7-7　長期利用可能暗号技術とプライバシー保護データマイニングへの応用

Le Trieu Phong　青野良範　林　卓也　王　立華

本稿では、セキュリティ基盤研究室が新たに開発した準同型暗号技術 “SPHERE” と、その応用例としてプライバシー保護型ロジスティック回帰分析システムを紹介する。SPHERE は暗号化データでの演算が可能であるだけでなく、暗号化データのセキュリティレベルを安全に更新できるというユニークな機能を持つ。遺伝子情報などのプライバシーを長期にわたり保護する必要がある情報でのデータマイニングへの応用が期待される。

1　まえがき

データマイニング技術の発達により、ビッグデータの解析に基づく様々なビジネスが新たに展開されている。データの中にはプライバシーに関わる情報が含まれることがあり、プライバシーを保護した状態でのデータ解析が必要となっている。その一手法として「準同型暗号」の利用がある。準同型暗号ではデータを暗号化したまま様々な演算が行えるため、暗号化データで統計処理を行い、復号鍵を持つものだけがその統計結果を得られるといった、プライバシーを考慮した統計処理システムの構築が可能となる。

ゲノムワイド関連解析に代表される、疾患データや遺伝子情報を扱うデータ解析においては、それらが漏洩した際に本人だけでなく親戚・子孫にまで影響が及ぶ可能性があるため、通常のデータ以上に長い期間安全に保つ必要がある。一方、計算機の進化や暗号解読技術の発展に伴い、暗号の解読能力も年々向上していくため、暗号化データは時間とともに安全性が損なわれてしまう。暗号の安全性は、計算機や解読技術の進化を予測に入れながら見積もられているが、その未来予測の難しさなどから、高々数十年程度先までしか安全性を保証することができない。更に長期にわたって安全に利用するためには、例えば、復号してからより高いセキュリティレベルの暗号方式で再び暗号化する、といった一時的に漏洩リスクが高まるなどの問題がある方法を取らざるを得なかった。

これらの事柄を背景に我々は、新たな準同型暗号技術 SPHERE（Security-updatable Public-key Homomorphic Encryption with Rich Encodings）を開発した。SPHERE は統計処理などを扱える準同型暗号であるというだけでなく、安全に、漏洩リスクを高めることなくセキュリティレベル（鍵長）の更新が可能である。このため、暗号化データを長期間にわたって安全に利活用することが可能となる。

また、実際のシステムを想定し、SPHERE による暗号化データでのロジスティック回帰分析の計算実験を行った。ロジスティック回帰分析には暗号化データでの計算に適さない演算が含まれているため、そのままでは高速な計算が困難であるが、指数関数や対数関数の多項式近似、データ提供者側でのデータの事前加工などの改良により、これを解決した。1 億件の擬似データで実験を行い、30 分程度での処理が可能であることを確認している。

2　新たな準同型暗号技術 SPHERE

我々が開発した SPHERE では、平文は $\mathbb{Z}_p$（ただし、$\mathbb{Z}_p = \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$ と表現）の ℓ 次元ベクトル、暗号文は $\mathbb{Z}_q$ の $n+\ell$ 次元ベクトルであり、準同型演算として複数回の加算と 1 回の掛け算（ベクトルのテンソル積）、さらに、セキュリティレベルの更新機能をサポートする。暗号方式を図 1 に示す。図中 ParamGen( ) はパラメータ生成、KeyGen( ) は鍵生成、Enc( ), Dec( ) はそれぞれ暗号化、復号を表す。また、pk は公開鍵、sk は秘密鍵を表す。暗号文、鍵の安全性は Learning with Error 問題に帰着される。安全性証明などの詳細については文献 [1] を参照されたい。

2.1　Learning with Error 問題

q を法とする整数の一様分布から抽出した行列 A と整数ベクトル $b = (Ax + e \bmod q)$ が与えられたとき、整数ベクトル x を求める問題を Learning with Error（LWE）問題という。ここで、e は分散 s^2 の離散ガウス分布から抽出したノイズベクトルである。LWE 問題の計算方法は様々にあるが、現在最も高速なもののひとつに最短ベクトル問題への帰着がある。最短ベクトル問題及びその計算量評価については、文献 [2] を参照いただきたい。LWE 問題の計算量はベクトル x の次元の指数時間で与えられるため、x の次元が大き

PKE part

ParamGen(1^λ):
Fix $q = q(\lambda) \in \mathbb{Z}^+$
Fix $l \in \mathbb{Z}^+$
Fix $p \in \mathbb{Z}^+$, $\gcd(p, q) = 1$
Return $pp = (q, l, p)$

KeyGen($1^\lambda, pp$):
Take $s = s(\lambda, pp) \in \mathbb{R}^+$
Take $n = n(\lambda, pp) \in \mathbb{Z}^+$
$R, S \xleftarrow{g} \mathbb{Z}_s^{n\times l}$, $A \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$
$P = pR - AS \in \mathbb{Z}_q^{n\times l}$
Return $pk = (A, P, n, s)$, $sk = S$

Enc($pk, m \in \mathbb{Z}_p^{1\times l}$):
$e_1, e_2 \xleftarrow{g} \mathbb{Z}_s^{1\times n}$, $e_3 \xleftarrow{g} \mathbb{Z}_s^{1\times l}$
$c_1 = e_1 A + pe_2 \in \mathbb{Z}_q^{1\times n}$
$c_2 = e_1 P + pe_3 + m \in \mathbb{Z}_q^{1\times l}$
Return $c = (c_1, c_2)$

Dec($S, c = (c_1, c_2)$):
$\overline{m} = c_1 S + c_2 \in \mathbb{Z}_q^{1\times l}$
$m = \overline{m} \bmod p$
Return m

Homomorphic part

Add(c, c'):
Return $c + c' \bmod q$

AddM($c_{\mathrm{mul}}, c'_{\mathrm{mul}}$)
Return $c_{\mathrm{mul}} + c'_{\mathrm{mul}} \bmod q$

DecM(sk, c_{mul}):
Let $sk = S \in \mathbb{Z}_q^{n\times l}$

Mul(pp, pk, c, c'):
Return $c_{\mathrm{mul}} = c^{\mathsf{T}} c' \in \mathbb{Z}_q^{(n+l)\times(n+l)}$

DecA(sk, c_{add}):
identical to Dec

$$\overline{m} = \begin{bmatrix} S \\ I_l \end{bmatrix}^{\mathsf{T}} (c_{\mathsf{mul}}) \begin{bmatrix} S \\ I_l \end{bmatrix} \in \mathbb{Z}_q^{l\times l}$$ (I_l: the identity matrix)
Return $\overline{m} \in \mathbb{Z}_p^{l\times l}$

図 1　準同型暗号技術 SPHERE の暗号処理詳細

くなるほど計算が困難になる。また、LWE 問題は、従来の公開鍵暗号方式が安全性の根拠とする素因数分解問題や離散対数問題とは異なり、多項式時間の量子アルゴリズムがいまだ知られていないため、大規模な量子計算機の登場以降も安全に利用可能な“耐量子暗号”の安全性根拠として注目されている。

暗号文から平文の解読を例に、SPHERE と LWE 問題の関係を見る。SPHERE の暗号文 $c = (c_1, c_2)$ は、$c_1 = e_1 A + pe_2 \bmod q, c_2 = e_1 P + pe_3 + m \bmod q$ で与えられる。A, Pは公開鍵であり、攻撃者には既知、e_1, e_2, e_3 はノイズベクトルであり攻撃者には未知、m は平文である。$m = c_2 - e_1 P + pe_3 \bmod q$ であり平文は $\mathbb{Z}_p$ のベクトルであるから、e_1 が得られると $m = (c_2 - e_1 P) \bmod p$ により平文が得られ、解読に成功する。しかし、e_1 を得るには $c_1 = (e_1 A + pe_2) \bmod q$ を解かなければならない。これは LWE 問題に相当するため、LWE 問題が十分に困難であれば暗号文から平文の解読は困難であると考えられる。

2.2　セキュリティレベルの更新

SPHERE の安全性は LWE 問題に帰着され、LWE 問題の困難性は秘匿されたベクトルの次元（SPHERE ではパラメータ n で与えられる）の指数時間となる。このため、n を新たな $n'(> n)$ となるように、暗号文の情報や構造を崩さずに変換できれば、セキュリティレベルが更新できる。これを実現するために、dimension switching[3] という手法を応用した。セキュリティレベルの更新処理を図 2 に示す。図中、更新前後の鍵は $(pk_i, sk_i) = \{(A_i, P_i, n_i), S_i\}$ であり、$i = 1,2$ がそれぞれ更新前と更新後を表す。また、Bits( ) は暗号文の情報を保ったまま、各成分をノイズと同程度に小さくするビット化関数、Power2( ) は Bits (c_1) Power2 (S_1) = $c_1 S_1$ となる関数である。UKGen( ) は更新鍵の生成、Update( ) は暗号文のセキュリティレベル更新処理である。

Key rotation and security update

UKGen($pp, pk_1, sk_1, pk_2, sk_2$):
Let $pk_i = (A_i, P_i, n_i, s_i)$. Let $sk_i = S_i$ $(i = 1, 2)$
Let $\kappa = \lceil \log_2 q \rceil$. Take $X \xleftarrow{\$} \mathbb{Z}_q^{n_1\kappa\times n_2}$, $E \xleftarrow{g} \mathbb{Z}_{s_2}^{n_1\kappa\times l}$
$Y = -XS_2 + pE + \mathsf{Power2}(S_1) \in \mathbb{Z}_q^{n_1\kappa\times l}$
Return $uk_{n_1\to n_2} = (X, Y)$

Update($pp, c, uk_{n_1\to n_2}, pk_2$):
Let $c = (c_1, c_2) \in \mathbb{Z}_q^{1\times n_1} \times \mathbb{Z}_q^{1\times l}$
Let $pk_2 = (A_2, P_2, n_2, s_2)$
Let $uk_{n_1\to n_2} = (X, Y)$, and $f_1, f_2 \xleftarrow{g} \mathbb{Z}_{s_2}^{1\times n_2}$, $f_3 \xleftarrow{g} \mathbb{Z}_{s_2}^{1\times l}$
$E_0 = f_1[A_2|P_2] + p[f_2|f_3] \in \mathbb{Z}_q^{1\times(n_2+l)}$
$F = [\mathsf{Bits}(c_1)X|\mathsf{Bits}(c_1)Y + c_2] \in \mathbb{Z}_q^{1\times(n_2+l)}$
Return $c' = E_0 + F \in \mathbb{Z}_q^{1\times(n_2+l)}$

図 2　セキュリティレベル更新処理詳細

2.3　固定小数点数のエンコード

本節冒頭で述べたとおり、SPHERE の平文空間は各要素が $\mathbb{Z}_p$ の ℓ 次元ベクトルである。しかし、統計処理システムなどの、準同型暗号で構築したい実際の処理システムでは（精度付き）実数値を扱う必要がある。ここでは、$\mathbb{Z}_p$ 係数多項式、そして、整数・固定小数点数へのエンコード手法について述べる。

$\mathbb{Z}_p$ 係数多項式のエンコードは、多項式 $A(x) = \sum_{i=0}^{\ell-1} a_i x^i$ の各係数を各要素に持つベクトル $A = (a_0 \ldots a_{\ell-1})$ を考えれば良い。この表現であれば、ベクトルの加減算 $A \pm B$ は対応する多項式の加減算 $A(x) \pm B(x)$ と自明に対応付く。多項式乗算は、ベクトルのテンソル積 $A^{\mathsf{T}}B$ の各要素がベクトル A, B の各要素の積 $a_i b_j$ a となることから、$A^{\mathsf{T}}B$ の要素を適当に和を取ることで $A(x) \times B(x)$ の各係数を計算できる。

整数・固定小数点数のエンコードは、それらの符号付きバイナリ表現を

$$N = \sum_{i=-L}^{\ell-L-1} n_i 2^i \ (n_i \in \begin{cases} \{0,1\} \text{ if } N \geq 0 \\ \{-1,0\} \text{ if } N < 0 \end{cases}$$

とし、各n_iを多項式の係数と対応付けることにより定義する。$L = 0$のときは整数、$L > 0$のときは小数点以下L桁精度の固定小数点数である。$\mathbb{Z}_p$係数多項式とSPHEREの平文の演算は対応づくから、SPHEREの平文の演算により、整数・固定小数点数の演算が可能となる。ベクトルでの演算結果の各係数が$\mathbb{Z}_p = \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$の範囲内であれば、対応づけた多項式$N(x)$と$N$が一対一対応するが、演算結果が$\mathbb{Z}_p$の範囲から出てしまうと正しく整数・固定小数点数に戻せなくなるため、演算回数やpの大きさを適切に制御する必要がある。

2.4　実装結果

SPHEREをソフトウェア実装し、暗号処理時間の測定を行った。暗号処理の計算時間を表1に、セキュリティアップデート処理の計算時間を表2に示す。表中、bit-secはビットセキュリティを表し、Key rotationは同セキュリティレベルでの鍵更新、Security updateはセキュリティレベル更新処理を指す。実験はXeon E5-2660 v3（2.60 GHz）で行い、全て1スレッドで計算している。

表1　暗号処理時間の測定結果（ミリ秒）

bit-sec	KeyGen	Enc	Dec	Add	Mul	AddM	DecM
80	1428	63.2	0.92	0.003	35.1	29.3	1313
128	2513	94.7	1.22	0.004	60.8	50.1	2296
256	7249	313	2.05	0.010	164	136	6643

表2　セキュリティアップデート処理の測定結果（秒）

	bit-sec → bit-sec	UKGen	Update
Key rotation	80 → 80	165.6	1.1
	128 → 128	291.4	1.9
	256 → 256	846.6	5.3
Security update	80 → 128	238.2	1.5
	128 → 256	519.8	3.3

3　プライバシー保護データマイニングへの応用 – ロジスティック回帰分析

ロジスティック回帰分析は、教師あり機械学習の一種であり、機械的なデータの分類を比較的少ない計算量で行えることからその応用先は多岐にわたる。例えば、検査データから患者が病気であるかどうかを診断するサービスなどが考えられる。このような場合、検査データはプライバシーに関わる情報であるから、当然ながら慎重に扱わなければならない。検査データを安全に扱いつつ、ロジスティック回帰分析を行うために、我々は準同型暗号技術を応用した。我々の開発したシステムでは、訓練データと分類対象のデータは暗号化されているため、完全に保護される。

我々の開発したシステムのデータ処理モデルを図3に示す。データ提供者（患者本人や医療機関など）はそれぞれがデータを暗号化し、中央サーバに保存する。サーバは暗号の準同型性を使ってロジスティック回帰分析に関する処理を行い、それをデータ分析者に送信する。データ分析者はそれを復号することで、学習済みロジスティック回帰係数が取り出せる。

3.1　ロジスティック回帰分析

学習対象のデータセットは、N_{data}件のレコード

$$\{x^{(i)}, y^{(i)}\}_{1 \leq i \leq N_{data}}$$

で表現され、各レコードは$d+1$次元実数ベクトル$x^{(i)} = \left(1, x_1^{(i)}, \ldots, x_d^{(i)}\right)$とラベル$y^{(i)} \in \{0,1\}$のペアとする。回帰係数$\theta = (\theta_0, \ldots, \theta_d)$を変数とするコスト関数$J$を

$$J(\theta) = \frac{\lambda}{2N_{data}} \sum_{j=1}^{d} \theta_j^2 + J^*(\theta)$$

と定義する。ただし、

$$J^*(\theta) = \frac{1}{N_{data}} \sum_{i=1}^{N_{data}} \left[-y^{(i)} \log\left(h_\theta\left(x^{(i)}\right)\right) - \left(1 - y^{(i)}\right) \log\left(1 - h_\theta\left(x^{(i)}\right)\right)\right]$$

とする。ここで、$h_\theta(x) = h_\theta(x_0, \ldots, x_d)$はシグモイド関数で、

$$h_\theta(x) = \frac{1}{1 + \exp(-\theta^\top x)} = \frac{1}{1 + \exp(-\sum_{j=0}^{d} \theta_j x_j)}$$

と定義される。常に$x_0 = 1$とする。

ロジスティック回帰分析の学習フェーズでは与えられたデータセットに対して、コスト関数を最小化する

$$\theta^* = \text{argmin}_\theta J(\theta)$$

を計算する。

推定フェーズでは、新たに入力された判定対象のデータ$x^{new} = (1, x_1^{new}, \ldots, x_d^{new})$に対して、それに対応

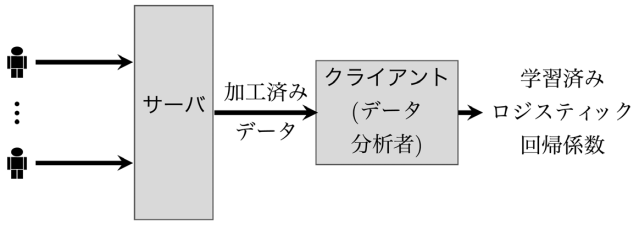


図3　想定しているデータ処理のモデル

するラベル y^{new} が {0,1} のどちらに属するのかを以下の式で予測する。

$$y^{new} = \begin{cases} 1 \text{ if } h_{\theta^*}(x^{new}) \geq \text{thres} \\ 0 \text{ if } h_{\theta^*}(x^{new}) < \text{thres} \end{cases}$$

ここで、thres∈(0,1) は閾値で、大抵の場合 thres=1/2 が用いられる。

3.2　準同型暗号に向けた処理の改良 1: 多項式近似による指数・対数関数の除去

関数 $J^*(\theta)$ は、その定義に指数関数・対数関数を含むため、準同型暗号で正確に実装しようとすると非常に複雑な形になってしまう。その問題を避けるため、それらを適当な多項式、特にここでは二次多項式で近似した形で学習アルゴリズムを構成する。

関数 $\log(\frac{1}{1+\exp(u)})$ の二次近似 $\sum_{j=0}^{2} a_j(u^j)$ を用いて、$\log(h_\theta(x))$ 及び $\log(1-h_\theta(x))$ を

$$\log(1-h_\theta(x)) \approx \sum_{j=0}^{2} a_j(\theta^\top x)^j,\ \log(h_\theta(x)) \approx \sum_{j=0}^{2} (-1)^j a_j(\theta^\top x)^j$$

と近似する。このとき、上式を使った $J^*(\theta)$ の近似 $J^*_{approx}(\theta)$ は

$$J^*_{approx}(\theta) = \frac{1}{N_{data}} \sum_{j=1}^{2} \sum_{r_1,r_2}^{d} a_j\left(\theta_{r_1},\dots,\theta_{r_j}\right) A_{j,r_1,r_j} - a_0$$

ただし、

$$A_{1,r_1,r_1} = \sum_{i=1}^{N_{data}} \left(2y^{(i)}-1\right)\left(x_{r_1}^{(i)}\right) \quad (1)$$

$$A_{2,r_1,r_2} = \sum_{i=1}^{N_{data}} -\left(x_{r_1}^{(i)} x_{r_2}^{(i)}\right) \quad (2)$$

となる。

近似係数としては、テイラー展開によるもの

$$\text{(Taylor) } a_0 = -\log 2, a_1 = -0.5, a_2 = -0.125$$

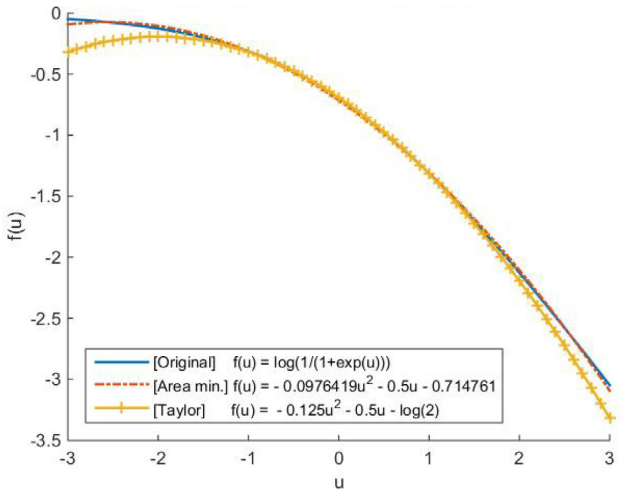


図 4　オリジナルの関数とその二次多項式近似

がよく知られているが、二次の展開では誤差が比較的大きいため、区間 $x \in [-3,3]$ での最小二乗法により誤差を最小化したもの

$$\text{(LSM) } a_0 = -0.714761, a_1 = -0.5, a_2 = -0.0976419$$

を用いた。図 4 にオリジナルの関数とともに、それぞれの二次多項式による近似のグラフを示す。

3.3　準同型暗号に向けた処理の改良 2: データ提供者の事前計算による乗算の除去

指数関数・対数関数の多項式近似により、準同型暗号方式が二次形式の計算をサポートしていればロジスティック回帰分析が可能である。しかし、表 1 にあるように SPHERE の乗算 Mul( ) やその復号 DecM( ) は比較的遅いため、例えば 1 億件のレコードなどの大規模なデータセットの分析には更なる効率化が必要である。

3.2 の式(1)、(2)を見ると、各項 $a_{1,r_1}^{(i)} = \left(2y^{(i)}-1\right)\left(x_{r_1}^{(i)}\right), a_{2,r_1,r_2}^{(i)} - \left(x_{r_1}^{(i)} x_{r_2}^{(i)}\right)$ はレコード $\{x^{(i)}, y^{(i)}\}$ で構成されていることが分かる。つまり、$a_{1,r_1}^{(i)}, a_{2,r_1,r_2}^{(i)}$ の計算はデータ提供者が暗号化前に計算が可能である。これを使って、準同型暗号によるロジスティック回帰分析を以下のように行う。

レコード $\{x^{(i)}, y^{(i)}\}$ を持つデータ提供者は、$a_{1,r_1}^{(i)}, a_{2,r_1,r_2}^{(i)} (0 \leq r_1, r_2 \leq d)$ を計算し、それぞれ暗号化、その結果をサーバに送信する。サーバは受け取った暗号文 $\text{Enc}(a_{1,r_1}^{(i)}), \text{Enc}(a_{2,r_1,r_2}^{(i)})$ それぞれを準同型加算することで $\text{Enc}(A_{1,r_1,r_1}), \text{Enc}(A_{2,r_1,r_2})$ が得られる。あとはクライアントが復号し、$A_{1,r_1,r_1}, A_{2,r_1,r_2}$ から $J^*_{approx}(\theta)$ が得られ、それを用いて学習済みロジスティック回帰係数 θ^* を計算すれば良い。

この方式ではデータ提供者は $a_{1,r_1}^{(i)}, a_{2,r_1,r_2}^{(i)}$ それぞれを暗号化する必要があるが、サーバは準同型加算のみで良いため、我々が想定しているモデルのような、データ提供者がサーバに比べて非常に多いモデルでは効率的な計算が可能である。また、準同型加算のみで良いことから、Paillier 暗号 [4] などの加算のみをサポートする準同型暗号方式による構成も可能である。

3.4　実験結果

前述の改良について、(1) 大規模な擬似データセットでのサーバの計算時間の計測、(2) 実際のデータセットでの統計学的指標の評価を行った。後者は二次多項式近似による実用性への影響を評価するためである。

大規模な擬似データセットでのサーバの計算時間を図 5 に示す。レコード数は 1 億件と 2 億件で、横軸はデータの次元 d である。計算実験は 128 ビットセキュリティを実現するパラメータで行い、Xeon E5 -2660 v3（2.60 GHz）を 2 つ備えたサーバで、20 スレッドで

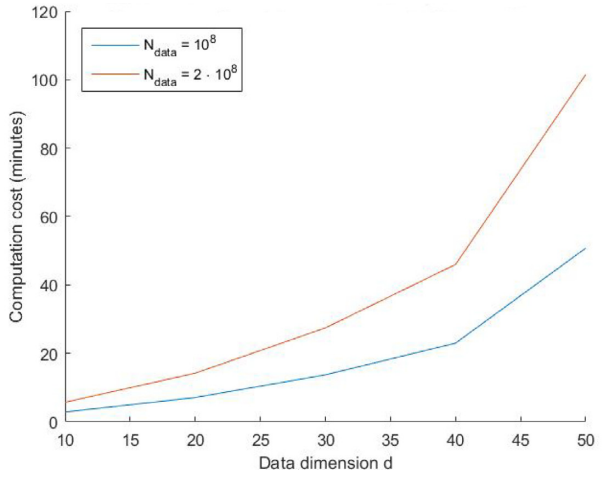


図５　大規模擬似データセットでのサーバの計算時間

計算している。$d \leq 40$ 程度であれば、1 億件のデータセットでも 30 分未満で分析が完了する事が分かる。

次に、実際のデータセットでの統計学的指標の評価を表 3 に示す。データセットはカリフォルニア大学アーバイン校が公開する実データリポジトリ [5] の中から、北米ピマインディアンの糖尿病に関するデータセット（Pima）と心臓の単一光子放射断層撮影の結果と心臓病の有無に関するデータセット（SPECTF）の 2 点で、評価指標として正解率、F 値、AUC を扱った。各指標の定義については、例えば文献 [6] などを参照いただきたい。正解率、F 値、AUC ともに大きな外れはなく、多項式近似による影響が少ないことが分かる。この他のデータセットにおける評価等については [7][8] を参照いただきたい。

表３　オリジナルの関数と二次多項式近似での正解率、F 値、AUC の比較

データセット	暗号化の有無	コスト関数	正解率	F 値	AUC
Pima	暗号化なし	オリジナル	80.2%	0.688525	0.873653
	暗号化あり	二次近似	80.7%	0.694215	0.876347
SPECTF	暗号化なし	オリジナル	79.1%	0.876972	0.783333
	暗号化あり	二次近似	75.4%	0.851613	0.761628

4　まとめ

本稿では、セキュリティ基盤研究室が開発した長期利用可能な準同型暗号技術 SPHERE とその応用としてのプライバシー保護型ロジスティック回帰分析システムの構築について述べた。本稿では省略したが、ロジスティック回帰分析のほか、線形回帰分析や生体認証への応用も行っている [1]。

IoT 等によりデータの収集・分析が容易になる中で、それらのデータから漏れ得る個人に紐づく情報の保護は喫緊の課題である。我々が開発した暗号技術及びその応用技術がこれらの課題の解決策のひとつとなることを期待する。

【参考文献】

1　Y. Aono, T. Hayashi, L. T. Phong, and L. Wang, “Fast and Secure Linear Regression and Biometric Authentication with Security Update,” IACR Cryptology ePrint Archive 2015, 692, 2015.

2　青野良範，林卓也，篠原直行，“暗号の安全性評価技術の高度化，”情報通信研究機構研究報告，本特集号，7-1，2016.

3　Z. Brakerski and V. Vaikuntanathan, “Efficient Fully Homomorphic Encryption from (Standard) LWE,” IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, pp.97–106, 2011.

4　P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” Advances in Cryptology– International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT ’99, Lecture Notes in Computer Science, vol.1592, pp.223-238, 1999.

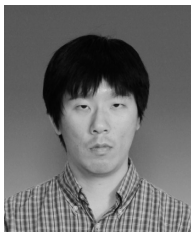
5　UCI Machine Learning Repository, http://archive.ics.uci.edu/ml/

6　中川裕志，“東京大学工学教程 情報工学 機械学習，”東京大学工学教程編纂委員会，2015.

7　Y. Aono, T. Hayashi, L. T. Phong, and L. Wang, “Scalable and Secure Logistic Regression via Homomorphic Encryption,” 6th ACM on Conference on Data and Application Security and Privacy, CODASPY 2016, pp.142–144, 2016.

8　Y. Aono, T. Hayashi, L. T. Phong, and L. Wang, “Privacy-Preserving Logistic Regression with Distributed Data Sources via Homomorphic Encryption,” accepted to IEICE Transactions on Information and Systems, vol.E99-D, no.8, 2016.

Le Trieu Phong
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（学術）
暗号プロトコル設計と安全性評価



青野良範　（あおの　よしのり）
サイバーセキュリティ研究所
セキュリティ基盤研究室
研究員
博士（理学）
暗号解析、格子理論

林　卓也　（はやし　たくや）
サイバーセキュリティ研究所
セキュリティ基盤研究室
研究員
博士（機能数理学）
暗号解析、高速実装

王　立華　（おう　りつか）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号プロトコル設計と安全性評価