様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月 ２４ 日現在

機関番号：２０１０３
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３０１５６

研究課題名（和文）メニーコア・コプロセッサによる暗号高速実装の研究

研究課題名（英文）Study of Fast Implementation of Cryptosystems with Many-core Co-processor

研究代表者
白勢　政明（SHIRASE, Masaaki）

公立はこだて未来大学・システム情報科学部・准教授

研究者番号：７０５３０７５７

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：本研究は、2013年に流通を開始したメニーコア・コプロセッサによる暗号高速実装法を確立するために、（１）暗号アルゴリズムの改良と（２）複数ファイルの並列暗号処理実装法を研究した。
（１）については、座標変換や新しい座標系の導入、２次曲線の利用を用いた加算法の提案により、近年普及が進んでいる楕円曲線暗号や高機能暗号に必要なペアリング演算の高速化を達成した。（２）については、OpenSSL暗号ライブラリの利用を前提とした共通鍵暗号の並列実装を提案した。また、冗長鍵による公開鍵暗号の高速並列実装法を研究した。

研究成果の概要（英文）：This study has focused on (1) improvement of cryptographic algorithms and (2) implementation of cryptosystems in parallel for multiple files in order to establish fast implementation method cryptosystems with many-core coprocessor, which distributed to the market in 2013.
For (1), this study proposed fast algorithms for elliptic curve and pairing-based cryptosystems due to coordinate transform, introduction of new coordinate system, and new addition method using quadratic curve. For (2), this study proposes a parallel implementation of symmetric key cryptosystem using OpenSSL cryptographic library, and is doing research a parallel implementation of public key cryptosystem using a redundant key.

研究分野：情報学

キーワード：メニーコア・コプロセッサ　楕円曲線暗号　ペアリング暗号　AES　並列実装

１．研究開始当初の背景

(1)暗号技術の必要性の高まり:
クラウドコンピューティングでは，利用者は必要な時に計算資源やデータをネットワークを通じて利用し，故障の対応やデータの管理，OS やアプリケーションのアップデートの対応は運営企業に委託するため，利用者はこれらを意識する必要がなく利便的である．しかしながら，個人の PC での処理では暗号化が不要であった私有データのアクセスに対しても，クラウドコンピューティングではネットワーク内を移動するため，データの暗号化が必要となる．このようにクラウドコンピューティングの普及により暗号技術の利用頻度が高まることが予想された．

情報通信機器を用いる様々な活動において，訴訟対策，法令遵守，説明責任のため，不正無く活動を行っていることを証明するデジタルフォレンジックの重要性の認識が高まっており，その手法の一つに，作業の痕跡や履歴に関する電子データに時刻情報の連結に電子署名を施し逐次保存することがある．従って，デジタルフォレンジックの運用により，暗号技術の一種である電子署名の利用頻度の上昇が予想された．

(2)暗号新技術の普及:
近年，ペアリングと呼ばれる楕円曲線上の双線型性写像を利用した暗号新技術(ペアリング暗号)の研究が盛んになっており，その 1 つに属性ベース暗号がある．属性ベース暗号では，動画配信を例にとると，配信会社は視聴権限者の属性情報を論理演算しその結果を鍵として動画データを暗号化/配信し，権限所有者のみが各自保有する鍵でデータ復号し視聴可能となる．つまり属性ベース暗号は，アクセス制御可能な安全な通信を提供できる．しかしながら，属性ベース暗号ではペアリング計算を多く必要とし，高速なペアリング計算の実装法が求められている．

(3)GPU による公開鍵暗号の実装:
実用化されている公開鍵暗号(RSA 暗号や楕円曲線暗号)では，多倍長整数(160 から 2048 ビット)の剰余乗算(乗算の後に剰余をとる演算，$a \times b \bmod n$)を多数(数百～数千回)繰り返す必要があり，その処理の計算コストは大きい．そこで近年，メニーコア化されている GPU を使用して公開鍵暗号の処理を並列に行う研究が盛んになっている．

(4)メニーコア・コプロセッサの誕生[引用①]:
CPU 開発会社は近年，コプロセッサのメニーコア化(数十以上のコアの搭載)に注力しており，2013 年に Intel Xeon Phi の販売が開始された．メニーコア・コプロセッサの性能を十分に活かすためには，並列化を意識したプログラミングが重要である．CPU 開発会社は並列プログラムを容易に記述するための拡張言語に対応したコンパイラを開発しており，更に，並列化を補助する開発ツールの提供を行っている．コプロセッサは演算ボードという位置づけであるが，Intel Xeon Phi のコプロセッサ・コアの構造は CPU コアとほぼ同一である．

以上のような背景により，メニーコア・コプロセッサへの暗号システムの並列実装法の確立が必要であると考えられた．

２．研究の目的

本研究の対象を，公開鍵暗号は RSA 暗号と比較して処理速度が高速で鍵サイズが小さく近年急速に普及が進んでいる楕円曲線暗号，及び属性ベース暗号を実現できるペアリング暗号とし，共通鍵暗号はデファクトスタンダードである AES とした．本研究の目的は，これらに対する高速暗号アルゴリズムの提案と，処理の高速性や低消費電力性，実装容易性を有するメニーコア・コプロセッサに適したと並列実装法を提案することである．

実用的な暗号システムのメニーコア・コプロセッサへの並列実装法が確立させることで，現在普及過程中であるクラウドコンピューティングやデジタルフォレンジックの効率的な安全運用の推進や，属性ベース暗号処理の効率化によりデータ配信の安全なアクセス制御等に貢献したい．

３．研究の方法

(1)暗号アルゴリズムの改良
本研究が対象とする共通鍵暗号 AES は，AES-NI 命令をサポートする市販 CPU で既に高速に処理できるため，本研究ではアルゴリズムの改良は公開鍵暗号のみに焦点を当てる．楕円曲線暗号やペアリング暗号といった公開鍵暗号における，多倍長整数表現，剰余乗算を含む暗号アルゴリズムに対して，メニーコア・コプロセッサに適した並列処理法の調査をし，これらの高速なアルゴリズムの提案を行う．

(2)並列実装手法の確立と実装評価
メニーコア・コプロセッサには，高速 64 ビット整数乗算，物理的乱数の可用性，コンパイラと開発ツールの充実，多数の 512 ビット SIMD ビットレジスタの搭載，x86 アーキテクチャの採用，という GPU とは異なる特徴を有しており，本研究はこれらを活用できる並列実装法を提案する．その後メニーコア・コプロセッサを導入し，CPU 実装との比較を中心に実装評価を行う．

４．研究成果

(1)暗号アルゴリズムの改良
① 準備-楕円曲線と楕円曲線暗号
本研究の成果の紹介に際し必要となる事項をここで解説する．
Weierstrass 標準形

$$E: y^2 = x^3 + Ax + B$$

等で与えられる曲線を楕円曲線といい，Eの点P,Qに対してEの別の点$P+Q$が定義できる．$P\neq Q$に対して$P+Q$を計算する公式を加算公式，$P+P=2P$を計算する公式を 2 倍算公式という．更にこの加算によりE上の点の集合は無限遠点Oを単位元とする群をなす．この加算を繰り返すことで，$P\in E$ と整数nからスカラー倍

$$nP=P+P+\cdots+P\ (n\text{個の和})$$

が定義される．

ペアリング・フレンドリー曲線と呼ばれる特殊な楕円曲線EとそのツイストE'に対して

$$e(aP,bQ)=e(P,Q)^{ab}$$

を満たす写像

$$e:E\times E'\to F_{p^k}$$

をペアリングという．ペアリングは Miller のアルゴリズムにより計算される．ペアリングを用いることで，ID ベース暗号，タイムリリース暗号，属性ベース暗号といった高機能暗号を実現でき，これらを総称してペアリング暗号と言う．

Barreto と Naehrig はペアリング・フレンドリー曲線の効率的な構成法を与えている．zを変数とする多項式$p(z),t(z),n(z)$を

$$p(z)=36z^4+36z^3+24z^2+6z+1$$
$$n(z)=36z^4+36z^3+18z^2+6z+1$$

と定義すると，$p(z)$と$n(z)$が素数となる整数zに対して$F_{p(z)}$上楕円曲線$y^2=x^3+B$はペアリング・フレンドリーになる．この楕円曲線は BN 曲線と呼ばれる．

楕円曲線暗号の支配的演算は有限体F_p上楕円曲線のスカラー倍である．ペアリング暗号もスカラー倍は必要である．従って，楕円曲線暗号とペアリング暗号の実装において，スカラー倍のコスト削減は重要である．

本稿では乗算コストを **M**，2 乗算コストを **S** で表記する．

② 座標変換によるスカラー倍の高速化[発表⑨]

本研究は，Weierstrass 標準形$E:y^2=x^3+Ax+B$で与えられるEと$P\in E$に対して，スカラー倍 nP を高速に計算する方法を提案した．この方法では，初めに Pが$P'=(\chi,\pm\chi)\in E'$となるような座標変換$\phi:E\to E'$を行う．次にE'でスカラー倍nP'を計算する．Pは特別な座標を持っているため，nP'の計算コストはnPより低い．最後に逆変換$\phi^{-1}:E'\to E,nP'\mapsto nP$を行う．なお，$P=(x_0,y_0)\in E$とすると

$$E':y^2=x^3+(x_0^4/y_0^4)Ax+(x_0^6/y_0^6)B$$

及び，

$$P'=(x_0^3/y_0^2,\pm x_0^3/y_0^2)\in E'$$

となる．その結果，普通のバイナリ法を用いる時は，射影座標系でのスカラー倍の計算コストは 2.6%削減でき，ヤコビアン座標系でのスカラー倍の計算コストは 3.1%削減できる．単純電力解析に耐性を持つバイナリ法を用いる時は，射影座標系でのスカラー倍の計算コストは 4.3%削減でき，ヤコビアン座標系でのスカラー倍の計算コストは 4.9%削減できる．

③ Pと$2P$の座標に着目する楕円曲線スカラー倍の高速化[発表⑥]

絶対値が小さな整数a,bに対して$P=(a\chi,b\chi)$となっている場合でも②の手法を用いてスカラー倍を同様に計算でき，更に$2P$の座標も同様な性質を持つとき，ウィンドウ法によるスカラー倍計算に②の手法を適用できる．そこで，絶対値が小さな整数a,b,c,dに対して，

$$\begin{aligned}P&=(a\chi,b\chi)\\2P&=(c\chi',d\chi')\end{aligned}$$

となるベースポイントPを持つ楕円曲線$E:y^2=x^3+B$の構成法を考察した．$P=(a\chi,b\chi)$がEの点であるとすると，

$$B=b^2\chi^2-a^3\chi^3 \qquad (1)$$

を満たす．また，$P=(a\chi,b\chi)$に 2 倍算公式を適用すると，

$$c\chi'=\frac{9a^4\chi^2-8ab^2\chi}{4b^2}$$

$$d\chi'=\frac{-27a^6\chi^3+36a^3b^2\chi^2-8b^4\chi}{4b^3}$$

となり，次が得られる．

$$-27a^6c\chi^2+(-18a^4bd+36a^3b^2c)\chi+(16ab^3d-8b^4c)=0 \qquad (2)$$

よって，(2)を満たすa,b,c,d,χを見つけ，(1)によりBを計算すると，$E:y^2=x^3+B$はベースポイント$P=(a\chi,b\chi),2P=(c\chi',d\chi')$を持つ楕円曲線となる．

$$\begin{aligned}\alpha&=-27a^6c\\\beta&=-18a^4bd+36a^3b^2c \qquad (3)\\\gamma&=16ab^3d-8b^4c\end{aligned}$$

とおくと，$\beta^2-4\alpha\gamma$が定義体で平方数ならば 2 次方程式(2)は定義体で根を持ち，目的とする楕円曲線とベースポイントが得られる．よって以下のようなアルゴリズムを構成できる．

アルゴリズム 1

入力：整数a,b,c,d
出力：$P=(a\chi,b\chi),2P=(c\chi',d\chi')\in E$となる$E:y^2=x^3+B$と$P,2P$

1. (3)のように(α,β,γ)を計算
2. $\beta^2-4\alpha\gamma$が定義体上平方数ならば
   2-1. 方程式(2)の根χに対して$P=(a\chi,b\chi)$とする
   2-2. 普通に$2P=(c\chi',d\chi')$を計算
   2-3. (1)よりBを計算し，$E:y^2=x^3+B$と$P,2P$を返す
3. $\beta^2-4\alpha\gamma$が非平方数ならば failure

定義体を有理数体とし，$a,b,c,d\leq|4|$となる整数を入力として**アルゴリズム 1** を実行すると 50 例の出力を得た．これらの例のBはすべて$B=2^i3^j,i\equiv 2,j\equiv 3\ (\mathrm{mod}\ 6)$の形をしていた．

アルゴリズム 1 をペアリング・フレンドリー曲線である BN 曲線に適用することで，以

下の命題が得られた.

命題 1

$z \equiv 1,7,13,19,25,31 \pmod{36}$を満たすとする. すると,

$$B \in \{108, \frac{27}{16}, \frac{4}{27}, \frac{256}{27}, \frac{16384}{27}, \frac{1}{432}, \frac{27}{1024},$$

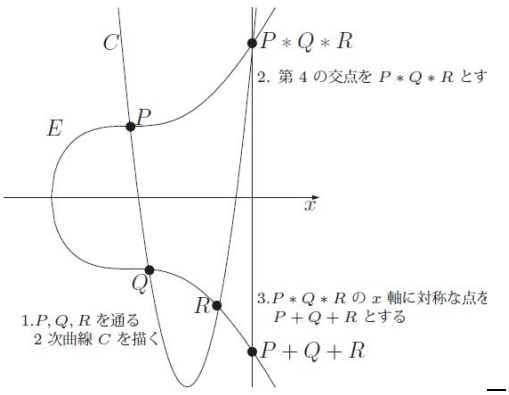
$$\frac{4}{19683}, \frac{256}{19683}, \frac{16384}{19683}, \frac{1}{27648}\}$$

に対して$y^2 = x^3 + B$は BN 曲線となり, 各Bに対して次のような点Pと点$2P$を持つ.

B	Pの座標	$2P$の座標
108	$(6, \pm 18)$	$(-3, \pm 9)$
27/16	$(3/2, \pm 9/4)$	$(-3/4, \pm 9/8)$
4/27	$(2/3, \pm 2/3)$	$(-1/3, \pm 1/3)$
256/27	$(8/3, \pm 16/3)$	$(-4/3, \pm 8/3)$
16384/27	$(32/3, \pm 128/3)$	$(-16/3, \pm 64/3)$
1/432	$(1/6, \pm 1/12)$	$(-1/12, \pm 1/24)$
27/1024	$(3/8, \pm 9/32)$	$(-3/16, \pm 9/64)$
4/19683	$(2/27, \pm 2/81)$	$(-1/27, \pm 1/81)$
256/19683	$(8/27, \pm 16/81)$	$(-4/27, \pm 8/81)$
16384/19683	$(32/27,$ $\pm 128/81)$	$(-16/27,$ $\pm 64/81)$
1/27648	$(1/24,$ $\pm 1/96)$	$(-1/48,$ $\pm 1/192)$

④ 2 次曲線を用いた楕円曲線・ペアリング演算[発表⑦,⑧]

楕円曲線暗号の主演算であるスカラー倍算は, 一般に加算公式と 2 倍算公式によって計算される. 加算公式と 2 倍算公式は一般に, 楕円曲線$E: y^2 = x^3 + Ax + B$とある直線Lとの交点の座標から導かれる. 本研究では, 楕円曲線Eと 2 次曲線$C: y = ax^2 + bx + c$との交点がP, Q, R, Sの時, $S = P * Q * R (\Leftrightarrow P + Q + R + S = O)$が成り立つことを示した.



この結果を利用することで, $P = (x_1, y_1), Q = (x_2, y_2)$に対して, $P + 2Q = (x_3, y_3)$は連立方程式

$$\begin{aligned} y_1 &= ax_1^2 + bx_1 + c \\ y_2 &= ax_2^2 + bx_2 + c \\ \frac{3x_2^2 + A}{2y_2} &= 2ax_2 + b \end{aligned}$$

の解a, b, cを用いると

$$x_3 = \frac{1 - 2ab}{a^2} - x_1 - 2x_2$$

$$y_3 = -ax_3^2 - bx_3 - c$$

となることを示した.

この結果を使って Miller のアルゴリズムを計算すると, 256 ビットの Ate ペアリングのコストを 15～17%削減できることを実証した.

⑤ Twisted Edwards 曲線の加算アルゴリズムの改良とペアリングへの応用[発表①, ②,④]

Twisted Edwards 曲線

$$ax^2 + y^2 = 1 + dx^2y^2$$

はスカラー倍を高速に計算でき, 特に$a = -1$の場合, 混合座標系を用いることで加算は 7**M**, 2 倍算は 3**M**+4**S** で計算でき, これらは最も低いコストの楕円曲線の加算と 2 倍算であることが知られている. また, 加算・2 倍算は並列実装も可能である[引用②].

本研究は, 平面上の点(x, y)を$x = X/Z, y = Y/W$を満たすX, Y, Z, Wを使って(X, Y, Z, W)で表現する新しい座標系を導入し, この座標系での twisted Edwards 曲線の加算公式と 2 倍算公式を導出した. 特に$-x^2 + y^2 = 1 + dx^2y^2$に対して, 混合座標系にすることなく, 加算は 7**M** で, 2 倍算は 3**M**+4**S** で計算できる.

BN 曲線は Twisted Edwards 曲線では表現できないことが知られているため, 本研究は twisted Edwards 曲線で表現できるペアリング・フレンドリー曲線の探索手順を提案した.

ペアリング・フレンドリー曲線の探索手順

1. $p \equiv 1 \pmod 6$を満たす素数pに対して, $4p = t^2 + 3s^2$を満たす整数t, sを見つける
2. $n = p + 1 - t$とセットし, $n = 2^k n_1 (n_1$は奇数$)$と表す
3. $i = 0,1, \ldots, k$に対して
   $2^i n_1 \mid ((t-1)^4 - (t-1)^2 + 1)$ (4)
   を満たすiが存在すればステップ 4 へ
   そうでなければ
   $p \leftarrow$次の$p \equiv 1 \pmod 6$
   としてステップ 1 へ
4. p, i, n_1, tを出力
5. トレースtを持つF_p上楕円曲線が twisted Edwards 曲線で与えられるかチェック
6. $p \leftarrow$次の$p \equiv 1 \pmod 6$としてステップ 1 へ

ステップ 5 には次の定理を利用する.

定理 2

pを$p \equiv 1 \pmod{12}$を満たす素数とする. E_1をj-不変数 0 を持つF_p上の楕円曲線とし, そのトレースをt_1とする. $E_{-1/(3\sqrt{3})}: y^2 = x^3 - 1/(3\sqrt{3})$のトレースを$t_{-1/(3\sqrt{3})}$とする. すると, E_1が twisted Edwards 曲線で与えられることの必要十分条件は

$$t_1 = \pm t_{-1/(3\sqrt{3})}$$

が成り立つことである．

この探索手順により，twisted Edwards 曲線で与えられる$F_{188355534529}$上ペアリング･フレンドリー曲線を発見できた．

(2)暗号並列実装[発表③,⑤]

① 共通鍵暗号の並列実装

マルチコア CPU やメニーコア・コプロセッサを使って，電子書籍コンテンツのような数百の複数ファイルを並列に AES 暗号化するためのプログラムを実装し，各ファイルサイズを 128B～4MB とした時の実行時間を評価した．暗号実装の容易性のために OpenSSL 暗号ライブラリを活用した．並列実装基盤として OpenMP や pthread を使用した．

マルチコア CPU や GPU を利用しての AES の並列化の従来研究は，1 ブロックの AES 暗号化の高速化のためのラウンド処理の並列化，または 1 つのファイルの AES 暗号化の高速化のためのブロック単位での並列処理，に分類できる．しかしながら電子書籍のように複数ファイルの暗号化の需要がありメニーコア性を十分に活用するため，本研究では，2 つのディレクトリ名を引数とし，1 つ目のディレクトリに入っているファイルすべてに対して 128 ビット AES によりファイル単位で並列に暗号化または復号し，その結果すべてを 2 つ目のディレクトリに出力するプログラムを実装した．なお，実装実験環境は表 1 で，実装実験パラメータは表 2 で与える．また，並列実装基盤の違いの影響を簡単にまとめると表 3 のようになった．

Intel Xeon Phi サーバ ： Express5800HR120a-1
ホスト CPU ： Intel Xeon E5-2640(6 コア，2.5GHh)×2
コプロセッサ ： Intel Xeon Phi 5110P (60 コア，1.05GHz) ×1
コンパイラ ： インテル C++ Studio XE 2013 Linux 版

表 1: 実装実験環境

パラメータの種類	パラメータの値
使用プロセッサ	Intel Xeon Intel Xeon Phi
ファイル 1 つのサイズ(B)	128，256，512，1K，2K，4K，8K，16K，32K，64K，128K，256K，512K，1M，2M，4M
スレッド数	1，2，4，10，20，50，100

表 2: 実装実験のパラメータ

並列実装基盤	pthread	OpenMP
暗号化関数での malloc 使用	無	有
異常遅延	無	有
暗号化速度	速	遅
最適プロセッサ	Intel Xeon	Intel Xeon

表 3: 異なる並列実装基盤での比較

並列実装基盤に pthread を用いると OpenMP の使用で生じた異常遅延を防ぐことができたが，メニーコア・コプロセッサのコア数に匹敵する処理速度は得られなかった．また，コア数で劣る Intel Xeon の方が Intel Xeon Phi より AES 暗号処理が高速であった．この原因の更なる調査が必要である．

② 楕円曲線暗号の並列実装

楕円曲線暗号の支配的な処理はスカラー倍算であり，暗号化では公開鍵$P \in E$と乱数rからrPを計算する必要がある．公開鍵が冗長鍵$\{P, 2P, 4P, 8P, \ldots\}$として与えられている場合，スカラー倍の並列計算法を考案でき(図 1)，現在はメニーコア・コプロセッサを使用してのスカラー倍の計算速度の上昇率を調査中である．

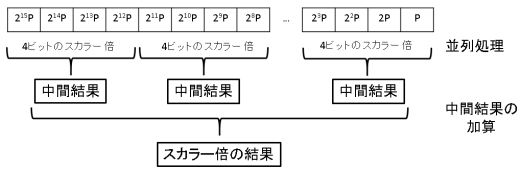


図 1: 冗長鍵によるスカラー倍

＜引用文献＞

① ジム・ジェファース等著，すがわらきよふみ訳，インテル Xeon Phi コプロセッサー，カットシステム．

② H. Hisil et al., Twisted Edwards Curves Revisited, ASYACRYPT2008.

５．主な発表論文等

〔学会発表〕（計　９件）

① Masaaki Shirase, Coordinate System for Elliptic Curve Cryptosystem on Twisted Edwards Curve，ICCE-TW2016，2016 年 5 月 27 日，埔里（台湾）．

② 白勢政明, 埋込み次数 12 と j-不変数 0 を持つ楕円曲線，SCIS2016，2016 年 1 月 22 日，ANA クラウンプラザホテル熊本ニュースカイ（熊本県・熊本市）．

③ 白勢政明，メニーコア・コプロセッサによる複数ファイルの並列共通鍵暗号実装，FIT2015，2015 年 9 月 15 日，愛媛大学城北キャンパス（愛媛県・松山市）．

④ 白勢政明, Edwards 曲線の加算アルゴリズムの改良, ISEC, 2015 年 9 月 4 日, 機械振興会館（東京都・港区）.

⑤ 白勢政明, メニーコア・コプロセッサ XeonPhi での暗号並列実装, CSEC, 2015 年 3 月 5 日, 法政大学小金井キャンパス（東京都・小金井市）.

⑥ 白勢政明, P と 2P の座標に着目する楕円曲線スカラー倍の高速化, SCIS2015, 2015 年 1 月 20 日, リーガロイヤルホテル小倉（福岡県・北九州市）.

⑦ 永井善孝, 2 次曲線を用いたペアリング暗号演算, CSS2014, 2014 年 10 月 22 日, 札幌コンベンションセンター（北海道・札幌市）.

⑧ Yoshitaka Nagai, Elliptic Curve Scalar Multiplication with a Bijective Transform, IMIS2014, 2014 年 7 月 3 日, Birmingham (United Kingdom).

⑨ 白勢政明, 2 次曲線を用いた楕円曲線演算, SCIS2014, 2014 年 1 月 23 日, 城山観光ホテル（鹿児島県・鹿児島市）.

６．研究組織

(1)研究代表者

白勢　政明（SHIRASE, Masaaki）
公立はこだて未来大学・システム情報科学部・准教授
研究者番号：７０５３０７５７