるスマートメータによって計測される．計測された情報はネットワークを介して，メータ

データ管理システム (Meter Data Management System:MDMS) に送信され，そこに蓄積される．蓄積された情報は電力制御や課金などに用いられるが，その情報には需要家のプライバシ情報が含まれている．このため，MDMS に蓄積される電力利用情報は保護する必要がある．また，電力制御や需要家への課金サービスのために電力使用量の合計を計算する必要がある．このため，先行研究 [1] においては，準同型暗号を用いることで電力利用情報の保護を行い，かつ暗号化した状態での加算を可能にしている．

また，スマートグリッドでは，エネルギー管理システム (Energy Management System:EMS) における電力系統の制御や，家庭や企業の電気機器の需要応答対応が行われている．需要応答対応は供給側において電力がひっ迫した際に，需要家側の不要不急の電気機器を制御することで，一時的に電力を一定の範囲内で抑制している．しかし，EMS における電力抑制のみでひっ迫状況を抜け出せない場合が考えられる．

本論文では，需要家側と協力することで，電力量削減を目指す電力量削減プロトコルを提案する．電力ひっ迫の際には，需要家側に一定割合の削減目標を提示して，電力量削減を行うように要請する．削減目標を達成した需要家は供給側から電気料金値下げなどのサービスが受けられる．したがって，ひっ迫状況から脱すると，各需要家に対して，提示した削減目標を達成したかどうかを確認する．確認はひっ迫状況に陥った際の電力とひっ迫状況から脱した際の電力とを比較することで行う．電力利用情報は暗号化されているため，暗号化した状態での比較が望ましい．そこで，本論文では準同型暗号を用いることで，暗号化した状態での比較を可能としたプロトコルの提案を行う．

2　スマートグリッド

2.1　スマートグリッドとその構成

スマートグリッドとは，既存の電力網の監視制御や計測に情報通信技術を用いる次世代電力網である．スマートグリッドでは，電力需要家の電力利用情報は通信機能を持つ電力計であるスマートメータによって計測される．また，スマートグリッドは「IT による電力系統側の需給バランス調整」と「需要端部分の IT 化」による需要応答への対応や，太陽光発電などの再生可能エネルギーの利用促進などによって実現されると考えられている [1].

「IT による電力系統側の需給バランス調整」は系統側の電力周波数制御を行う EMS で実現される．また，需要家のスマートメータからの電力利用情報を一元管理している MDMS が存在する．これに蓄積されたデータをもとに EMS は電力制御を行う．電力需給がひっ迫した際には，EMS を用いて需要家側の不要不急の電気機器を一時的に抑制している．また，電力をどれだけ抑制するかは事前の契約により決定している．このように，電力網の制御や最適化を行うことで，省エネルギーやコスト削減を目指している．

一方,「需要端部分の IT 化」は次世代メータリンク基盤 (Advanced Metering Infrastructure：AMI) という基盤で実現される．AMI は EMS, MDMS とスマートメータなどが連携し，各需要家の電力利用情報の集計や需要応答対応などが実現される．MDMS では各スマートメータから一定時間ごとに電力利用情報の集計を行い蓄積している．その情報を EMS や課金サービスに提供することにより，電力制御や電力料金の請求を行うと考えられている．

2.2　プライバシの問題

スマートグリッド化以前における電力利用情報では一ヶ月単位で計測や料金請求が行われていたため，より細分化した電力利用情報を知ることはできない．一方，スマートグリッド化が行われた場合，需要家の電力利用情報はスマートメータでリアルタイムに計測し，一定時間ごとに MDMS に蓄積される．このため，MDMS は各需要家の時間ごとの電力利用情報を詳細に把握することが可能である．時間ごとの電力利用情報には，生活習慣や使用機器を推測できる情報が含まれている．これは需要家のプライバシの侵害を招く恐れがある．

EFF(Electronic Frontier Foundation)[2] は，スマートメータは重大なプライバシ侵害を招くという見解を示している．また，日本の経済産業省における報告書 [3] においても「スマートメータから提供される電力等使用情報は，個人の生活習慣情報等が含まれた個人情報に該当する」と指摘されている．

このことから，MDMS に蓄積される電力利用情報にはデータのアクセス制御や暗号化などの保護が必要であるといえる．

3 準同型暗号を用いた従来手法

3.1 準同型暗号の概念

準同型暗号とは，暗号文同士を演算することにより，異なる平文に対応する暗号文が計算できる性質を持つ暗号である．具体的には，平文 m_1, m_2 において，式 (1) のような性質を満たす暗号を指す．

$$E(m_1) \star E(m_2) = E(m_1 \circ m_2) \tag{1}$$

ここで，関数 $E(\cdot)$ は暗号化関数である．式 (1) における $\star$ や $\circ$ には $+$ や $\times$ のような二項演算子を用いる．また，式 (1) の右辺における $\circ$ が $+$ であるとき，その暗号は加法準同型性を有するという．同様に，$\circ$ が $\times$ であるとき，乗法準同型性を有するという．

3.2 Paillier 暗号

Paillier 暗号とは，1999 年に P. Paillier が考案した加法準同型性を有する公開鍵暗号である [4]．最初に，鍵の生成方法を記す．二つの大きい素数 p, q を生成し，その積を n とする．また，$p-1, q-1$ の最小公倍数を λ，法 n^2 において位数が $n\alpha$ となるような値を g とする．ここで，$\alpha = 1, 2, \cdots, \lambda$ である．公開鍵として (n, g)，秘密鍵として (p, q, λ) が選ばれる．また，n を安全な公開鍵とするには，生成する 2 つの素数のビット長を等しくし，かつビット長を 512bit 以上にする必要がある [5].

次に，暗号化手順を示す．最初に，n 未満の平文 m を選択する．次に，n 未満の乱数 r を生成する．これらを用いて，式 (2) により暗号化を行う．

$$c = g^m \cdot r^n (\mathrm{mod}\ n^2) \tag{2}$$

ここで，c は暗号文である．暗号化において，乱数 r が用いられているので同じ平文を暗号化しても異なる値の暗号文となる性質を持つ．

次に，復号化手順を示す．復号する n^2 未満の暗号文 c を式 (3) に代入することで復号を行う．

$$m = \frac{L(c^\lambda (\mathrm{mod}\ n^2))}{L(g^\lambda (\mathrm{mod}\ n^2))} (\mathrm{mod}\ n) \tag{3}$$

ここで，関数 L は式 (4) のように定義される．

$$L(u) = \frac{u-1}{n} \tag{4}$$

また，Paillier 暗号では，任意の平文 m_1, m_2 において，式 (5) が成り立つ．

$$D(E(m_1) \times E(m_2) (\mathrm{mod}\ n^2)) = m_1 + m_2 (\mathrm{mod}\ n) \tag{5}$$

ここで，関数 $D(\cdot)$ は復号化関数である．さらに，平文 m において，式 (6) が成り立つ．

$$D(E(m)^k (\mathrm{mod}\ n^2)) = km (\mathrm{mod}\ n) \tag{6}$$

ここで，$k \in \mathbb{N}$ である．

3.3 準同型暗号を用いた従来手法によるプライバシ保護

2.2 節において，MDMS に含まれる電力利用情報はデータのアクセス制御や暗号化などの保護をする必要があることを述べた．ここでは暗号化による保護方法について述べる．

EMS では電力制御を行っているため，MDMS において一定時間ごとに総電力使用量を計算する必要がある．また，課金サービスには需要家の一定期間の電力使用量の合計を送信する必要もある．しかし，適切でない暗号処理を行うと，合計計算を行うために MDMS 内に蓄積される各需要家の電力使用量を一度復号しなければならない．復号を行えば電力使用量が把握できてしまい，プライバシの保護を達成できない．

そこで加法準同型性を有する Paillier 暗号を用いることで，復号することなく総電力使用量に対応する暗号文を計算し，電力利用情報を保護する方法が提案されている [1]．これを以下に説明する．また、その概要を図 1 に示す．

1. 各需要家のスマートメータが公開鍵を用いて一定時間ごとに電力使用量を暗号化し，その後暗号化したデータを MDMS に送信する．
2. MDMS が各需要家から送られてきた暗号化されたデータを需要家ごとに蓄積する．
3. (a) MDMS が時間ごとの電力使用量を加法準同型性を利用して計算し，結果を EMS に送信する．
   (b) EMS が受信したデータの復号を行い，それに基づき電力制御を行う．
4. (a) MDMS が各需要家の一定期間の電力使用量の合計を加法準同型性を利用して計算し，結果を課金サーバに送信する．
   (b) 課金サーバが受信したデータの復号を行い，各需要家の電力使用量から請求金額を計算する．

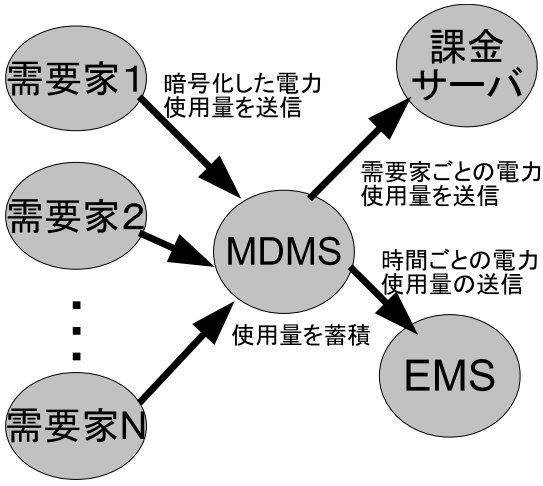

図 1: 準同型暗号を用いたプライバシ保護

MDMS に蓄積される各需要家の時間ごとの電力使用量は暗号化されているため，生活情報等のプライバシ情報を把握することはできない．また，EMS に送信されるデータを復号しても，各需要家の電力使用量を把握することはできない．同様に，課金サーバに送信されるデータを復号しても，需要家の時間ごとの電力使用量を知ることはできない．

このように，Paillier 暗号を用いることで需要家のプライバシ保護や EMS，課金サーバへ送るデータの合計計算を可能にしていることがわかる．

4 提案手法

4.1 電力量削減プロトコルの概要

EMS では，電力需給状況がひっ迫した際には，需要家の不要不急の電気機器を制御することで電力使用量を抑制するが，これだけではひっ迫状況を脱せない可能性が生ずる．そこで，そのような場合に適用できる電力量削減プロトコルを提案する．今回提案するプロトコルは電力ひっ迫時に需要家側と協力することで電力使用量を削減するものである．供給側は，需要家側に「x% 削減」のような一定割合の削減目標を提示して，電力削減を行うように要請する．また，需要家側はその提示された割合を達成できれば，電気料金値下げなどのサービスが受けられることになる．プロトコルの流れを以下に示す．また，その概要を図 2, 図 3 に示す。

1. 各需要家のスマートメータが公開鍵を用いて一定時間ごとに電力使用量を暗号化し，その後暗号化したデータを MDMS に送信する．
2. MDMS が各需要家から送られてきた暗号化されたデータを需要家ごとに蓄積する．
3. MDMS が時間ごとの電力使用量を加法準同型性を利用して計算し，結果を EMS に送信する．
4. EMS が受信したデータの復号を行い，それに基づき電力制御を行う．ここで，ひっ迫状況に陥った場合は 5 に移る．ひっ迫状況

を脱した場合は 7 に移る．ひっ迫状況でない場合はここで終了する．

5. EMS がひっ迫状況に陥ったことを MDMS に報告する．また，このときに $x\%$ 削減することを提示する．
6. MDMS が受けた報告内容と提示された削減目標を全需要家に対して伝える．その後，ひっ迫状況を脱するまで 1 から 6 を繰り返す．なお，提示された削減目標は 1 回目のみ伝える．
7. EMS がひっ迫状況を脱したことを MDMS に報告する．
8. 報告を受けた MDMS は各需要家のひっ迫状況に陥った時間の電力使用量とひっ迫状況を脱した時間の電力使用量との比較を行う．
9. MDMS は各需要家の暗号化された比較結果を課金サーバに送信する．
10. 課金サーバは送られてきた結果を復号し，どの需要家が提示された削減目標を達成したのかを確認する．削減目標を達成した需要家を記録しておき，その需要家に対して電気料金値下げなどのサービスが受けられるようにする．

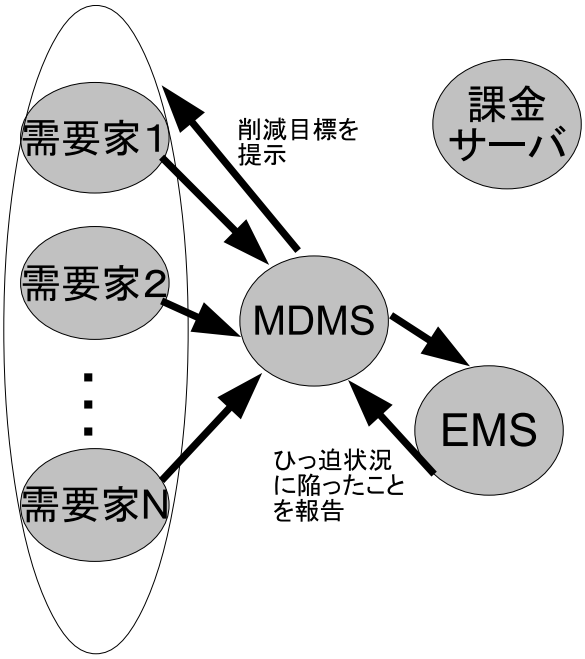

図 2: 電力量削減プロトコルの概要図 (1 から 6 まで)

このような流れで，電力量削減を行う．なお，8 における比較アルゴリズムの詳細は 4.2 節で述べる．

このプロトコルを用いることによりプライバシの保護をしつつ，電力量の削減が可能となることがわかる．

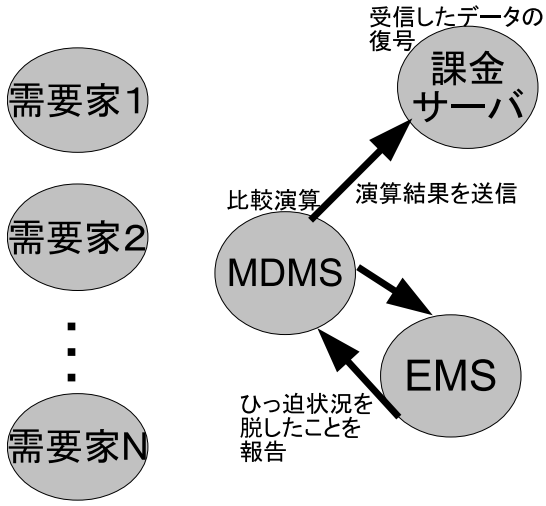

図 3: 電力量削減プロトコルの概要図 (7 から 10 まで)

4.2 比較アルゴリズム

4.2.1 比較アルゴリズムの内容

最初に，Paillier 暗号を用いた二つの値を比較するアルゴリズム [6] について記す．平文を m_1, m_2 とし，これらの値の範囲を $n/2$ 未満とする．また，各平文に対応する暗号文をそれぞ

れ c_1, c_2 とする．ここで，比較を行うため，式 (7) の計算を行う．

$$c = \frac{c_1}{c_2} (\mathrm{mod}\ n^2) \tag{7}$$

式 (5) より，暗号文同士の除算は平文において差を求めることになる．このことから，式 (7) は差 $m_1 - m_2$ に対応する暗号文を求めていることがわかる．

$m_1 \geq m_2$ の場合，差は正，または 0 となる．よって，差が 0 以上となった場合の判定基準は $D(c) < n/2$ となる．一方，$m_1 < m_2$ の場合，差は負となる．このとき，差の範囲は式 (8) のようになり，法 n においては式 (9) となる．

$$-\frac{n}{2} < \quad D(c) \quad < 0 \tag{8}$$

$$\frac{n}{2} < \quad D(c) \quad < n (\mathrm{mod}\ n) \tag{9}$$

法 n において，値が n 未満であることは自明であるので，差が負になった場合の判定基準は $D(c) > n/2$ となる．式 (10) に判定基準をまとめる．

$$\begin{cases} m_1 \geq m_2 \ (D(c) < \frac{n}{2}) \\ m_1 < m_2 \ (D(c) > \frac{n}{2}) \end{cases} \tag{10}$$

よって，式 (7) より c を求め，式 (10) を基に判定することで，元の暗号文を復号することなく，どちらの値が大きいかを知ることができる．

次に，提案プロトコルで用いる比較アルゴリズムについて記す．ひっ迫状況に陥った際の電力使用量（平文）を m_1，ひっ迫状況を脱した際の電力使用量（平文）を m_2 とする．また，各平文に対応する暗号文をそれぞれ c_1, c_2 とする．$x\%$ 削減 ($x \in \mathbb{N}$) の提示が行われるとすると，式 (11) の計算が行われることが望ましい．

$$c = \frac{{c_1}^{1-\frac{x}{100}}}{c_2} (\mathrm{mod}\ n^2) \tag{11}$$

式 (6) より，式 (11) におけるべき乗計算は平文における乗算となる．しかし，この計算では c_1 の指数部が整数にならないことがある．法計算ではべき乗数は整数でなければならないから，式 (11) の右辺を 100 乗することでべき乗数を整数に変換する．それを式 (12) に示す．

$$c' = \frac{{c_1}^{100-x}}{{c_2}^{100}} (\mathrm{mod}\ n^2) \tag{12}$$

つまり，式 (12) では m_1 を $100 - x$ 倍，m_2 を 100 倍して差をとることで，$x\%$ の削減が達成できたことを確認していることになる．また，式 (12) の判定方法は式 (10) と同様である．

一方，式 (12) で計算された結果は課金サーバで復号され，需要家がどれだけ削減を達成したかという差分情報が知られてしまう．そこで，乱数 R を生成し，式 (12) に対してべき乗計算を行うことで，差分情報を分からないようにする．それを式 (13) に示す。

$$C = \left(\frac{{c_1}^{100-x}}{{c_2}^{100}} \right)^R (\mathrm{mod}\ n^2) \tag{13}$$

ここで，式 (13) は平文においては式 (12) を復号して得られる結果を R 倍した結果と同等である．また，式 (13) の判定方法は式 (10) と同様である．

式 (12) においては c' を復号することにより「需要家がどれだけ削減したか」という情報を得られる可能性があった．一方，式 (13) においては C を復号しても，元の値を R 倍することで，そのような情報を得られないようにしている．したがって，式 (13) における C を計算することで，プライバシ情報を明かすことなく，需要家が削減目標を達成しているかどうかを知ることができると考えられる．

4.2.2 比較アルゴリズムで用いる値の選び方

最初に，乱数 R について記す．式 (13) において，平文は最大で $100R$ 倍される．比較に用いられる平文は $n/2$ 未満でなければならないため，$100R$ 倍された平文も $n/2$ 未満でなければならない．つまり，元の平文 m_1, m_2 は $mR < n/200$ の範囲を満たさなければならないことがわかる．

また，乱数 R は削減達成の結果が変わらないように範囲を決める必要がある．ここで，乱数 R の範囲を計算しやすくするために，電力の予想最大使用量を M と設定する．このとき，乱数 R は $R < n/200M$ の範囲を満たさなければ比較結果を変えてしまうことがわかる．したがって，乱数 R のビット長は式 (14) により表される．

$$size\ R = size\ n - size\ M - 8 \tag{14}$$

ここで，$size\ X$ とはその数値 X のビット長を指す．また，式 (14) における 8 は $size$ 200 を表している．

次に，公開鍵 n について記す．公開鍵 n は平文 m_1, m_2 や乱数 R が大きい値を取れるように十分大きくする必要がある．ここで，1 ヵ月の家庭における電力使用量について考える．例えば，平成 23 年度における京都市の 1 世帯当たりの電力使用量は年間で 5,350kWh[7] であることから，1 ヵ月当たりの平均はおよそ 446kWh となる．また，1 ヵ月当たりの電力使用量の最大は 592kWh である．スマートメータが MDMS に 1 時間ごとにデータを送信すると仮定すると，1 回あたりのデータの値は数百 W であると考えられる．すなわち，比較に用いられるデータは 10^3 程度の大きさであると考えられるので，公開鍵 n は 2×10^5 程度以上でなければならない．

一方，3.2 節で述べたように，Paillier 暗号の安全性のためには公開鍵 n を構成するための素数のビット長は 512bit 以上である必要がある．これは上述した電力データを扱うのに十分なサイズであることが分かる．

4.2.3 計算量

比較アルゴリズムの時間計算量，および空間計算量について記す．比較のため，暗号化や復号化における時間計算量，および空間計算量も含めて表 1 に示す．

表 1: 各演算における計算量

演算	時間計算量	空間計算量
比較	$O((size\ n)(size\ n^2)^2)$	$O(size\ n^2)$
暗号化	$O((size\ n)(size\ n^2)^2)$	$O(size\ n^2)$
復号化	$O((size\ \lambda)(size\ n^2)^2)$	$O(size\ n^2)$

表 1 より，比較アルゴリズムにおける時間計算量は暗号化における時間計算量と同等であることがわかる．また，空間計算量は他の二つの演算と同等であることがわかる．これより，比較アルゴリズムにおける計算時間と必要空間は暗号化と同じくらいの時間と空間を要すると見積もることができる．

5 むすび

本論文では，スマートグリッドにおけるプライバシ保護を行う従来手法を基に，需要家との協力でひっ迫状況を脱する電力量削減プロトコルを提案した．また，削減目標達成を確認するための比較アルゴリズムにおいても需要家のプライバシ情報を明かすことなく比較を行うことが可能であることを示せた．

また，MDMS は比較アルゴリズムにおいて求めた演算結果を課金サーバに送信し，そこで復号を行う．ここで，公開鍵 n のビット長が大きくなると計算量が大きくなる．また，需要家が多くなると，復号するデータ数が多くなるため，計算時間が長くなる．このことから，課金サーバに対する負荷が増加することが考えられる．今後，これらに関してさらに詳細な検討が必要である．

参考文献

[1] 山中晋爾，駒野雄一，伊藤聡，“準同型暗号を用いたスマートグリッドにおけるプライバシ保護方式の検討”，信学技報，vol.111, no.240，pp.7-12，Oct. 2011.

[2] New “Smart Meters” for Energy Use Put Privacy at Risk, EFF, https://www.eff.org/deeplinks/2010/03/new-smart-meters-energy-use-put-privacy-risk，2012/01/25 参照

[3] スマートメーター制度検討会報告書，経済産業省，http://www.meti.go.jp/committee/summary/0004668/report_001_01_00.pdf，2012/01/24 参照

[4] P.Pailler, “Public-key cryptosystems based on composite degree residuosity classes”, EUROCRYPT, pp.223-238, 1999.

[5] J.A.Buchmann, INTRODUCTION TO CRYPTOGRAPHY Second Edition, Springer，July 2004.

[6] D.C.Parkes, M.O.Rabin, S.M.Shieber, and C.Thorpe, “Practical secrecy-preserving, verifiably correct and trustworthy auctions”, Electronic Commerce Research and Applications, vol.7, no.3, pp.294-312, 2008.

[7] 【平成 23 年度】京都市内のご家庭における電気・都市ガス月間使用量（速報値）／京都市 環境政策局 地球温暖化対策室, 京都市情報館, http://www.city.kyoto.lg.jp/kankyo/page/0000121674.html, 2012/08/21 参照