



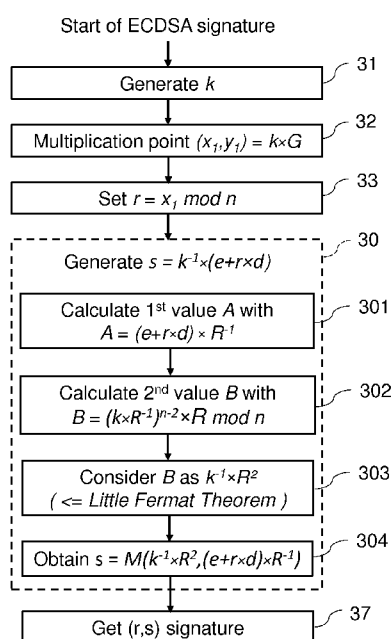
- (51) **International Patent Classification:**
H04L 9/32 (2006.01) *G06F 7/72* (2006.01)
- (21) **International Application Number:**
PCT/EP2017/068683
- (22) **International Filing Date:**
24 July 2017 (24.07.2017)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
16305978.5 28 July 2016 (28.07.2016) EP
- (71) **Applicant:** GEMALTO SA [FR/FR]; 6 Rue de la Verrerie, 92190 MEUDON (FR).
- (72) **Inventors:** SINARDI, Guntur; GEMALTO SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR). BEN YOUSSEF, Tarek; GEMALTO SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR).
- (74) **Agent:** LOTAUT, Yacine; GEMALTO SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) **Title:** EFFICIENT ECDSA SIGNATURE AND VERIFICATION**FIG.3**

(57) **Abstract:** The verification and signature processes of the cryptosystem Elliptic Curve digital Signature Algorithm (ECDSA) require an efficient implementation of modular multiplication. Montgomery modular multiplication consists in replacing division by an arbitrary number with division by a fixed number. Montgomery multiplication requires costly pre-computation of a constant R^2 to change the representation of the operands from scalar representation to Montgomery representation. Embodiments propose a faster method for performing ECDSA verification and signature processes using the Montgomery multiplication, which avoids the costly pre-calculation of the Montgomery constant R^2 , by making use of the Montgomery multiplication properties and little Fermat theorem.

EFFICIENT ECDSA SIGNATURE AND VERIFICATION

BACKGROUND**Technical Field**

- 5 The present invention relates to an Elliptic Curve Digital Signature Algorithm (ECDSA) signature and verification algorithm in Elliptic Curve Cryptography (ECC) over prime field.

Related Art

- The approaches described in this section could be pursued, but are not necessarily approaches that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, the approaches described in this section are not prior art to the claims in this application and are not admitted to be prior art by inclusion in this section.

- ECDSA is an algorithm of numerical signature using a public and private key. The public key is accessible to everybody, and everybody can check the integrity of the message and the authenticity of the entity that has been sent.

- This algorithm uses the concepts of Elliptic Curve Cryptography. To use ECC, the emitting and receiving parties must agree on all the elements defining the elliptic curve, that is, the domain parameters of the scheme. The field is defined by a prime integer n , in the case of ECC over prime field. The curve is defined by a series of points having coordinates x and y which satisfy the equation $y^2 = x^3 + ax + b$. The elliptic curve is thus defined by the constants a and b used in its defining equation. Each couple of coordinates (x, y) is an element of the underlying field, as each point of the curve is defined by a pair of field elements.

- ECDSA works with a private key scalar d , and the clear text message m . The output is a bi-dimensional signature (r, s) , wherein the component r and s of the signature are integers. There is further defined n as the Curve Order, which is a prime number, and G as the Generator point of the Elliptic Curve.

Considering that Alice wants to sign a message m using the ECDSA algorithm to Bob, Alice shall use a pair of keys (d, Q) , where d is the private key and Q is the public key. The public Q is obtained according to the following process:

- an integer k is chosen within the range between 1 and $n-1$;
- 5 - there is calculated $Q - kP$ where Q is the public key and P is a point of the elliptic curve $E(K)$ of prime order n , where K is a finite corps; and,
- the private key d is given by $s \cdot \log_P(Q) \bmod n$.

In the above, and throughout the following specification, the vocable « $\bmod n$ » stands for « *modulus n* ». The logarithm guarantees the difficulty to find the
10 private key d knowing the public key Q .

Let us first present the ECDSA signature process.

A digital signature is a bi-dimensional value which allows the recipient of a message to verify the message's authenticity using the authenticator's public key.

To digitally sign a message m , the following steps are performed:

- 15 1. Select a random integer k , such that $1 \leq k \leq n-1$
2. Compute $k \times G = (x1, y1)$ and $r = x1 \bmod n$.
If $r = 0$ then go back to step 1.
3. Then compute $k^{-1} \bmod n$.
4. Further, compute $e = \text{SHA-1}(m)$ where SHA is a hash function that
20 converts the variable length message to a fixed-length message digest.
A secure hash function does have the following distinctive properties:
 - Irreversibility: it is computationally infeasible to determine the message from its digest
 - Collision resistance: it is impractical to find more than one message
25 that produces a given digest
 - High avalanche effect: any change in the message produces a significant change in the digest
5. Finally, compute $s = k^{-1}(e + d \times r) \bmod n$.
If $s = 0$ then go back to step 1.

The signature of the message is composed of the couple of integers (r,s) .

Let us now turn to the ECDSA verification process.

The purpose of the verification process is to verify the message's authenticity using the authenticator's public key. Using the same secure hash algorithm as in
 5 the signature process, the message digest signed by the authenticator is computed. This digest, along with the public key $Q(x,y)$ and the digital signature components r and s , leads to the result.

More precisely, the following steps are performed:

1. First verify that r and s are integers within the interval $[1;n-1]$
- 10 2. If so, then compute $e = SHA-1(m)$
3. Compute $w = s^{-1} \bmod n$
4. Compute $u_1 = e \times w \bmod n$ and $u_2 = r \times w \bmod n$
5. Then compute $X = u_1G + u_2Q$
6. Further compute $v = x_1 \bmod n$ where $X = (x_1, y_1)$
- 15 7. Finally, accept the signature as valid if, and only if $v = r$.

The Montgomery Multiplication is widely used to speed-up the modular arithmetic calculation in both the signature and verification processes as presented above. More specifically, it is used for the calculation of the inverse k^{-1} and s^{-1} , respectively. The Montgomery Multiplication between any values x and y is
 20 defined as $M(x,y) = x \times y \times R^{-1} \bmod n$, or simply $x \times y \times R^{-1}$. The Montgomery Constant is denoted by $R^2 \bmod n$, where R is coprime with n . This constant is needed to change from normal form to Montgomery form. Indeed, for any value x , the "Montgomery form of x " is given by $x \times R \bmod n$ or simply $x \times R$.

Thus, the methods known in the current state of the art need to precompute R^2 to
 25 be able to get the Montgomery form. However, precomputing the constant R^2 is a costly operation in terms of calculation power and memory space needed.

SUMMARY

The present invention proposes an improved method that avoids the calculation of R^2 and thus simplify the calculations carried out in the ECDSA signature and verification processes.

- 5 To that end, there is proposed to use exponentiation based on Montgomery multiplications, which can be noted ME for the purpose of the following explanation. For any integer “a” converted in the Montgomery form $a.R \bmod n$ and for an exponent “e”, the exponentiation ME to the power e would result in $ME(a.R \bmod n, e) = a^e \times R \bmod n$. One important observation is that the result of
- 10 the exponentiation is already the Montgomery form of a^e .

- In embodiments of the signature scheme according to the invention, there is used the same exponentiation based on Montgomery multiplications ME applied as $ME(k, n-2)$, where “k” can be further written as “ $k \times R^{-1} \times R$ ” and thus the above “a” is just equal to “ $k \times R^{-1}$ ”. It can then be deduced $ME(k, n-2) = (k \times R^{-1})^{n-2} \times R \bmod n$
- 15 $= k^{-1} \times R^2 \bmod n$ since n is prime. The one with ordinary skills in the art will appreciate that no conversion to Montgomery is needed and no multiplication by R is needed. The improvement is thus achieved by simply injecting “k” in the exponentiation based on Montgomery multiplications (ME).

- Further, the same method is applied in embodiments of the verification scheme
- 20 according to the invention, where “k” is replaced by “s”.

Indeed, according to a first aspect, there is proposed a cryptographic method comprising an Elliptic Curve Digital Signature Algorithm (ECDSA) signature scheme comprising:

- generating a bi-dimensional signature (r, s) having a first signature component r
- 25 and a second signature component s , said bi-dimensional signature (r, s) being associated to a message m ,

wherein generating the bi-dimensional signature (r, s) comprises:

- generating a random number k ;

- obtaining a bi-dimensional value (x_1, y_1) having a first component x_1 and a second component y_1 , and corresponding to $k \times G$, where G is a bi-dimensional generator point of the elliptic curve;

5 - setting r to x_1 modulus n , where n is a prime number corresponding to the elliptic curve order;

- generating s as $k^{-1} \times (e + r \times d)$, where k^{-1} is the inverse of k , where d is a private key scalar number and where e equals $H(m)$ with H being a hash function, said generating comprising :

10 - calculating a first value $(e + r \times d) \times R^{-1}$ by the addition of the Montgomery multiplication of r and d modulus n , to the Montgomery multiplication of e and unity modulus n ;

- calculating a second value $(k \times R^{-1})^{n-2} \times R$ as the exponentiation of the Montgomery form of $k \times R^{-1}$ to the power $n-2$ modulus n , and thus obtaining $k^{-1} \times R^2$ as said second value because this second value is mathematically
15 equivalent to $k^{-1} \times R^2$ as a result of Fermat's little Theorem,

- obtaining s by calculating the Montgomery multiplication between the second value $k^{-1} \times R^2$ and the first value $(e + r \times d) \times R^{-1} \bmod n$.

A second aspect of the invention relates to a computer program product comprising one or more stored sequences of instructions that are accessible to a
20 processor and which, when executed by the processor, cause the processor to carry out the steps of the method of the above first aspect.

A third aspect of the invention relates to a cryptographic system comprising:

- an interface unit for receiving a message m and for outputting a bi-dimensional signature (r, s) associated to said message m ; and,
25 - a computer unit adapted to generate the bi-dimensional signature (r, s) using an Elliptic Curve Digital Signature Algorithm (ECDSA) signature scheme according to the above first aspect.

A fourth aspect of the invention relates to a cryptographic method comprising an Elliptic Curve Digital Signature Algorithm (ECDSA), verification scheme,

wherein the verification scheme comprises:

- receiving a bi-dimensional signature (r,s) having a first signature component r and a second signature component s , said bi-dimensional signature (r,s) being associated to a message m ;
- 5 - generating the Montgomery form of s^{-1} , where s^{-1} is the inverse of s , said generating comprising:
 - calculating a first value $(s \times R^{-1})^{n-2} \times R$ as the exponentiation of the Montgomery form of $s \times R^{-1}$ to the power $n-2$, where n is a prime number corresponding to the elliptic curve order and R is a given number coprime
 - 10 with n , with $R^2 \bmod n$ being the Montgomery Constant, and thus obtaining $s^{-1} \times R^2$ as said first value because said first value is mathematically equivalent to $s^{-1} \times R^2$ thanks to Fermat's little Theorem,
 - calculating the Montgomery Multiplication of the reduced first value $s^{-1} \times R^2$ with the unity, to obtain a second value $s^{-1} \times R \bmod n$,
- 15 - calculating a third value u_1 as the Montgomery multiplication between the second value $s^{-1} \times R$ and $e \bmod n$, where e equals $H(m)$ with H being a hash function; and
- calculating a fourth value u_2 as the Montgomery multiplication between the second value $s^{-1} \times R$ and the first signature component $r \bmod n$, and
- 20 - calculating a bi-dimensional value (x_1, y_1) having a first component x_1 and a second component y_1 , and corresponding to the addition of $u_1 \times G$ and $u_2 \times Q$, where G is a bi-dimensional generator point of the elliptic curve and Q is a public key point which equals $d \times G$, with d being a private key scalar number; and,
- determining that the signature is valid if the first component value $x_1 \bmod n$
- 25 of the bi-dimensional value (x_1, y_1) equals r .

A fifth aspect of the invention relates to a computer program product comprising one or more stored sequences of instructions that are accessible to a processor and which, when executed by the processor, cause the processor to carry out the steps of the method according to the above fourth aspect.

Finally, a sixth aspect of the invention relates to a cryptographic system comprising:

- an interface unit for receiving a bi-dimensional signature (r,s) associated to a message m ; and,
- 5 - a computer unit (30) adapted to determine whether the signature (r,s) is valid using an Elliptic Curve Digital Signature Algorithm (ECDSA) signature scheme according to the fourth aspect.

As will become more apparent from the description of preferred embodiments which will be provided below, the proposed method uses the inverse Montgomery
10 form to generate the ECDSA signature, and proceed with ECDSA verification without calculating the constant R^2 . The approach essentially consists in modifying the algorithm embedded in smart card, for instance, in order to take advantage of the Montgomery multiplication properties so as to render the pre-computation of the constant R^2 useless.

- 15 Embodiments of the invention are expected to significantly reduce the delay of calculation methods for the signature and verification processes, since the heavy calculation of R^2 is not needed anymore.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention are illustrated by way of example, and not
20 by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to same or similar elements, and in which:

- Figure 1 is a flow chart illustrating steps of a signature process according to the prior art;
- Figure 2 is a flow chart illustrating steps of a verification process according
25 to the prior art;
- Figure 3 is a flow chart illustrating steps of a signature process according to embodiments of the first aspect of the present invention;
- Figure 4 is a flow chart illustrating steps of a verification process according to embodiments of the fourth aspect of the present invention; and,

- Figure 5 is a block diagram of an embodiment of cryptographic systems according to the third aspect and the sixth aspect of the invention, which are adapted to run computer program products according to the second aspect and to the fifth aspect of the invention, respectively.

5

DESCRIPTION OF PREFERRED EMBODIMENTS

To get the signature and its verification using ECDSA in ECC over prime field, order of the Generator Point (also called Curve Order n , which is a prime number) is used as a modulus in a significant part of the calculation. The Montgomery Multiplication is a widely used method allowing to speed-up arithmetic operations
 10 such as the inversion of a given variable. Indeed, modular inversion using Montgomery Multiplication is faster than the standard, *i.e.* scalar inversion.

The problem with Montgomery Multiplication is the need to precompute a constant $R^2 \bmod n$, commonly denoted by R^2 . This constant is needed for computing the conversion of the operand from normal form to Montgomery form, and vice versa.

15 With reference to the flow chart of **Figure 1**, a method of calculating the signature of a clear text message e according to standard algorithm using the Montgomery comprises the following steps.

At 11, a random integer k is generated.

At 12, the bi-dimensional value (x_1, y_1) is obtained through the calculation of $k \times G$,
 20 where G is the bi-dimensional generator point of the elliptic curve.

At 13, calculation of r is performed by equating r with $x_1 \bmod N$.

At 14, the constant R^2 is calculated in order to be able to switch from normal representation to Montgomery representation.

At 15, the modular inversion of k is generated.

25 At 16, the component s of the signature is calculated by $s = k^{-1}(e + rd)$.

Finally, at 17, the elements r and s of the signature are made available to, *e.g.* the application program which shall use them.

With reference to the flow chart of **Figure 2** the basic steps of a method of ECDSA verification according to the prior art comprises the following steps.

At 21, first, the calculation of R^2 is performed.

Then, at 22, the modular inversion of s is calculated.

At 23, there is performed the calculation of u_1 which equals $s^{-1} \times e$, and of u_2 which is equal to $s^{-1} \times r$.

- 5 The calculation of the elements (x_1, y_1) is executed at 24. More precisely, (x_1, y_1) equals to $u_1 G + u_2 Q$.

Finally, at 25, the signature is validated if and only if the first component value x_1 modulus N of the bi-dimensional value (x_1, y_1) equals r .

- 10 Now, the pre-computation of R^2 at step 11 of the ECDSA signature generation scheme and at step 21 of the ECDSA verification scheme is a costly operation.

Embodiments of the present invention allow proceeding without the need for the calculation of R^2 by using nice properties of Montgomery form and the Montgomery multiplication along with the little Fermat theorem.

- 15 By thus avoiding the calculation of R^2 , embodiments lead to faster ECDSA signature and verification schemes.

Referring to **Figure 3**, there is shown therein a flow chart illustrating steps of the signature process according to embodiments of the first aspect of the present invention.

- 20 First steps 31, 32 and 33 of the method are identical to steps 11, 12 and 13, respectively, of the method according to the prior art as shown in Figure 1 and described in details above. Namely, at 31 a random number k is generated, at 32 the bi-dimensional element (x_1, y_1) is obtained by setting $(x_1, y_1) = k \times G$, and at 33 the first signature component r of the signature (r, s) is obtained by the following equating : $r = x_1 \bmod n$. Steps 31 to 33 will not be described again in more details
25 here.

The process then goes on with step 30 which, compared to the process as shown in Figure 1, replaces step 16, along with previous step 15 of modular inversion of k using the Montgomery multiplication and, above all, along with the heavy step 14 of pre-calculation of the constant R^2 .

At 30, indeed, step 30 with sub-steps 301 to 305 are performed to obtain $s = k^{-1} \times (e + r \times d)$ instead of steps 14 and 15 of the method according to prior art as previously described with reference to Figure 1.

The proposed method is based on the following observations.

- 5 First, the second signature component s can be written as the Montgomery form of $s \times R^{-1}$, since $s = s \times R^{-1} \times R$.

Second, considering the Montgomery Multiplication and Exponentiation by Squaring method, it can be observed that the exponentiation of « Montgomery form of $s \times R^{-1}$ » to the power $n-2$ equals to « Montgomery form of $(s \times R^{-1})^{n-2}$ ».

- 10 Finally, Fermat's little theorem states that if n is a prime number, then for any integer a , we have $a^{n-2} = a^{-1}$.

If a is not divisible by n , Fermat's little theorem is equivalent to the statement that a^{n-1} is an integer multiple of n , meaning that $a^{n-1} \equiv 1 \pmod{n}$. This further implies that $a \times a^{n-2} \equiv 1 \pmod{n}$. This also means that a^{n-2} is actually the inverse of a modulus n .

Hence, provided that n is prime, one can opt to raising any value to the exponent $n-2$ whenever one needs to calculate its inverse modulus n .

Here, and since n is prime, the little Fermat theorem provides that $(s \times R^{-1})^{n-2} \times R$ equals to $(s \times R^{-1})^{-1} \times R$.

- 20 Hence, $s^{-1} \times R^2$ is obtained because the above product can be reduced to $s^{-1} \times R^2$ by calculating $(s \times R^{-1})^{-1} \times R = s^{-1} \times R \times R = s^{-1} \times R^2$. Stated otherwise, $(s \times R^{-1})^{n-2} \times R$ is equivalent to $s^{-1} \times R^2$.

- In addition, $M(s^{-1} \times R^2, 1) = s^{-1} \times R$. Hence, the Montgomery form of $s^{-1} \pmod{n}$ can be obtained by calculating the Montgomery multiplication between $s^{-1} \times R^2$ and unity, namely the Montgomery multiplication of $s^{-1} \times R^2$ with 1.

In view of the above observations, step 30 of calculating s comprises the following steps 301 to 304.

At 301, the computation of a first value A is performed with $A = (e + r \times d) \times R^{-1}$. This can be achieved, according to embodiments, by adding $M(r, d) = r \times d \times R^{-1}$ and

$M(e,1) = e \times R^{-1}$. Stated otherwise, $(e+r \times d) \times R^{-1}$ is obtained by the addition of the Montgomery multiplication of r and d modulus n on one hand to the Montgomery multiplication of e and unity modulus n on the other hand.

At 302, there is calculated a second value B , with $B = (k \times R^{-1})^{n-2} \times R \bmod n$ as the exponentiation of the Montgomery form of $k \times R^{-1}$ to the power $n-2$ modulus n . B is equivalent to $k^{-1} \times R^2$, as a result of Fermat's little theorem and thus, at 303, B is considered as being $k^{-1} \times R^2$. The one with ordinary skills in the art will appreciate that, so to speak, 303 is a virtual step which is illustrative for the purpose of clarity of the present disclosure only, in the sense that it does not comprise any additional calculations.

At 304, s is eventually obtained by calculating the Montgomery multiplication between the value B , namely $k^{-1} \times R^2$, which has been obtained at 304, and the first value A which has been obtained at 301, namely $(e+r \times d) \times R^{-1} \bmod n$.

Finally, the Signature process ends at 37 with the output of the bi-dimensional signature (r,s) associated to the encrypted message m . Step 37 is equivalent to step 17 of Figure 1. This result is thus achieved without the constant R^2 having been computed as such, contrary to what is done in the prior art.

There will now be described steps of a Verification process according to embodiments of the present invention, with reference to **Figure 4**. This process aims at verifying the signature (r,s) associated to an encrypted message m . This process can be carried out at a recipient level, where the message m is received and is checked for validity.

At 40, the Montgomery form $s^{-1} \times R$ of s^{-1} modulus n is calculated. This can be achieved, according to embodiments of the fourth aspect of the present invention, by carrying out the following step 401, 402 and 403.

The goal of this step is to obtain the Montgomery form of s^{-1} without the drawback of having to pre-compute the Montgomery constant R^2 as in the prior art.

Similar with ECDSA Signature as described in much details above with reference to step 30 of Figure 3, s can be written as $s \times R^{-1} \times R$. Further, by performing the same inversion method on s itself (similar to the computation of k^{-1} in the above

described ECDSA Signature process), a first value D corresponding to the Montgomery form of $s \times R^{-1}$ raised at the power $n-2$ modulus n is obtained at 401.

Then, at 402, the first value D ($s \times R^{-1}$) ^{$n-2$} $\times R$ is considered in the form $D = s^{-1} \times R^2$ thanks to Fermat's little theorem. , 402 is a virtual step which is illustrative for the purpose of clarity of the present disclosure only, in the sense that it does not comprise any additional calculations.

Hence, $s^{-1} \times R$ is obtained at 403 by computing the Montgomery multiplication $M(s^{-1} \times R^2, 1)$ of $s^{-1} \times R^2$ with unity.

Once $s^{-1} \times R$ is thus obtained, ECDSA Verification can proceed as usual.

Indeed, further step 43 is similar to step 13 of Figure 1, and consists in calculating $u_1 = s^{-1} \times e \bmod n$ and $u_2 = s^{-1} \times R \bmod n$. Namely:

u_1 is obtained by computing the Montgomery multiplication between $s^{-1} \times R$ and e , that is to say $M(s^{-1} \times R, e) = s^{-1} \times e$; and,

u_2 is obtained by computing the Montgomery multiplication of $s^{-1} \times R$ with r , i.e., $M(s^{-1} \times R, r) = s^{-1} \times r$.

At 44, the bi-dimensional value (x_1, y_1) is calculated as: $(x_1, y_1) = u_1 \times G + u_2 \times Q$. The one with ordinary skills in the art will appreciate that this step is equivalent to step 14 of Figure 1.

At the test 45, if $x_1 \bmod n$ equals to r , then it is determined that signature is valid.

Otherwise, the bi-dimensional value (r, s) is held to be an invalid signature. Again, it will be noted that this final determination step is equivalent to step 15 of Figure 1.

With reference to the block diagram of **Figure 5**, there will now be described embodiments of the cryptosystems according to the third and sixth aspects of the invention. Such cryptosystems can be adapted to run computer program products according to the second and to the fifth aspects of the invention, respectively.

Each of these computer programs comprise one or more stored sequences of instructions that are accessible to a processor and which, when executed by the

processor, cause the processor to carry out the corresponding cryptographic method.

In the shown embodiments, the computer unit 30 comprises at least one processor 31, at least one memory 32 to store data used during the execution of the calculations by the processor 31, and at least one rewritable non-volatile
5 memory 33 used to store *e.g.* specific parameters or running commands to properly execute the method.

Memory 32 can be a Random Access Memory (RAM) of any suitable type, for instance a SRAM, a DRAM or SDRAM. Memory 33 can be a Read Only Memory
10 (ROM), of any suitable type for instance an EPROM or a Flash memory.

The cryptosystem further comprises an interface 34 (I/F).

For the implementation of the ECDSA signature scheme, the interface unit 34 is adapted for receiving a message m and for outputting a bi-dimensional signature (r,s) associated to said message m .

15 For the implementation of the ECDSA verification scheme, the interface unit 34 is adapted for receiving a bi-dimensional signature (r,s) associated to a message m .

In view of the foregoing, it will be apparent to the one with ordinary skills in the art that ECDSA signature and verification schemes can be performed without the usage of R^2 . Stated otherwise, smart use of the properties of the Montgomery
20 Multiplication in view of the little Fermat theorem allows an optimized way to obtain an ECDSA signature of a message and to check validity of such an ECDSA signature.

In addition, a person skilled in the art will appreciate that various parameters disclosed in the description may be modified and that various embodiments
25 disclosed and/or claimed may be combined without departing from the scope of the invention.

CLAIMS

1. A cryptographic method comprising an Elliptic Curve Digital Signature Algorithm, ECDSA, signature scheme comprising:
 - 5 - generating a bi-dimensional signature (r,s) having a first signature component r and a second signature component s , said bi-dimensional signature (r,s) being associated to a message m ,

wherein generating the bi-dimensional signature (r,s) comprises:

 - generating (31) a random number k ;
 - 10 - obtaining (32) a bi-dimensional value (x_1, y_1) having a first component x_1 and a second component y_1 , and corresponding to $k \times G$, where G is a bi-dimensional generator point of the elliptic curve;
 - setting (33) r to x_1 modulus n , where n is a prime number corresponding to the elliptic curve order;
 - 15 - generating (30) s as $k^{-1} \times (e + r \times d)$, where k^{-1} is the inverse of k , where d is a private key scalar number and where e equals $H(m)$ with H being a hash function, said generating comprising :
 - calculating (301) a first value $(e + r \times d) \times R^{-1}$ by the addition of the Montgomery multiplication of r and d modulus n , to the Montgomery multiplication of e and unity modulus n ;
 - 20 - calculating (302) a second value $(k \times R^{-1})^{n-2} \times R \bmod n$ as the exponentiation of the Montgomery form of $k \times R^{-1}$ to the power $n-2$ modulus n and thus obtaining $k^{-1} \times R^2$ as said second value,
 - obtaining (305) s by calculating the Montgomery multiplication between
 - 25 the second value $k^{-1} \times R^2$ and the first value $(e + r \times d) \times R^{-1} \bmod n$.

2. A computer program product comprising one or more stored sequences of instructions that are accessible to a processor and which, when executed by the processor, cause the processor to carry out the steps of the method of claim 1.

5 3. A cryptographic system comprising

- an interface unit (34) for receiving a message m and for outputting a bi-dimensional signature (r,s) associated to said message m ; and,

- a computer unit (30) adapted to generate the bi-dimensional signature (r,s) using an Elliptic Curve Digital Signature Algorithm, ECDSA, signature scheme

10 according to Claim 1.

4. A cryptographic method comprising an Elliptic Curve Digital Signature Algorithm, ECDSA, verification scheme,

wherein the verification scheme comprises:

15 - receiving a bi-dimensional signature (r,s) having a first signature component r and a second signature component s , said bi-dimensional signature (r,s) being associated to a message m ;

- generating (40) the Montgomery form of s^{-1} , where s^{-1} is the inverse of s , said generating comprising:

20 - calculating (401) a first value $(s \times R^{-1})^{n-2} \times R$ as the exponentiation of the Montgomery form of $s \times R^{-1}$ to the power $n-2$, where n is a prime number corresponding to the elliptic curve order and R is a given number coprime with n , with $R^2 \bmod n$ being the Montgomery Constant, and thus obtaining $s^{-1} \times R^2$ as said first value;

25 - calculating (403) the Montgomery Multiplication of the first value $s^{-1} \times R^2$ with the unity, to obtain a second value $s^{-1} \times R \bmod n$,

- calculating (43) a third value u_1 as the Montgomery multiplication between the second value $s^{-1} \times R$ and $e \bmod n$, where e equals $H(m)$ with H being a hash function; and

- calculating (43) a fourth value u_2 as the Montgomery multiplication between the second value $s^{-1} \times R$ and the first signature component $r \text{ modulus } N$, and
 - calculating (44) a bi-dimensional value (x_1, y_1) having a first component x_1 and a second component y_1 , and corresponding to the addition of $u_1 \times G$ and $u_2 \times Q$,
 5 where G is a bi-dimensional generator point of the elliptic curve and Q is a public key point which equals $d \times G$, with d being a private key scalar number; and,
 - determining (45) that the signature is valid if the first component value $x_1 \text{ modulus } N$ of the bi-dimensional value (x_1, y_1) equals r .
- 10 5. A computer program product comprising one or more stored sequences of instructions that are accessible to a processor and which, when executed by the processor, cause the processor to carry out the steps of the method of claim 4.
6. A cryptographic system comprising:
- 15 - an interface unit (34) for receiving a bi-dimensional signature (r, s) associated to a clear text message m ; and,
- a computer unit (30) adapted to determine whether the signature (r, s) is valid using an Elliptic Curve Digital Signature Algorithm, ECDSA, signature scheme according to Claim 4.

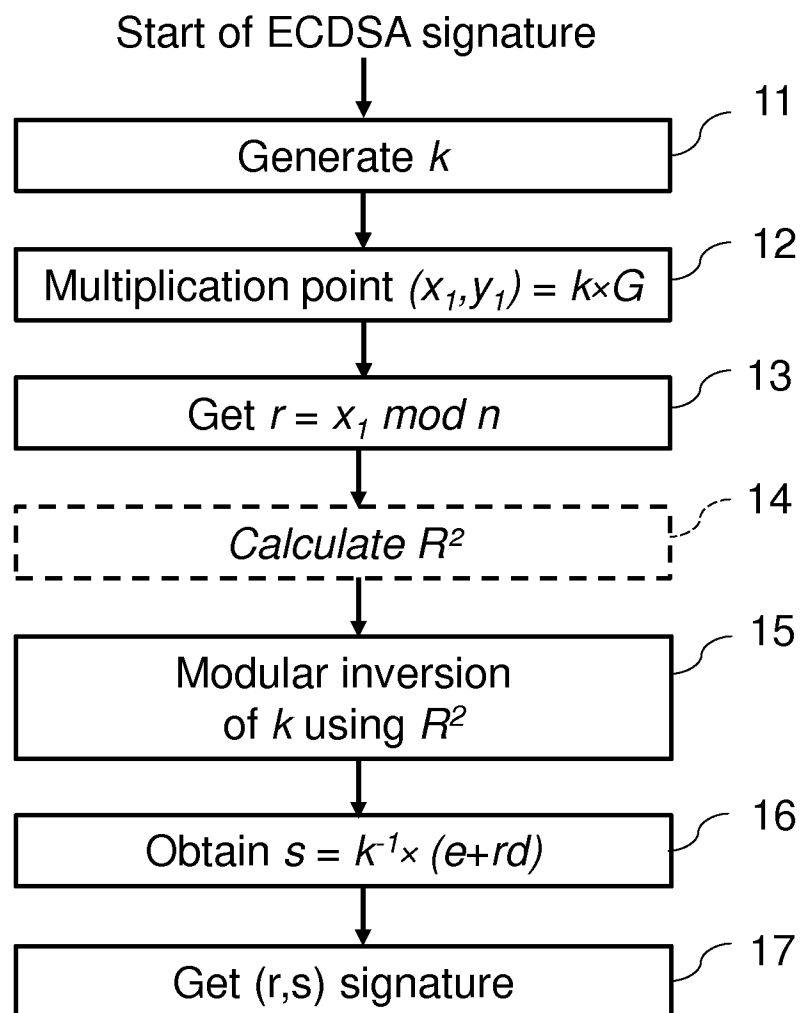


FIG.1
PRIOR ART

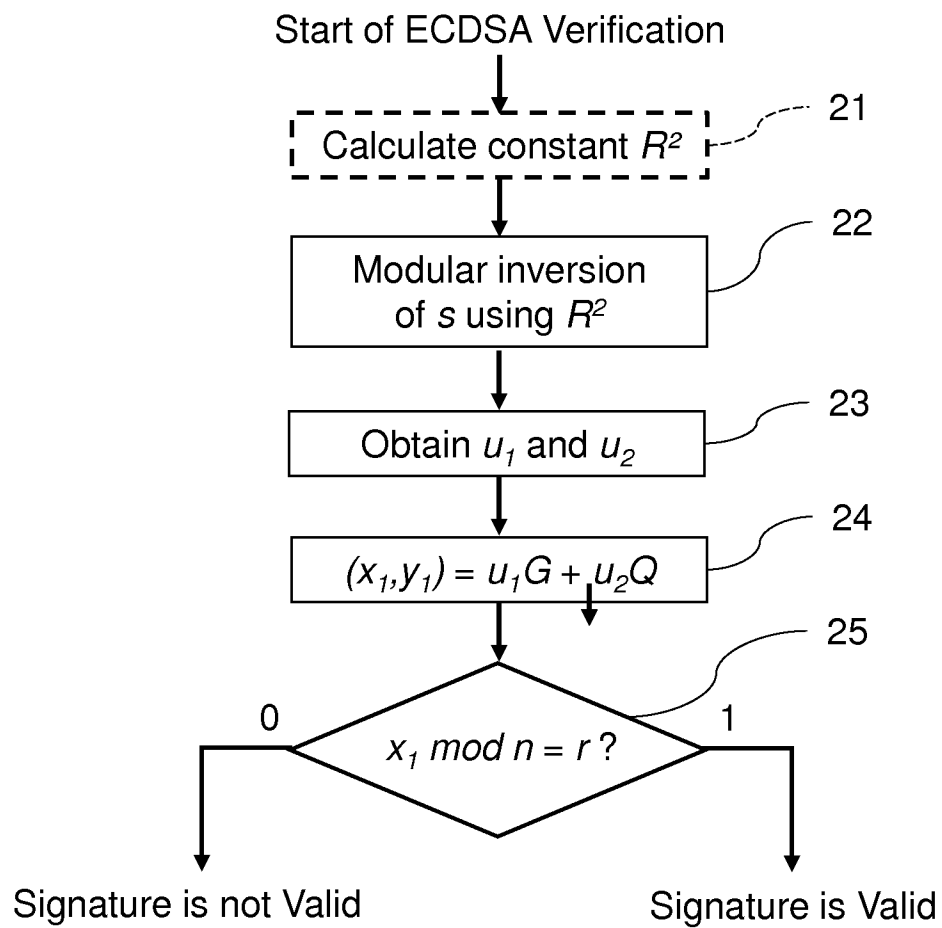


FIG.2
PRIOR ART

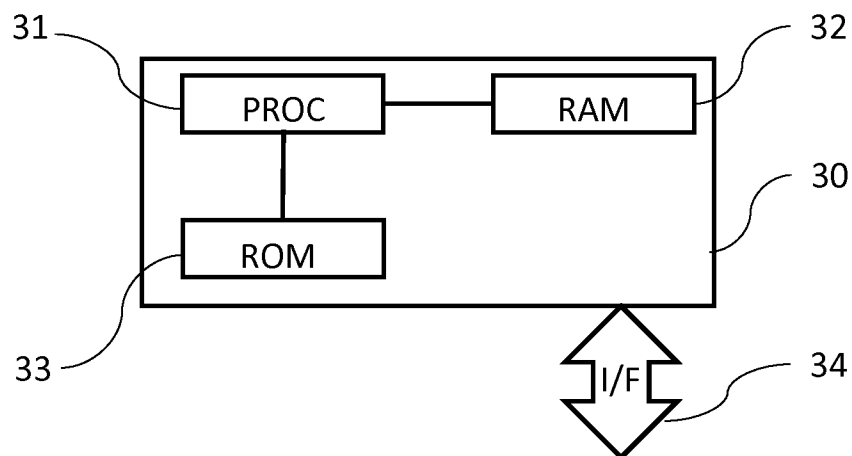


FIG.5

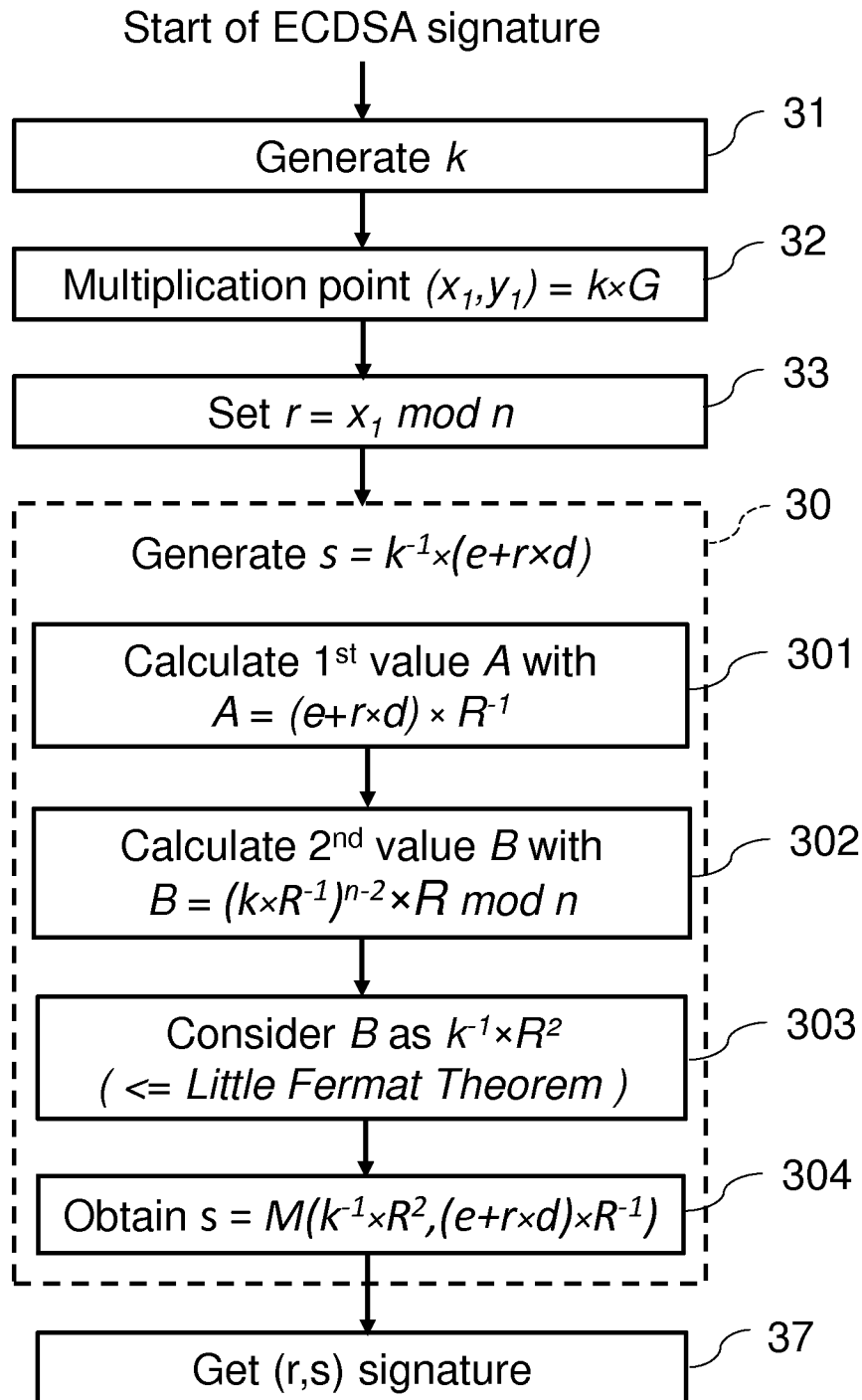


FIG.3

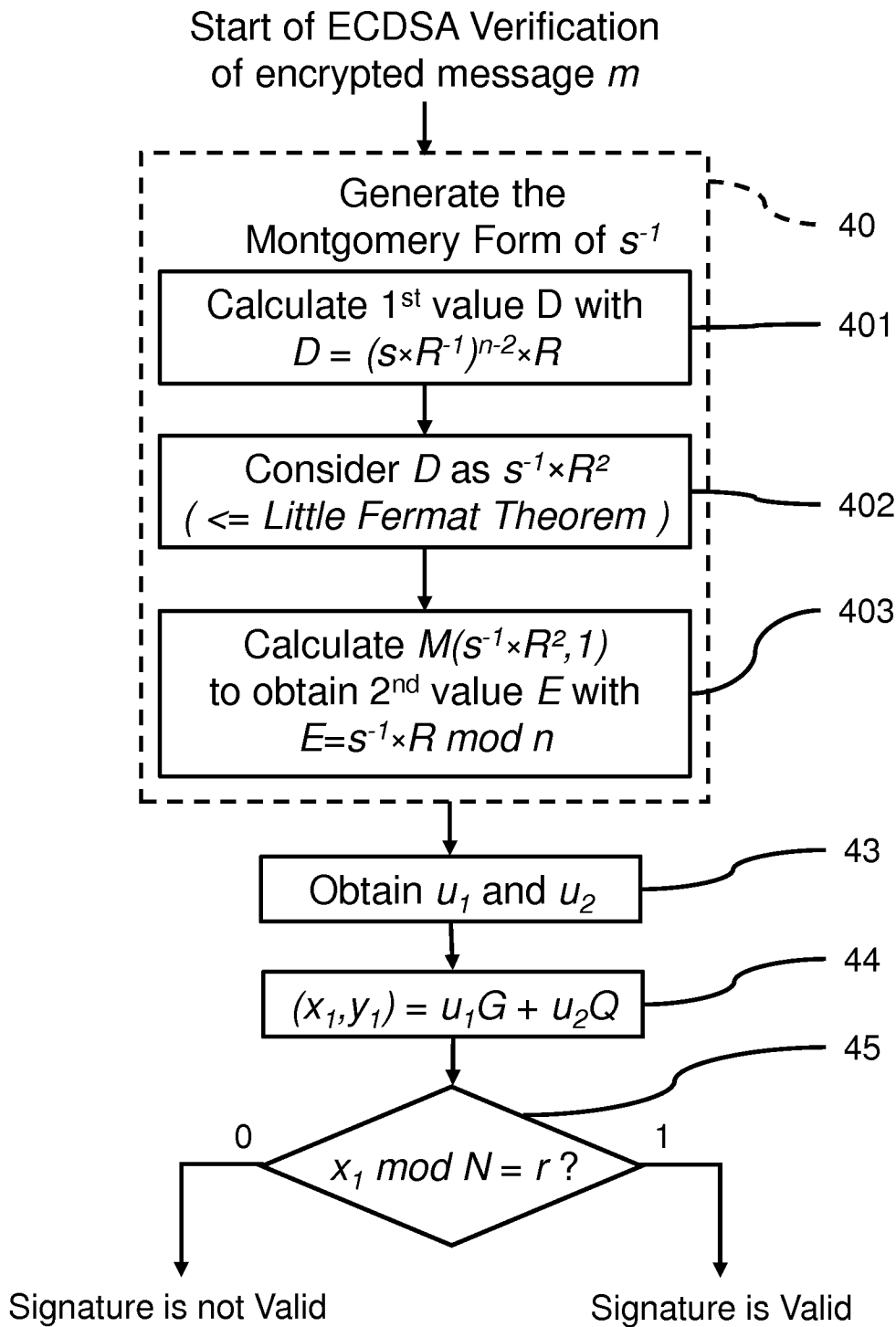


FIG.4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/068683

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32 G06F7/72
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BOSCHER ARNAUD ET AL: "Optimal Use of Montgomery Multiplication on Smart Cards", 19 April 2006 (2006-04-19), NETWORK AND PARALLEL COMPUTING; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 252 - 262, XP047305476, ISSN: 0302-9743 ISBN: 978-3-642-27653-8 sectino 6 ----- -/--	1-6



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

25 October 2017

Date of mailing of the international search report

07/11/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Billet, Olivier

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2017/068683

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DAVID NACCACHE ET AL: "Montgomery-suitable cryptosystems", 19 July 1993 (1993-07-19), ALGEBRAIC CODING. FIRST FRENCH-ISRAELI WORKSHOP, SPRINGER, DE, PAGE(S) 75 - 81, XP047000934, ISBN: 978-3-540-57843-7	4-6
A	section 9 -----	1-3
X	US 6 088 453 A (SHIMBO ATSUSHI [JP]) 11 July 2000 (2000-07-11)	4-6
A	figure 3 -----	1-3
A	EP 2 015 171 A1 (GEMPLUS [FR]) 14 January 2009 (2009-01-14) paragraphs [0022], [0027] -----	1-6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2017/068683

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-6

ECDSA implementation

1.1. claims: 1-3

Efficient ECDSA signature generation

1.2. claims: 4-6

Efficient ECDSA signature verification

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/068683

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6088453	A	11-07-2000	NONE

EP 2015171	A1	14-01-2009	EP 2015171 A1 14-01-2009
			EP 2162820 A1 17-03-2010
			US 2010177887 A1 15-07-2010
			WO 2009003740 A1 08-01-2009
