一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
IT2017-11,EMM2017-11(2017-05)

個人認証機能を有するデジタル署名型 QR コード

先名　健一
合同会社 QR テクノロジー　〒195-0055 東京都町田市三輪緑山 1-2-3-109
E-mail:　1729manifold@gmail.com,　sakina@qr-technology.matrix.jp

あらまし　本研究では、最初に、QR コードに楕円曲線デジタル署名アルゴリズムを組み込んだデジタル署名型 QR コード（DSQR コード）を提案している．DSQR コードは認証サーバを用いることなく、オフラインにおいて DSQR コード自身の真偽判定を実現する．次に、個人認証を可能にする修正されたデジタル署名アルゴリズムを提案している．提案アルゴリズムでは、署名値にパスワードを排他的論理和で埋め込むことにより、パスワードの解読が困難になると共に、パスワードの外部記憶媒体保管が不要になる．この提案アルゴリズムを DSQR コードに組み込むことにより、DSQR コードの真正性判定と共に個人認証が可能になる．提案手法を実機に組み込み、その動作性を確認している．最後に、DSQR コードで用いる署名方法は、メッセージ添付型/復元型の両方の特徴をもつデジタル署名であることを示す．
キーワード　QR コード、DSA、ECDSA、個人認証、パスワード

Digital signature type QR code with personal identification function

Ken-ichi Sakina
QR Technology LLC, 1-2-3-109 MiwaMidoriyama, Machida, Tokyo, 195-0055, Japan

Abstract　In this study, we propose a digital signature type QR code (DSQR code) that incorporates an elliptic curve digital signature algorithm into a QR code. The DSQR code makes it possible to determine the authenticity of the DSQR code itself offline without using an authentication server. In addition, we propose a modified digital signature algorithm that enables personal authentication. In the proposed algorithm, it is difficult to decrypt the password because the password is embedded in the signature value with exclusive OR. By incorporating this proposed algorithm into the DSQR code, individual identification can be performed together with authenticity judgment of the DSQR code. We incorporated the proposed method into actual machine and confirmed its effectiveness.
Keywords　QR code, ECDSA, DSA, Personal identification, Password

1．まえがき

QR コード[1]は、当初、工場において部品を管理する目的で開発された二次元コードであるが、近年は様々な用途に広く利用されている．例えば、Web サイトへのアクセスや飛行機の搭乗券、イベント会場の入場チケット、店舗における支払いなどが挙げられる．しかし、QR コードの生成は容易なため、その偽造・改ざんなどの不正も常に発生し得る[2][3][4]．例えば、正規の QR コードの上に他の QR コードを添付して悪意ある Web サイトに誘導するフイッシングやコンサート会場の QR コード付き入場チケットを複製して複数人に売り渡す事件などがある．

上記のような QR コードに関する不正を検知すべく対策も研究されている．その一つに、デンソーウェーブの開発した SQRC がある．これは、QR コードの使用されていないコード語領域（埋め草コード語領域）に挿入された秘密情報を真正性の判定に使う方式で、その判定には認証サーバ等による秘密情報の照合が必要である[5]．また、オフラインにおいて QR コードの認証を試みる研究もある．例えば、QR コードシンボルの下部に QR コードの格納データである URL を記載し、格納データを復号した結果と、OCR で QR コード下部の URL を読み取った結果との比較から不正を検知する方式[6]や Wet Paper 符号[7]を用いた情報ハイディング技術により QR コードの不正を検知する方式[8]などが提案されている．しかしながら、これらのオフライン方式は、付加データの読取りに高い精度が要求されるため、技術的な困難を伴う．また、QR コードの真正性の認証ではないが、２枚の QR コードを使って秘密情報を保護する手法も提案されている[9]．

本研究では、楕円曲線デジタル署名アルゴリズム（以降、ECDSA）或いはその修正アルゴリズム(以降、MECDSA)を用いて、オフラインにおいて QR コードの真正性判定と個人認証の両機能を備える QR コードを

提案する．このような機能を有するQRコードをデジタル署名型QRコード（以降、DSQRコード）と定義する．DSQRコードは、QRコードをベースにしてECDSA、或いはMECDSAによりデジタル署名を作成し、それをQRコードのコード語領域に排他的論理和によって埋め込んだものである．この署名によりDSQRコードに偽造・改ざんがあると、検証のアルゴリズムによって不正が検知される．また、MECDSAを用いると、DSQRコードの真正性とパスワードによる個人認証の両方の検証を同時に行うことができる．

本研究では、DSQRコードの生成アプリとそれを読み取るリーダアプリを作成し、リーダアプリをAndroidスマートフォンに実装した．その結果、汎用のコードリーダと同程度にスムーズに動作すること及びDSQRコードの真正性判定と個人認証の機能が正しく作動することが確認された．なお、DSQRコードを利用したPC間の相互認証も提案している[10].

2．楕円曲線

pを5以上の素数とするとき、有限体$GF(p)$は

$$GF(p)=\{0,1,2,\cdots,p-1\} \tag{1}$$

で与えられる．$GF(p)$上の楕円曲線$E/GF(p)$は、$a,b\in GF(p)$として、

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

を満たす点(x,y)と無限遠点Oとからなる．（2）の形式をWeierstrassの標準形という[11][12]．$GF(p)$上の楕円曲線の$GF(p)$-有理点の集合には楕円曲線に特有の加法と2倍算が定義される(付録参照)．また、楕円曲線上の点Gのk倍（kは正の整数）を

$$kG=\overbrace{G+G+\cdots+G}^{k個} \tag{3}$$

によって定義する．このとき、$nG=O$となるnをGの位数といい、更に、Gを生成元とする巡回群$<G>=\{G,2G,\cdots,(n-1)G,O\}$が構成される．$G$を楕円曲線上のベースポイントといい、$<G>$の各要素は楕円曲線上の点である．ところで、楕円曲線上の離散対数問題（ECDLP）とは、PとQを$<G>$の相異なる任意の要素するとき、

$$Q=kP \tag{4}$$

を満たす整数kを求める問題である．Gの位数nが十分大きいと、（4）を満たすkを算出することは困難である．楕円曲線を使う暗号やデジタル署名ではこの困難性を利用する．

一般に、有限体$GF(p)$上における逆元計算は、乗算と比較して計算コストが高い．（2）の楕円曲線上における2点の和及び点の2倍算の計算には各演算ごとに1回の逆元計算が含まれるため（付録参照)、（3）の計算を行うと$k-1$回の逆元計算が必要になる．そのため、本研究では、アフィン座標系での（2）を射影座標系(X,Y,Z)に変換した

$$Y^2Z=X^3+aXZ^2+bZ^3 \tag{5}$$

を用いる．射影座標系においては楕円曲線上の2点の和及び点の2倍算の計算には有限体上の逆元計算は含まれなく、アフィン座標系への逆変換$(X/Z,Y/Z)$の1回の逆元計算で済む．加えて、点Gの整数倍kGの計算には、2進展開法を用いて計算の高速化を図っている[13].

3．楕円曲線デジタル署名アルゴリズム（ECDSA）

デジタル署名方式は、あるメッセージが偽造・改ざんされていないことを検証する仕組みである．また、この仕組みを利用すると署名したことを後から否認することもできない．デジタル署名には、RSA署名、DSA署名、ECDSA署名などがあるが[11]、本研究では、署名値のサイズを考慮してECDSA署名を採用する．楕円曲線上の離散対数問題はECDSA署名の偽造・改ざんを困難にしている．ECDSAによる署名生成および署名検証は以下のようなプロトコルからなる．

Step1 システムパラメータの設定と鍵の生成

・楕円曲線$E/GF(p)$と素数位数nのベースポイント$G\in E(GF(p))$を定める．

・一方向性ハッシュ関数Hを定める．

・乱数$d\in Z_p^*$を生成して楕円曲線上で

$$Q=dG \tag{6}$$

を計算する．dを秘密鍵、Qを公開鍵とする．

楕円曲線のドメインパラメータとハッシュ関数を併せてシステムパラメータという．なお、公開鍵Qとシステムパラメータは、DSQRコードの生成アプリとリーダアプリで共有する．

Step2 署名生成

乱数$k\in Z_p^*$を生成し、kGのx成分を計算する．

$$c=(kG)_x \bmod n \tag{7}$$

次に、署名したいメッセージmに対して、

$$s=k^{-1}(H(m)+dc) \bmod n \tag{8}$$

$$u = s^{-1} \bmod n \tag{9}$$

を計算し、(c, u) をメッセージ m に対する署名とする.

Step3 署名検証

公開鍵 Q と与えられたメッセージ m 及び署名 (c, u) に対して以下のように検証する.

$$u_1 = H(m)u \bmod n \tag{10}$$

$$u_2 = cu \bmod n \tag{11}$$

$$u_1 G + u_2 Q = (x', y') \tag{12}$$

このとき、$x' = c \pmod n$ が成り立てば、署名を受理し、そうでなければ棄却する.

通常、上記 Step2 の $u = s^{-1} \bmod n$ の計算は署名検証の Step3 に含めるが、署名検証を実行するモバイル端末の計算コストを軽減するために署名生成時に処理する.

4. 修正 ECDSA（MECDSA）

ECDSA は、署名によってメッセージの真正性を検証するものであるが、ここでは ECDSA を若干修正することでパスワードによる個人認証も可能なアルゴリズム MECDSA を提案する. 筆者の知る限り、このようなアルゴリズムは公表されていない.

Step1 パラメータの設定と鍵の生成

ECDSA と同じであるので省略する.

Step2 署名生成

乱数 $k \in Z_p^*$ を生成し、kG の x 成分を

$$c = (kG)_x \bmod n \tag{13}$$

とする. 署名したいメッセージ m に対して、

$$s = k^{-1}(H(m) + dc) \bmod n \tag{14}$$

$$u = s^{-1} \bmod n \tag{15}$$

を計算する. パスワードを p_w とし、c との排他的論理和

$$\tilde{c} = c \oplus p_w \tag{16}$$

を求め、$(\tilde{c}, u)$ を署名とする.

Step3 署名検証

公開鍵 Q と与えられたメッセージ m 及び署名 $(\tilde{c}, u)$ に対して以下のように検証する.

パスワード p_w を入力し、$\tilde{c}$ との排他的論理和

$$c = \tilde{c} \oplus p_w \tag{17}$$

より c を求め、以下の計算をする.

$$u_1 = H(m)u \bmod n \tag{18}$$

$$u_2 = cu \bmod n \tag{19}$$

$$u_1 G + u_2 Q = (x', y') \tag{20}$$

このとき、$x' = c \pmod n$ が成り立てば、入力したパスワード p_w とメッセージ m は共に真正なものと判定し、パスワードを含めた署名を受理、そうでなければ棄却する.

このように、MECDSA の署名検証では、パスワードとメッセージが共に正しいときのみ署名が受理される. 従って、パスワードによる個人認証も可能になる. アルゴリズムから分かるように、パスワードは乱数的に変化する署名値に排他的論理和で埋め込まれているため、署名値からパスワードを解読することはできない. したがって、パスワードの漏洩は原理的に起こり得ない. なお、この MECDSA は、DSA 署名など他のデジタル署名と一般的なメッセージにも利用できる.

5. Reed-Solomon 符号

Reed-Solomon 符号（以降、RS 符号）は、代数幾何符号である Goppa 符号の特別な場合に相当し、バースト誤りの訂正に優れた符号である. RS 符号は、QR コードやコンパクトディスク、無線通信など、情報伝達の信頼性を高めるために幅広く利用されている.

RS 符号は、基礎体 $GF(2)$ の m 次のガロア拡大体 $GF(2^m)$ 上で定義される最大距離分離符号である[14]. QR コードの場合は $m = 8$ であるので、符号長 n は $n = 2^8 - 1 = 255$ シンボルとなるが（1 シンボル＝8 ビット）、QR コードでは情報シンボル数を少なくして短縮された RS 符号を使用している. RS 符号の復号には、アルゴリズムの分かり易い Euclid 復号法[15]がよく用いられる. 実際、Google のオープンソースライブラリ ZXing[16]では、2 次元コードリーダに Euclid 復号法が使われている. 受信した RS 符号語（受信語）には一般に情報伝達に伴う誤りが存在し得る. このとき、誤り訂正可能な範囲の誤りであれば、復号アルゴリズムを実行することにより、誤り位置と誤り値が正確に求められ、情報は正しく復元される.

6. DSQR コードの生成と認証

6.1 ベースとなる QR コード

本研究で使用する QR コードは 7 H 型で、符号長 39 バイトの RS 符号語が 4 つと符号長 40 バイトの RS 符号語が 1 つから構成されており、格納できる情報データ量は 66 バイトまでとなっている. また、誤り訂正可能なバイト数は、各符号語とも 13 バイトであるので、コード全体では 65 バイトまでの誤り訂正が可能であ

る．

図１は、「合同会社 QR テクノロジー」を情報データとして格納している QR コードである．QR コードのもつ誤り訂正能力により、QR コードの汚れや破損などのために読取り誤りがあるときでも一定範囲の誤りであれば正しい情報データに復元される．H 型の QR コードは最大約 30%の誤りを訂正するが、スマートフォンを使用した実際の読取りでは高々数%の読取り誤りしか発生しなく、PC のリーダアプリに至っては読取りは殆ど発生しない．そのため、使用されない誤り訂正能力は他の処理に使うことが可能である．

図１　QR コード

6.2 署名生成（パスワードなし）

6.1 で生成した QR コードにおいて、情報データをビット系列に変換し、それを適当に分割して生成したベクトルを $\mathbf{m}_i$ $(i=1,\cdots,5)$ で表す．また、RS 符号の生成行列を G とするとき、各符号語ベクトル $\mathbf{w}_i$ $(i=1,\cdots,5)$ は、

$$\mathbf{w}_i = \mathbf{m}_i G \qquad (i=1,\cdots,5) \tag{21}$$

より求められる．

いま、$\mathbf{w}_i$ $(i=1,\cdots,5)$ を連接して得られるビット系列を

$$m = \mathbf{w}_1 \| \mathbf{w}_2 \| \cdots \| \mathbf{w}_5 \tag{22}$$

とおく．これはデジタル署名対象のメッセージに相当する．

ここでは、第３節の ECDSA の Step2 に従って QR コードのデジタル署名を生成する．図２は署名に使用する楕円曲線のドメインパラメータ secp160r1 である [17]．このドメインパラメータは、DSQR コード生成アプリとリーダアプリで共通に使用する．まず、乱数 $d \in Z_p^*$ を生成して、$Q = dG$ を求め、d を秘密鍵、Q を公開鍵とする．次に、乱数 $k \in Z_p^*$ を生成し、式（７）より署名値の一つ、c を算出する．更に、一方向性ハッシュ関数 SHA-1 を用いて、式（２２）の m に対するハッシュ値 $H(m)$ を求め、式（８）、（９）よりもう一つの署名値 u を算出する．このようにして算出した数値例を以下に示す．

---------- 数値例 ----------

秘密鍵：(160bit)
ff0fb952558e37c8a8ce3f589523350017be0e6
公開鍵：(160bit×2)
9ad905eed902a1c9e35ec50252d6cf99aa96517c,
4712b4cf8457c1700e9f6a575b166549fbe2996b
署名値: (160bit×2)
c = fe9788850eeac0f6e062b05ba0fad9ea061fa161
u =343842430d451cc121f7cad10523cdf7c5aa52e3

[**secp160r1** のドメインパラメータ]
p =FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF7FFFFFFF
a =FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF7FFFFFFC
b =1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
・楕円曲線のベースポント G の x 成分と y 成分：
4A96B5688EF573284664698968C38BB913CBFC82,
23A628553168947D59DCC912042351377AC5FB32
・G の位数（素数）：
n =1000000000000000000001F4C8F927AED3CA752257

図２　楕円曲線のドメインパラメータ

6.3 DSQR コードの生成

6.2 で生成した 160bit×2(=40Byte)のデジタル署名値 (c,u) を図１の QR コードに排他的論理和で埋め込む．まず、署名値の連接 $c \| u$ のビット系列表現を適宜分割し、$\mathbf{w}_i$ の次元と同じになるように、0 をパディングしてベクトル $\mathbf{v}_i (i=1,\cdots,5)$（以降、署名ベクトル）をつくる．次に、式（２１）と署名ベクトルとの排他的論理和をとり、

$$\mathbf{w}'_i = \mathbf{m}_i G \oplus \mathbf{v}_i \qquad (i=1,\cdots,5) \tag{23}$$

とおく．$\mathbf{w}'_i$ は符号語に署名値を埋め込んだベクトルになっていて、$\mathbf{v}_i (i=1,\cdots,5)$ は誤りに相当する．

このようにして得られた $\mathbf{w}'_i (i=1,\cdots,5)$ を QR コードの符号語 $\mathbf{w}_i$ $(i=1,\cdots,5)$ と置換して生成される QR コードを DSQR コードと定義する．図３は、以上のようにして生成された DSQR コードである．

ここでは、ベースとなる２次元コードを QR コードに限定しているが、DataMatrix などの２次元コードでもよい．

情報データ: 合同会社 QR テクノロジー
短縮 URL: https://goo.gl/2cw7ZI
ECDSA 署名値:
fe9788850eeac0f6e062b05ba0fad9ea061fa161,
343842430d451cc121f7cad10523cdf7c5aa52e3

図３　DSQR コードと ECDSA 署名値の例

6.4 DSQR コードの読取り

DSQR コードをリーダアプリで読み取り、受信語

$\mathbf{w}'_i$ $(i=1,\cdots,5)$を取得する．各受信語を Euclid 復号アルゴリズムを用いて復号して、符号語 $\mathbf{w}_i$ $(i=1,\cdots,5)$と署名ベクトル $\mathbf{v}_i$ $(i=1,\cdots,5)$ を求める．符号語からは、情報データである「合同会社 QR テクノロジー」が復元される．

6.5 DSQR コードの認証

6.4 で得られた符号語 $\mathbf{w}_i$ $(i=1,\cdots,5)$と署名ベクトル $\mathbf{v}_i$ $(i=1,\cdots,5)$を用いて、第３節の ECDSA の Step3 を実行する．

最初に、取得した符号語を連接して

$$m' = \mathbf{w}_1 \| \mathbf{w}_2 \| \cdots \| \mathbf{w}_5 \tag{24}$$

をつくり、ハッシュ値 $H(m')$を計算する．次に、署名ベクトルから算出した署名値(c,u)を用いて、式（１０）～式（１２）を計算し、x'を求める．このとき、$x' = c \pmod{n}$が成り立てば、この DSQR コードの正規性が認証されたことになる．

実際に、DSQR コードリーダアプリが挿入されたスマートフォンで DSQR コードを読み取ると、「**DSQR コード認証 YES**」及び正規の短縮 URL が表示される．

上記の DSQR コードの認証においては公開鍵を使用しているが、この公開鍵は認証局（CA）によって証明されたものではない．

また、DSQR コードを用いると署名生成者（発行者）が署名検証者（認証者）にもなっている簡易公開鍵基盤（SPKI）[18]を実現することができる．なお、CA によって証明された公開鍵を用いれば PKI も構築できる．

6.6 メッセージ添付/復元型デジタル署名方式

デジタル署名には、メッセージ添付型署名方式とメッセージ復元型署名方式の二通りがあるが[11]、DSQR コードに使われている署名方式は、誤り訂正符号語にデジタル署名を埋め込むというもので、メッセージ添付型とメッセージ復元型の両方の方式に属するタイプである．すなわち、署名を符号語の一部分に埋め込む点でメッセージ添付型であり、他方、その埋め込まれた部分が秘匿化され、検証時に復元するという点ではメッセージ復元型である．筆者の知る限り、このようなハイブリッド的な署名方式は公表されていない．

DSQR コードの署名方式は、2 次元コードに限らず、どのような利用形態の誤り訂正符号にも適用できるため、一般的なメッセージ添付/復元型の署名方式と言える．

7. 個人認証付き DSQR コード

ここでは、個人のパスワードを取り込んで個人認証が可能な DSQR コードの生成と認証について第４節の MECDSA を基に述べる．DSQR コードとの違いは、署名の生成部分と認証部分だけである．

7.1 署名生成（パスワードあり）

6.2 で生成したデジタル署名(c,u)に対して、パスワード p_w と c との排他的論理和

$$\tilde{c} = c \oplus p_w \tag{25}$$

を求め、$(\tilde{c},u)$ を署名とする．次に、その署名値の連接 $\tilde{c}\|u$ をビット系列で表し、6.3 と同じように連接から署名ベクトル $\mathbf{v}_i(i=1,\cdots,5)$を生成する．後は 6.3 と同じ手順で個人認証機能を有する DSQR コードが生成される．図４に DSQR コード（パスワードあり）の実例を示す．

7.2 DSQR コードの認証（パスワードあり）

DSQR コードをリーダアプリで読み取り、受信語 $\mathbf{w}'_i$ $(i=1,\cdots,5)$から符号語 $\mathbf{w}_i$ $(i=1,\cdots,5)$と署名ベクトル $\mathbf{v}_i$ $(i=1,\cdots,5)$ を取得する．署名ベクトルから署名 $\tilde{c}$ を抽出し、入力されたパスワード P_w との排他的論理和

$$c = \tilde{c} \oplus p_w \tag{26}$$

により署名値の一つ、cを算出する．そして、MECDSA の署名検証アルゴリズム Step3 に従って、$x' = c \pmod{n}$が成り立つか検証する．もし、成り立てば、パスワードと署名対象のメッセージが共に真正である．このとき、秘密情報が表示される．

情報データ: 合同会社QRテクノロジー
MECDSA 署名値:
f645350fc95f5e1b7aed61f8ee3cbd00a
e3b6f42,19a806b81ad6206abcaed34d
90ec617fe3188241
パスワード: 1234abc
(秘密情報)
短縮 URL: https://goo.gl/2cw7ZI

図４　DSQR コードと MECDSA 署名値の例

8. まとめ

ECDSA を QR コードに適用したデジタル署名型 QR コード（DSQR コード）を提案し、実機によってその有効性を確認した．また、デジタル署名アルゴリズムを修正することによって、パスワード等による個人認証も可能になるアルゴリズム MECDSA を提案し、実機によってその有効性を確認した。MECDSA は、パスワードを外部記憶媒体に保管する必要がないため、パスワードの漏洩を防ぐ一つの方式になる．最後に、誤り訂正符号とデジタル署名の組み合わせによるメッセージ添付/復元型の署名方式を提案した．この方式を用いると、メッセージの部分秘匿とメッセージ全体の

認証が同時に可能になる.

付　録

アフィン座標系における楕円曲線を

$$y^2 = x^3 + ax + b \quad (4a^3 + 27b^2 \neq 0) \qquad \text{(a-1)}$$

とする.

A1. 2点の和

楕円曲線上の2点を $P(x_1, y_1)$、$Q(x_2, y_2)$ とするとき、その2点の和 $P+Q$ の座標 (x_3, y_3) は次式で与えられる $(P \neq \pm Q)$:

$$x_3 = \lambda^2 - x_1 - x_2 \qquad \text{(a-2)}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \qquad \text{(a-3)}$$

ただし、$\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

A2. 点の2倍

楕円曲線上の点 $P(x_1, y_1)$ を2倍した点 $2P$ の座標を (x_3, y_3) とすると、

$$x_3 = \lambda^2 - 2x_1 \qquad \text{(a-4)}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \qquad \text{(a-5)}$$

ただし、$\lambda = \dfrac{3{x_1}^2 + a}{2y_1}$.

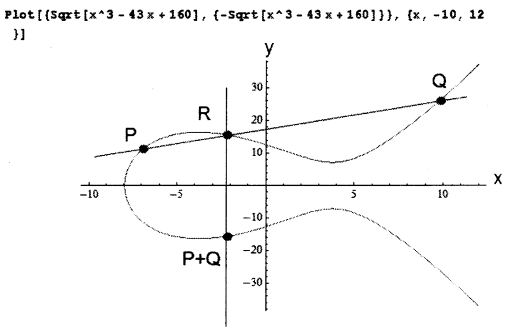

図5　楕円曲線上の2点の和

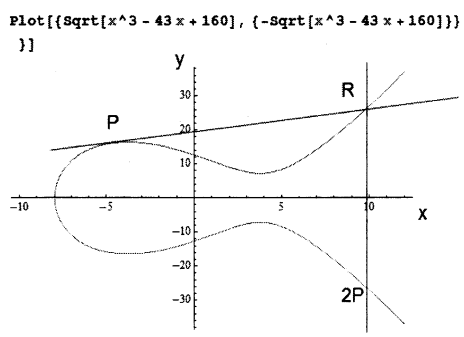

図6　楕円曲線上の点の2倍

文　献

[1] JIS X 0510, "二次元コードシンボル-QR コード-基本仕様," 日本規格協会, 2004.

[2] https://www.owasp.org/index.php/Qrljacking

[3]http://thehackernews.com/2016/07/qrljacking-hacking-qr-code.html

[4] https://goo.gl/B2XRvf　(SankeiBiz 2017.4.10 記事)

[5] 特開 2008－299422 (デンソーウェーブ)

[6] 柏井祐樹, 渡辺優平, 森井昌克, "オフラインサイト認証可能な QR コード," 第 11 回情報科学技術フォーラム(FIT2012), pp.107-112, 2012

[7] J. Fridrich, M.Goljan, and D.Soukal, " Wet paper codes with improved embedding efficiency," IEEE Transactions on Information Security and Forensics, vol.1,pp.102-110,2006

[8] 新見道治, 野田秀樹, "Wet Paper 符号と情報ハイディングを利用した QR コードの改ざん検出," 電気関係学会九州支部連合大会, p.148, 2012

[9]本庄俊太郎、古賀弘樹," 2 枚の二次元コードを用いた秘密分散法の一実現法," 電子情報通信学会論文誌 A, vol.J98-A,No.2, pp.221-231, 2015.

[10]先名健一, "DSQR コードを利用した Web システムにおける相互認証," 情報処理学第 78 回全国大会,pp.499-500, 2016

[11]宮地充子, "代数から学ぶ暗号理論,"日本評論社,2012

[12]J.H.シルヴァーマン、J.テイト,"楕円曲線論入門," 丸善出版,2012

[13]I.F.ブラケ、他,"楕円曲線暗号," ピアソン・エデュケーション,2001

[14]先名健一、"例題で学ぶ符号理論入門," 森北出版,2011

[15]平澤茂一、笠原正雄,"ユークリッド復号法,"IEICE Fundamentals Review Vol.4, No.3,2011

[16] https://github.com/zxing/zxing

[17] http://www.secg.org/
SEC2: Recommended Elliptic Curve Domain Parameters, Version 1.0

[18] https://tools.ietf.org/html/rfc2693