Gulf Journal of Mathematics
Vol 6, Issue 4 (2018) 44-50

A BLIND SIGNATURE BASED ON THE DLP AND RSA CRYPTOSYSTEM

S. EZZIRI[1*] AND O. KHADIR[2]

Abstract. In this work we propose a new blind signature protocol based on the Schnorr scheme and the RSA algorithm. We also study its security and complexity.

1. Introduction

In cryptography, a blind signature [1, pp. 271] [2, 3, 4] [8, pp. 475] [16, pp. 178], is a form of digital signature in which the content of a message is disguised before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature.
These special digital signatures constitue an important field in public key cryptography. It is typically used in privacy-related protocols where the signer and message author are different parties to ensure the anonymity of the participants. Such as in electronic payment systems and voting protocols [2, 5, 6, 10, 12].
The concept of cryptographic blind signature schemes is that one entity, the user, wants to obtain a signature on his message, without revealing it to the signer during the protocol. This is similar to the approach of zero-knowledge proof.
The method is generally based on developing the solutions of hard mathematical problems, like factoring, discrete logarithm and computing square root modulo a large composite number.

A secure blind signature scheme must satisfy three properties [2, 7, 14]:

Completeness: If the signer and the requester of the signature follow the algorithm of blind signature honestly, then the verification algorithm will always accept the signature obtained for the original message.

Note: A view of the protocol consists of all values and parameters that are accessible to the signer or any other party who is observing the communication between the signer and the requester of the signature.

Date: Received: Dec 2, 2018
*Corresponding author.
2010 *Mathematics Subject Classification.* 11T71, 94A60.
Key words and phrases. Schnorr blind signature, RSA cryptosystem, Discrete Logarithm Problem.

Blindness: Let the output of the protocol be the pair (m, s) (where m is the message and s the signature), and V be the "view" of verification of the blind signature. At any time, the signer will not be able to suggest any connection between V and (m, s). This means that it is improbable to link any valid pair (m, s) to the circumstance of the signature generation in which it was builted.

Unforgeability: A blind signature scheme is unforgeable if, whenever the blind signature is divulged, the signer will not be able to know who is the owner of the signature. Also for an attacker, the only way to obtain a valid signature is to follow the protocol with a signer possessing the private key.

In this work we propose a new secure blind signature scheme based on the discrete logarithm problem [8, pp. 103] and RSA cryptosystem [11]. We study its security and complexity.
The paper is organized as follows: In section 2, we recall the RSA blind signature. We describe the Schnorr blind signature in section 3. We present our contribution in section 4. Finally we conclude in section 5.
We denote by $\mathbb{N}$ and $\mathbb{Z}$ the sets of natural numbers and relative integers respectively. For $a, b \in \mathbb{N}$, $\gcd(a, b)$ expresses the greatest common divisor of a and b. We write $a \equiv b\,[n]$ if n divides the difference $a - b$. Furthermore, $\varphi(.)$ is the Euler function.

We start by describing the classical RSA blind signature.

2. Blind signature scheme based on the RSA cryptosystem

Chaum [2] proposed the first blind signature scheme, which was based on RSA and the hardness of the factoring problem.

According to [2] and [7], a blind signature scheme consists of five steps: key generation, masking the original message, signing, unblinding and verifying the result.

In all of the following let Bob be the signer and Alice be the requester of the signature. The protocol works as follows:

(1) To generate the RSA blind signature keys, Bob selects two random large primes p and q. He computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. Then he chooses an integer e sach that $gcd(e, \varphi(n)) = 1$. Let (e, n) be Bob's public key. The signer calculates his private key by the equation: $ed \equiv 1\,[\varphi(n)]$. As usual he publishes (n, e) and a one-way hash function H like SHA_1 for example [8, pp. 33] [15, pp. 119]. He destroys p, q and keeps d as his secret key.

(2) Alice chooses $r \in \mathbb{Z}_n^*$ and computes $m' \equiv r^e H(m)\,[n]$, where m is the message to be signed, and m' is the blinded version of the message m.

Alice submits m' to Bob.

(3) Bob computes $s' \equiv m'^d\,[n]$. Then he sends the signature s' to Alice.

(4) In order to obtain the signature of the original message m, Alice computes $s \equiv s'r^{-1}\,[n]$.

(5) Then she verifies the legitimacy of the signature s by checking whether $s^e \equiv H(m)\,[n]$ or not.

Indeed: we first have $s \equiv s'r^{-1}\,[n]$ then $s^e \equiv (s'r^{-1})^e\,[n]$, as $s' \equiv m'^d\,[n]$ so $s^e \equiv (m'^d r^{-1})^e\,[n]$. In addition we have $m' \equiv r^e H(m)\,[n]$, we replace by m' in the last equation we obtain $s^e \equiv ((r^e H(m))^d r^{-1})^e \equiv (r^{ed} H(m)^d r^{-1})^e\,[n]$. Since $ed \equiv 1\,[\varphi(n)]$ then $s^e \equiv (rH(m)^d r^{-1})^e \equiv H(m)\,[n]$.

In the next section we describe the Schnorr blind signature.

3. Schnorr blind signature

The Schnorr identification protocol [13] was also turned into a blind signature scheme which was proposed by D. Pointcheval and J. Stern in [9]. The transformation was used in electronic cash systems [9].

The Schnorr blind signature works by following the next steps :

(1) Bob starts by selecting two large prime integers p and q, such that $q \mid p-1$. They are published together with an element g of $(\mathbb{Z}/p\mathbb{Z})^*$ of order q. He chooses a secret key $x \in \mathbb{Z}/q\mathbb{Z}$, and computes $y \equiv g^{-x}\,[p]$. Then his public keys are y, g, p, q and a one-way hash function H.

(2) Alice wants to make a blind signature of a message m. In order to issue this signature, the signer Bob chooses a random number $k \in \mathbb{Z}/q\mathbb{Z}$, he computes and sends the result $r \equiv g^k\,[p]$. Alice blinds the message to sign with two random elements $\alpha, \beta \in \mathbb{Z}/q\mathbb{Z}$ and puts $r' \equiv rg^{-\alpha}y^{-\beta}\,[p]$, then she computes the value $e' \equiv H(m, r')\,[q]$. She sends the challenge $e \equiv e' + \beta\,[q]$ to the signer Bob.

(3) Bob returns the signature $s \equiv k + ex\,[q]$.

(4) Alice computes $s' \equiv s - \alpha\,[q]$.

(5) Then she verifies that (e', s') is a valid signature of the message m by the equation $r' \equiv g^{s'}y^{e'}\,[p]$.

Indeed: we first have $e' \equiv e - \beta\,[q]$ and $s' \equiv s - \alpha\,[q]$ then $g^{s'}y^{e'} \equiv$

$g^{s-\alpha}y^{e-\beta}\,[p]$. As $s \equiv k + ex\,[q]$, we replace in the last equation, we obtain $g^{s'}y^{e'} \equiv g^{k+ex}g^{-\alpha}y^{e}y^{-\beta}\,[p]$. Since the secret key x verifies $y \equiv g^{-x}\,[p]$ then $g^{s'}y^{e'} \equiv g^{k}g^{-\alpha}y^{-\beta}g^{ex}g^{-ex}\,[p]$. Hence the result $r' \equiv g^{s'}y^{e'}\,[p]$.

In the next section we present our own result.

4. Our contribution

4.1. **Description of our method.** In this section we propose a new secure blind signature based on the Schnorr scheme and RSA cryptosystem. Our protocol is as follows:

(1) The signer Bob chooses an integer prime P, such that $P = 2pq + 1$ where p and q are two large and distinct primes. He publishes P and keeps p and q secret. Let g a generator of $(\mathbb{Z}/P\mathbb{Z})^*$, and e a public RSA exponent that verifies $gcd(e, \varphi(P-1)) = 1$. Bob secret keys are p, q, $x \in \{0, ..., P-1\}$ and d such that $d \equiv \dfrac{1}{e}\,[\varphi(P-1)]$. His public keys are P, g, e, y such that $y \equiv g^{-x}\,[P]$, and he selects a one-way hash function H.

(2) Alice wants to sign a message m without revealing it. To be done the signer Bob starts with selecting a random number $k \in \{0, ..., P-1\}$, and computes $r \equiv g^{k}\,[P]$. Then he sends the result to Alice. In the second round Alice chooses two random elements $\alpha, \beta \in \{0, ..., P-1\}$. Note that $gcd(\alpha, P-1) = 1$. Then she masks the message to sign in such a way that $r' \equiv r^{\alpha^e}y^{-\beta}\,[P]$, and she calculates the value $z' \equiv H(m, r')\,[P-1]$. Then she sends the challenge $z \equiv \dfrac{z'+\beta}{\alpha^e}\,[P-1]$ to the signer Bob.

(3) Bob signs the challenge z proposed by Alice with the equation $s \equiv (k + zx)^d\,[P-1]$, and sends the result to Alice.

(4) Alice computes $s' \equiv \alpha s\,[P-1]$.

(5) Then she verifies the validity of the signature (z', s') by checking whether $g^{s'^e}y^{z'} \equiv r'\,[P]$ or not.

Indeed: the verification equation is $g^{s'^e}y^{z'} \equiv r'\,[P]$, then $g^{s'^e} \equiv r'y^{-z'}\,[P]$. We have $r' \equiv r^{\alpha^e}y^{-\beta}\,[P]$, we replace in the previous equation, so $g^{s'^e} \equiv r^{\alpha^e}y^{-\beta}y^{-z'}\,[P]$. Of course r verifies the equation $r \equiv g^{s^e}y^{z}\,[P]$, then $g^{s'^e} \equiv g^{s^e\alpha^e}y^{z\alpha^e}y^{-\beta}y^{-z'}\,[P]$.
In addition we have $z' \equiv z\alpha^e - \beta\,[P-1]$. Consequently $g^{s'^e} \equiv g^{(s\alpha)^e}\,[P]$. Hence we obtain the result $s' \equiv \alpha s\,[P-1]$.

4.2. **Example.** To illustrate our method, we present a numerical example.

(1) Assume that Bob selects a prime integer P, such that $P = 2pq + 1 = 11579339$, where $p = 2011$ and $q = 2879$ are primes. He publishes P and keeps p and q secret. Bob chooses $g = 2$ a generator of $(\mathbb{Z}/P\mathbb{Z})^*$, and $e = 11$. Note that $gcd(e, \varphi(P-1)) = 1$. His secret keys are $d \equiv \dfrac{1}{e} \equiv 5258891\,[\varphi(P-1)]$, $x = 467$. His public keys are g, e, y such that $y \equiv g^{-x} \equiv 826955\,[P]$, and he selects a one-way hash function H.

(2) Suppose that Alice wants to ask Bob to produce a signature for the message $m = 29281$ without revealing it. In the first round the signer Bob selects a random number $k = 21990$ and computes $r \equiv g^k \equiv 7559363\,[P]$. Then he sends the result to Alice. She chooses two random elements $\alpha = 7$, $\beta = 5$. Note that $gcd(\alpha, P-1) = 1$. Then she blinds the message to signe by following the steps: she computes $r' \equiv r^{\alpha^e} y^{-\beta} \equiv 8027424\,[P]$, and calculates the value $z' \equiv H(m, r')\,[P-1]$ using any hash function (like SHA_1 for example) assume that $z' \equiv H(m, r') \equiv 6849\,[P-1]$. Ultimately she submits the challenge $z \equiv \dfrac{z'+\beta}{\alpha^e} \equiv 11465250\,[P-1]$ to the signer Bob.

(3) After receiving the challenge z, Bob sign with the equation $s \equiv (k+zx)^d \equiv 6883400\,[P-1]$. Then he sends the result to Alice.

(4) Alice calculates $s' \equiv \alpha s \equiv 1866448\,[P-1]$.

(5) She checks that $g^{s'^e} y^{z'} \equiv r' \equiv 8027424\,[P]$. Then (z', s') is a valid signature for the message m.

4.3. **Security analysis.** Suppose that Oscar is an adversary who knows Bob public keys. Let us analyze the security of our protocol.

Completeness: : It can be clearly seen that if Alice and Bob follow the protocol honestly, then:

$$\begin{aligned} g^{s'^e} y^{z'} &\equiv g^{(\alpha s)^e} y^{z\alpha^e - \beta}\,[P] \\ &\equiv g^{\alpha^e((k+zx)^d)^e} y^{z\alpha^e-\beta}\,[P] \\ &\equiv g^{\alpha^e(k+zx)} y^{z\alpha^e-\beta}\,[P] \\ &\equiv r^{\alpha^e} y^{-z\alpha^e} y^{z\alpha^e-\beta}\,[P] \\ &\equiv r^{\alpha^e} y^{-\beta} \equiv r'\,[P] \end{aligned}$$

Thus the verification algorithm will always accept the signature (z', s').

Blindness: : Intuitively, it is easy to see that the message-signature pairs (z, s) and (z', s'), are statistically independent of each other and hence cannot be linked together due to the random variables α and β. Thereby implying unlinkability/blindness.

Unforgeability: : Since the factorization of $P-1$ is unknown to everyone except the signer, then even if the attacker Oscar knows the public key e he will not be able to find the secret key d. Also if Oscar has access to integers z' and r, he can not forge a signature s' using the equation $g^{s'^e}y^{z'} \equiv r' \, [P]$. Therefore the scheme is unforgeable.

4.4. **Complexity.** Let T_{mult}, T_{exp} and T_H be the time required to execute respectively a modular multiplication, an exponentiation and a hash function. We neglect the necessary time to compute modular additions, substractions and comparisons.

Bob needs to perform one modular exponentiation and one modular multiplication to generate his public and secret keys. In the blinding step, Bob must calculate one modular exponentiation, and Alice computes two modular multiplications, three modular exponentiations, and a hash function. To sign the challenge z Bob execute one modular multiplication, and one modular exponentiation. In the unblinding step Alice needs to compute one modular multiplication. Finally to verify the signature Alice requires one modular multiplication, and three modular exponentiations.

Then the total necessitate time [8, pp. 72] is:

$$T_{tot} = 6T_{mult} + 9T_{exp} + T_H = O((\log \ P)^2 + (\log \ P)^3)$$

So, our blind signature protocol works on a polylogarithmic time.

5. Conclusion

In this paper we proposed a new secure blind signature inspired by the Schnorr scheme and RSA algorithm. We studied its security and complexity.

6. ACKNOWLEDGMENT

This work is supported by the CNRST Research Scholarship and the MMS e-orientation project.

References

[1] J A. Buchmann, Introduction to Cryptography. New York: Springer-Verlag, 2001.
[2] D. Chaum, Blind signatures for untraceable payments. Advances in Cryptology, Crypto'82, pp. 199-203, 1982.
[3] D. Chaum, Blind signature systems. Advances in Cryptology, Crypto'83, pp.153-156, 1983.
[4] D. Chaum, Blinding for unanticipated signatures. Advances in Cryptology, Eurocrypt'87, pp. 227-233, 1987.
[5] D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash, Advances in Cryptology, Crypto '88, LNCS 403, Springer Verlag, pp. 319-327, 1988.
[6] D. Chaum: Privacy Protected Payment, SMART CARD 2000, Elsevier Science Publishers B.V. (North-Holland), pp. 69-93, 1989.
[7] S. Han and E. Chang, A pairing-based blind signature scheme with message recovery. Ardil, C. (ed), Sixth International Enformatika Conference (IEC), pp. 303-308, 2005.

[8] Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. Handbook of applied cryptography, 1996.
[9] D. Pointcheval and J. Stern. Provably secure blind signature schemes. Advances in Cryptology – Asiacrypt ' 96. Vol. 1163, pp. 252-265. Springer-Verlag, 1996.
[10] W. Qiu, How to construct DLP-based blind signatures and their application in E-Cash systems. Progress in Cryptography, The Kluwer International Series in Engineering and Computer Science. Vol. 769, pp. 73-80, 2004.
[11] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communication of the ACM, Vol. 21, pp. 120-126, 1978.
[12] B. Schneier, Applied Cryptography, J. Wiley, 1993.
[13] C.P. Schnorr, Efficient Identification and Signatures for Smart Cards. Crypto '89, LNCS 435, pp. 235-251, Springer Verlag, 1990
[14] B. Schoenmakers, Cryptographic Protocols. Lecture Notes, Technical University of Eindhoven, 2011
[15] D. R. Stinson, Cryptography: Theory and practice, Third Edition, Discrete mathematics and its applications, 2006.
[16] W. Trappe and L. Washington. Introduction to Cryptography with Coding Theory. Prentice Hall, 2nd edition, 2005.

[1,2]Laboratory of Mathematics, Cryptography, Mechanics and Numerical Analysis, Fstm, University Hassan II of Casablanca, Morocco
Email address: [1]Salma.ezziri@gmail.com, [2]Khadir@hotmail.com