A New Idea in Digital Signature Schemes

MOHAMMED A AL-FAYOUMI and SATTAR J ABOUD
Faculty of IT, Department of Computer Science
The University for Graduate Studies,
Amman - Jordan

Abstract: - Since the invention of the first idea of digital signatures relied on public key algorithms many properties are added, and numerous novel schemes are developed. Besides this grow, a novel idea in identification schemes relied on public key algorithms is also presented, that is zero knowledge proof of identity. However, along with this development many remarkable schemes for instance the Fiat-Shamir protocol is generated. The Fiat-Shamir protocol is relied on one particular type of digital signature scheme that is RSA scheme, but generates signature for its own, which is vulnerable compared with the digital signature generated by the RSA scheme. The zero knowledge identification scheme proofs ownership of the digital signature on publicly known messages. The aim of this paper is to present a new idea in digital signature schemes based on computational delegation and is claimed to be more efficient than the current schemes.

Keywords: - digital signature scheme, public key cryptosystem, zero knowledge identification, RSA scheme, computational delegation, Fiat-Shamir protocol.

1. Introduction

The purpose of this paper is to permit participants to identify themselves. To reach this target, let us begin with a general approach, where we have the proprietor and two representatives. The proprietor establishes the RSA public key pair [1], and has some acknowledge concerning the Fiat-Shamir zero knowledge proof of identity protocol [2]. Also, assume that the proprietor have a trusted authority who would determine the RSA modulus and then would give identity so to converse every user based on this public key pair. Also, we can employ it in a different way, we can always enhance a zero knowledge scheme using a digital signature scheme and this is the mechanisms of the Fiat-Shamir scheme. So the proprietor of the RSA public key pair (p,s) can generate a group of signatures $s_{i_1}, s_{i_2}, ..., s_{i_k}$, for $i = 1,2,...,m$ after he determines k messages where k is a security parameter, and delegate these to the representative R_i, who is permitted to create Fiat-Shamir signatures using means of these privates. It should be noted that k and m are smaller than the modulus n. The public key of R_i includes the selected public key p and the equivalent messages $m_{i_1}, m_{i_2}, ..., m_{i_k}$ which could be joined to the identity of R_i by a known rules, to reduce the size of the key. It directly follows that this method has the characteristic that:

1) The proprietor can masquerade a representative, but the representative can not impersonate the proprietor. Also, other representatives can not impersonate every other.

We acquainted of no means by which adequately number of representatives by co-operating all at once may impersonate the proprietor, even when we select larger security parameters k and m.

We will stress on the digital signature schemes, but we can deal with identification schemes. This means that the proprietor can get access anywhere, except the delegated representative. Certainly the messages connected to R_i might then specify the access rights of R_i. It is important to emphasis that characteristic 1) could not be reached using secret sharing method. But if a private key d of the proprietor is divided

between two shares d_1 and d_2, from which d could be built, it is not necessarily abide by that knowledge of d requires knowledge of d_i. But even so, in secret sharing methods, we do not intrinsically have any ways of verifying publicly, that R_i knows d_i. We can surely add special schemes as constructing block of a considerable protocol which would solve this, but in general, this needs that every representative have his own separated public key pair. We are therefore interesting in one additional characteristic than in [3], where recipient of a share can prove that he obtained a share, but can not verify to a trusted authority that he has a share from which the unique private key might be rebuilt. Alternatively we create the following assumption:

- Each representative does not have a separated public key. His public key includes the public key of the proprietor and his rank.

In the last part of the next section we are going to introduce a new fairly result in numbering theory which will permit to present what seems to be secured computational delegation using RSA public key encryption scheme.

2. A New Idea in Digital Signature Scheme

Let begin with a simple example, assume that we have a proprietor and two individual representatives of rank 1, as well as the characteristic 1) mentioned above, we need another characteristic that is as follows:

2) The representatives may pose as the proprietor by cooperation all together.

In this paper, we present a ranking pyramid scheme, such that the proprietor *R* is a representative of rank 0, who has two individual representatives of rank 1 R_0 and R_1 where the 3-tuple (R, R_0, R_1) is satisfied $1), 2)$ and $(\bullet)$, However, the representative of rank i, R_j, such that j is a bit string of size i, have two individual representatives of rank i + 1, R_{j_1} and R_{j_1} where the 3-tuple (R_j, R_{j_0}, R_{j_1}) is satisfied $1), 2)$ and $(\bullet)$, also concurrently all representatives at one rank might impersonate *R* by cooperation all together. Now let us construct the scheme with one proprietor and two representatives of rank 1. We will then propose a more general scheme. However we wish to enhance this example separately using the public key scheme, though it is a greater scheme at this point to follow of what seems to be possible.

The following theorem claimed to be an example of great mathematical background:

Theorem 1 Assume that p is a prime number with 1 mod 4. Also, there are integers x, y where: $p = x^2 + y^2 = (x + i * y)(x - i * y)$. In contrast, p is not a prime number in the Gaussian ring $Z[i]$, the integers are extended by the square root of -1, nevertheless the product of two prime numbers. Furthermore, the non-ordered pair (x, y) is unique according to the fact that $Z[i]$ is a unique factoring problem [4]. We name (x, y) $(= (y, x))$ an abridged Fermat pair. It is suitable to select notation where $x > y$ for all time.

Cornacchia method [5] proposes that p is a prime number with 1 mod 4. Where input $a^2 = -1 \bmod p$ and the result is (x, y). Actually Cornacchia method is a public one. However, if we can calculate a square root of $-1 \bmod p$, then we can obtain the abridged Fermat pair of p. But when we substitute p with the number n and the $\gcd(b, n) = 1$, then $a^2 + b^2 = 0 \bmod n \Leftrightarrow (a/b)^2 = -1 \bmod n$, thus any pair (a, b) achieving this formula is named a Fermat pair of *n*. It is easy to categorize those n which have a Fermat pair, and this is performed by Fermat theorem [6]. Note that if n is odd, then $n \equiv 1 \bmod 4$. Actually the problem is just exciting if for any prime divisor p of n is that $p \equiv 1 \bmod 4$, we were coped to simplify this considerably as follows:

Theorem 2 Assume n achieve that any prime divisor is $1 \bmod 4$.

The following are equal:

- n have a Fermat pair
- n have a abridged Fermat pair

Also, we can define a correspondence relationship on the Fermat pairs by $(x, y) \sim (w, v)$, if $\gcd(x * v \pm y * w, n)$ is not an appropriate divisor of n. This is correspondent to $\gcd(x * w \pm y * v, n)$ dose not an appropriate divisor of n. The correspondence classes are named Fermat classes. The Fermat class having (x, y) is indicated $[x, y]$.

Every Fermat class has a unique abridged Fermat pair. This abridged Fermat pair can be built from any Fermat pair in the class, which is as follows:
Suppose (x, y) and (w, v) are two Fermat pairs of n. Then the following are equal:

- $[x, y] \neq [w, v]$
- $1 < \gcd(x * v - y * w) < n$

The important remark is the following. Suppose (x, y) and (w, v) are two Fermat pair of (n) .Then $(x / y)^2 = (w / v)^2 = -1 \bmod n$ .Therefore $(x * v / y * w)^2 \equiv 1 \bmod n$. Also, there is a 1 – 1 equivalence among Fermat classes and factors of order 4 in the multiplicative inverse [7, 8] of the integers $\bmod n$ whose square is -1. But when we multiply two square roots of -1, a and b we obtain the factor of order 2, except a corresponds $\pm b$. The factor of order two $\bmod n$ produces a factoring of n into mutually prime factors. Certainly, if we establish $sq(-1) = \{x \bmod n \mid x^2 = -1 \bmod n\}$ and $\{e = c \bmod n \mid c^2 = 1 \bmod n\}$ then, are an Abelian group of order 2^c such that c is the element of different prime divisors of n. Also, if $x \in sq(-1)$ then $sq(-1) = x * e$, thus, the only difficulty is actually how to move from a Fermat pair to the related abridged Fermat pair. The algorithm is as follows:

2.1. Algorithm

Suppose a, b and n are positive integer numbers with $\gcd(a, b) = 1$ and $a^2 + b^2 = 0 \bmod n$ .Also, suppose that $(x * a) + (y * b) = n$. For integer number x, y such that $a > y$ and $a^2 > n$. Then $x^2 + y^2 = 0 \bmod n$ and $x^2 + y^2 < a^2 + b^2$. This is currently employed as follows. Suppose we given a Fermat pair (a, b), set the Fermat pair $(a / b, -1)$ then let $t = a / b \bmod n$. So $t^2 + 1 = 0 \bmod n$, if $t^2 < n$, we are performed, thus suppose this is not the case, so employ the Euclidian algorithm to the following equation $n = q * t + c$. then $t^2 + 1^2 > q^2 + c^2 = 0 \bmod n$. Repeat the operation with $n = t$, $t = c$ and keep continue on this until you find the result.

2.2. Example

Suppose p = 37 and q = 61 $\therefore n$ = 2257 $\because 1597^2 + 1 \equiv 0 \bmod 2257$, then 2257 =1*1597 + 660

repeat

$n \equiv q * z + r;$

$n = z;$

$z = r;$

until $n \equiv z^2 + r^2$

2.3. Tracing

n	*q*	*z*	*r*
2257	1	1597	660
1597	2	660	277
660	2	277	106
277	2	106	65
106	1	65	41
65	1	41	24
41	1	24	17

So, $2257 \equiv 41^2 + 24^2$

3. The Proposed Scheme

Suppose that $n = p * q$, such that $p, q = 1 \bmod 4$ are prime numbers. Then n has two precisely abridged Fermat pairs (x, y) and (w, v). In fact we require $2\log(n)$ bits to explain a Fermat pair, and just $\log(n)$ bits to illustrate the equivalent abridged Fermat pair, which is one of the good reasons for argument in the previous section. We estimate that:

A. It is hard to give n to compute a Fermat pair of n.
B. It is hard to give n and a Fermat pair to compute any non-corresponding Fermat pair.

Since the facts are as follows:

1. If factorization is hard then at least A or B is hard to solve.
2. If B is simple, we can resolve the allegedly hard question of the Fermat primes, it means which numbers of the type $2^a + 1$, where a a power of 2 is, are prime numbers.

We will assume that for the remainder of this section that the above points A and B are hard. Then we have the following data ranking:
Level $0(p, q)$
Level $1(x, y), (w, v)$
Level $2(n)$

At this point, we now have a clear reduce and select identification scheme, which works as follows:

Representative	Verifier
Select r at random	
Find $r^2 \bmod n$	$\rightarrow r^2 \bmod n$
	$\leftarrow$ Select 1 or 0
If 1	$\rightarrow x * r$
If 0	$\rightarrow r$

Such that $x \in sq(-1)$ denoted by (x, y). The verifier then lastly verifies that the final received value squared is $\pm$ the received value of the initial step. The argument on the above section illustrates that we are actually have the ability of classifying two separate delegates (x, y) and (w, v), and when they collaborate might detect the primes p and q so we are achieving the objective also having reached the general assumption mentioned above. This mean it is useful to see that we are employing abridged Fermat pairs. Additionally, it is adequate to keep one of the integers x and y while the other is computed from the known modulus. Alternatively, if (a, b) is selected at random, Fermat pair affirm A) above that given only a, it is not possible to recover b.

However, we will suggest certain means that simplify the proposed scheme. Assume that $p, q = 1 \bmod 2 * m$ are primes and $n = p * q$, we can then consider that for every $j = 2,3,..., m$ the set of components $sq\ j(-1) = \{a \bmod n \mid a$ rose to the power 2^{j-1} is $-1 \bmod n\}$.

It is simple to perceive that the cardinality of $sqj(-1)$ is $2^{2(j-1)}$. Detecting always a and $-a$, means that we have 2^{j-1} which is basically different elements of order 2^j where the $2^{j-1'th}$ power is -1. The problem now is that how to construct a computational delegation as suggested. It provides that it is not sufficient to consider elements, whose order is multiplication of 2.

3.1. Example

Assume $m = 3$ and u is an element of Zn with order 2^3, where $u^4 = -1$ and let $x = u^2$. We need two representatives of x, a and b. Select $a = u * c \bmod n$ and $b = u * c^{-1} \bmod n$ for certain c integer. This is just fine but no one can prove the identity of a without calculating some data concerning c, for example $c^2 \bmod n$. The first concept is to select c with appropriate number of order two, but this causes the representatives very influential. A good opportunity appears to select $c^2 \bmod n$ as a message which denotes the rank of a representative. It is then uncomplicated to adjust the proposed scheme to permit for identification of the representatives of x currently presented.

4. Discussions

It appears unacceptable for some one is restricted to select a modulus n which is the product of two prime numbers in which both should be 1 mod 4. A more general technique might be to employ Pell's formula as follows. $x^2 + g * y^2 \equiv 0 \bmod n$. This can be computed when g is a quadratic residue mod n, and this was observed by Fermat. In fact, we can present Fermat classes *w.c.r.g*, which we name a distinguisher, with requesting a pair (x, y) to achieve the above Fermat pair formula, then we define two Fermat pairs (x, y) and (w, v) to be a corresponding iff $\gcd(x * v \pm y * w, n)$ is not the acceptable divisor of n. Note that it by no means to tracks that (y, x) is a Fermat pair iff (x, y) is, except $g = 1$. Yet again, we would name a Fermat pair (x, y) and *w.c.e.g* abridged, if $x^2 + g * y^2 \equiv n$. Though, it is not accurate that the answer always exists [3]. However, we have the following equations: $p = x^2 + gy^2$, $q = w^2 + g * v^2$. Then

$$n = p * q = (x^2 + g * y^2)(w^2 + g * v)$$
$$= (x^2 * w^2 + g^2 * y^2 * v^2) + g(y^2 * w^2 + x^2 * v^2)$$
$$= (x * w + g * y * w)^2 + g(y * w - x * v)^2$$
$$= (x * w - g * y * w)^2 + g(y * w + x * v)^2$$

It is known that there is an answer for $g = 2$ if $p, q = 3 \bmod 8$ and for $g = 3$ when $p, q = 1 \bmod 3$.

5. Conclusions

We confess it has nothing to do with the obvious theme of this argument, but as academically tending authors, we can not resist. Given any solving to $x^2 + y^2 = w^2$ we directly see that (x, y) is a Fermat pair of w. It then follows that w has an equivalent abridged Fermat pair $p^2 + q^2 = w$. Obviously the formula we discuss at this time is

much general $x^2 + y^2 = k * w$ for any k and this justifies the title. It follows that in order to factor the RSA modulus n, which is the product of two prime numbers every should congruent to 1 mod 4, is corresponding to computing two different right-angle triangles, the hypotenuse of which is n, and the other sides have integer sizes.

References

[1] Rivest, R Shamir A and L Adelman, 1978, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communication of the ACM 21, 2, 120-126.

[2] Fiat, A., and Shamir, A, How to prove yourself: practical solutions to identification and signature problems, in advances in cryptology proceeding of crypto '86, Lecture notes in computer science 263, 1987, springer verlag, pp. 186-194

[3] M Bellare & S. Goldwasser, "Verifiable Partial Key Escrow", Proceeding of 4th ACM Conference on Computer and Communications Security, April 1997.

[4] J. R. Goldman, the Queen of Mathematics, a Historically Motivated Guide to Number Theory A. K. Peters, Ltd., 1998.

[5] H. Cohen, A Course in Computational Algebraic Number Theory, Springer Graduate Texts in Mathematics 138, Springer 1993.

[6] D. A. Cox, Primes of the Form $x^2 + ny^2$, Wiley Inter-science, 1989.

[7] Sattar Aboud, "*Baghdad Method for Calculating Multiplicative Inverse*" international Conference on Information Technology, Las Vegas, Nevada, USA, 2004, pp. 816-819.

[8] Sattar Aboud "*Fraction – Integer Method (FIM) for Calculating Multiplicative Inverse*", Journal of Systemics, Cybernetics and Informatics, Volume 2, Number 5, 2005, USA

.