A Registration Scheme to Allocate a Unique Identification Number

Manoj Kumar

Department of Mathematics,

Rashtriya Kishan (P.G.) College Shamli,

Choudhary Charan Singh University Meerut, Utter Pradesh - India.

E-mail- yamu_balyan@yahoo.co.in

Abstract. Identification is always a necessity of human life. Currently, our government has decided to allocate a unique identity to every Indian. This paper proposed a registration scheme, in which a controlling agency can generate a unique identification number in such a way that registration number cannot be forged and misused. In the proposed scheme, only the number holder can use his number and he/she can prove its validity to any third party, whenever necessary.

1. Introduction

Authentication is a key aspect of trust-based identity attribution, providing a codified assurance of the identity of one entity to another. Authentication methodologies include the presentation of a unique object such as a bank credit card, the provision of confidential information such as a password or the answer to a pre-arranged question, the confirmation of ownership of an e-mail address, and more robust but relatively costly solutions utilizing encryption methodologies. In general, business-to-business authentication prioritizes security while user to business authentication tends towards simplicity. New physical authentication techniques such as iris scanning, hand printing, and voice printing are currently being developed and in the hope of providing improved protection against identity theft. For these authentication methodologies, there is a need of valid identification [4, 7, 11, 16, 20, 21, 28, 29]. In other word, to apply the authentication methodologies, first we need valid infrastructures which support unique digital identification. Simply, we can say that identification is always a necessity of human life for authentication. Currently, our government has decided to allocate a unique identity to every Indian. In fact, physical signature is used to fulfill these requirements. Signature of the sender is the most important part of a message. Usually written signature is hard to duplicate. Therefore this is a natural tool to authenticate the communication. Since physical signature is meaningless in electronic messages; one has to rely on other methods like digital signature.

Public key cryptography discovered by W. Diffie and M. Hellman [8] in 1976 has revolutionized the ways of message communications through insecure media. It is now possible for the people who have never met before to communicate with one another in a secure and authenticate way over an open and insecure network such as Internet. Thus there is a growing use of public key techniques in cryptographic applications. In particular, digital signature scheme [3, 5, 6, 15, 19, 22] is one of the most important cryptographic tools, which is essential in implementing various security measures and authentication.

Digital signature scheme allows a user with a **public key** [1, 2] and a corresponding **private key** to sign a document in such a way that everyone can verify the signature on the document (using her/his public key), but no one else can forge the signature on another document. This **self-authentication** is required for some applications of digital signatures such as certification, by some authority. In many situations, signed message is sensitive to the signature receiver. Signatures on medical records, tax information and most personal/business transactions are such situations. Consider when a user A wants to generate a signature on a message m, sensitive for B and the message is also of concern to other users. For this situation, the form of the signature should be such that only B can directly verify the signature and that B can prove its validity to any third party C, whenever necessary. Such signatures are called **directed signatures** [10,12,13,14,23,24,25,26,27,29]. In directed signature scheme, the signature receiver B has full control over the signature verification process. Nobody can check the validity of signature without his cooperation. The concept of directed signatures was first presented by C.H.Lim and P.J. Lee [12,13]. It is a construction based on the GQ signature scheme [9].

Contribution

This paper proposed a registration scheme to allocate a unique identification number. Our scheme is based upon the concept of directed signature scheme. In the proposed scheme, a controlling agency can generate a unique identification number in such a way that only the number holder can use this number and he/she can prove its validity to any third party, whenever necessary. This paper also proves that the registration number cannot be forged and misused.

Organization

The rest of the paper is organized as follows. Section-2 presents some basic tools. Section-3 presents a registration scheme to allocate a unique registration number. In support of our proposed scheme, an illustration is provided in section-4. Section- 5 is about the security of the proposed scheme. Finally, comes to a conclusion in the section 6.

2. Preliminaries

2.1. Throughout this paper we will use the following system setting.

- A prime modulous p, where $2^{511} < p < 2^{512}$;
- A prime modulous q, where $2^{159} < q < 2^{160}$ and q is a divisor of $p - 1$;

- A number g, where $g \equiv k^{(p-1)/q} \bmod p$, k is random integer with $1 \leq k \leq p-1$ such that g >1; (g is a generator of order q in Zp^*).
- A collision free one-way hash function h [32];

The parameters p, q, g and h are common to all users. We assume that every user A chooses a random $x_A \in Zq$ and computes $y_A = g^{x_A} \bmod p$ .Here x_A is the private key of A and y_A is the public key of A. For our purpose, we use the directed signature scheme based on Schnorr's signature scheme [22]. These basic tools are briefly described below:-

2.2. Schnorr's signature scheme

In this scheme, the signature of A on message m are given by (r_A , S_A), where,

$$r_A = h(g^{k_A} \bmod p, m), \quad \text{and} \quad S_A = k_A - x_A . r_A \bmod p.$$

Here random $k_A \in Zq$ is private to A .The signature are verified by checking the equality

$$r_A = h\,(g^{S_A}\ y^{r_A} \bmod p, m).$$

3. A Registration Scheme to Allocate a Unique Identification Number

Registrations of various kinds are a common practice in our society, like that of vehicle, shop and factory etc. In daily life, there are so many situations, when it is necessary, beneficial and expedient to have a registration number for vehicles etc. This section proposes a registration scheme in which the registration number cannot be forged and misused. Under this scheme the validity of an allocated registration number can be verified at any time by any authority. The allocating authority and verifying authority may be different. For the practical implementation of this idea, we use a directed signature scheme.

We all are familiar with the present status of our registration system. A hand written signature is used for the allocation of registration number by the authority. Every signature is followed a lot of formalities and records. Unfortunately the present system is not much secure and is liable. We assume a government center, providing the registration number for the public. An officer Yamu , Y , heads this center. Y possesses a secret and public key pair (x_o, y_o). Again consider a public person Chaya, C, with a secret and public key pair (x_c, y_c) wants her registration number. The officer, Y generates a registration number with message m, so that C can directly collect her registration number. She can use her registration number publicly. She is able to prove its validity to any authorized party R whenever necessary. No one other than C can use this registration number because only she can prove its validity. This section is organized as follows.

3.1.1. Allocation of registration number by Y to C

(a). Y picks at random K_{y_1} and $K_{y_2} \in Zq$ and computes

$$Wy = g^{K_{y_1} - K_{y_2}} \bmod p \quad \text{and} \quad Zc = y_c^{K_{y_1}} \bmod p.$$

(b). Y again computes $r_y = h\,(Zc, Wy, m)$ and $S_y = K_{y_2} - x_0.r_y \bmod q$.

(c) . Y sends $\{ S_y, W_y, r_y, m, \}$ to C as her registration number.

3.1.2. Collecting and verification of registration number by C

(a). C collects $\{ S_y, W_y, r_y, m\}$ and make this public as her registration number.

(b). C computes $\mu = [\, g^{S_y} (y_0^{ry})\, W_y \,] \bmod p$, $Zc = \mu^{x_C} \bmod p$ and checks the validity of her registration by computing $r_y = h\,(Zc, Wy, m)$.

3.1.3. Verification Of registration number by authority R

(a) C sends to $\{ S_y, W_y, r_y, m, \mu \}$ to R.

(b) R checks if $r_y = h\,(Zc, W_y, m) \bmod q$.

If this does not hold R stops the process; otherwise goes to the next steps.

(c) C in a zero knowledge fashion [5, 9, 13] proves to C that $\log_\mu Z_C = \log_g y_C$ as follows.

- R chooses random $u, v \in Zp$ computes $w = \mu^u . g^v \bmod p$, and sends w to C.
- C chooses random $\alpha \in Zp$ computes $\beta = w. g^{\alpha} \bmod p$, and $\gamma = \beta^{x_C} \bmod p$,

  and sends β, γ to R.
- R sends u, v to C, by which C can verify that $w = \mu^u . g^v \bmod p$.
- C sends α to R, by which she can verify that

  $$\beta = \mu^u . g^{v+\alpha} \bmod p, \quad \text{and} \quad \gamma = Z_C^{u}\, y_C^{\,v+\alpha} \bmod p.$$

4. Illustration

The following illustration supports our scheme for practical implementation. Taking $p = 23$, $q = 11$ and $g = 5$.The secret and private key of users is as follow

For	Secret key	private key

Y	5	20
C	8	16

4.2.1. Allocation of registration number by Y to C

(a) Y picks at random $K_{y_1} = 7$, $K_{y_2} = 4$ and calculate

$$W_y = 10, \quad Z_y = 1 \text{ and } r_y = 2. \text{ (taking } m = 1)$$

(b) Y computes $S_y = 5$, and sends {10, 2, 5, 1} to C as her registration number.

4.2.2. Verification of registration number by C

(a). C collects her registration number {10,2,5,1} and makes this public.

(b). C checks the validity of her registration by computing $Z_C = 18$ and check if $r_y = 2$.

4.2.3. Validity proof of registration number by C to any authorized party R

(a) C computes $\mu = 6$, and $Z_C = 6^8 \bmod 23 = 18$. and sends (18,10,2,5,1) to R.

(b) R checks if $r_y = h(18,10,1) = 2$.

If this does not hold stops the process; otherwise goes to next step.

(c) Now C proves to 'R' that $\log_6 18 = \log_5 16$, in a zero knowledge fashion by using the confirmation protocol [23,24,25,26,27].

5. Security discussions

This signature scheme is secure if existential forgery (providing a new message –signature pair) is computationally infeasible. In this section, we discuss a possible attacks that can one forge a signature { $S_y, W_y, r_y, m,$} using the equation, $\mu = [\, g^{S_y} (y_0^{ry})\, W_y \,] \bmod p$? To compute the integer S_y from this equation is equivalent to solving the discrete logarithm problem. If any forger randomly selects S^* and sends { S^*, W_y, r_y, m } to B, the receiver B computes

$$\mu^* = [\, g^{S^*} (y_G)^R \; W \,] \bmod p, \quad Z^* = \mu^{* x_B} \bmod p.$$

and can check if $r_B = h(Z^*, W_B, m)$, to detect the forgery.

6. Conclusion

Thus above construction facilities the allocation of registration number in the electronic world with the following characteristics.

- Only the user can use his/her registration number, due to the property of directed signature scheme.
- The problems of forgery can be solved easily.
- By using this scheme, we can minimize the possible misuse of the present system.
- The obvious advantage of our scheme over present system is that the resulting registration number has no meaning to any third person.
- Since the relation between the signature and the signer secret key is not known to anyone but the designated receiver. Hence security level is much higher than any other scheme based on discrete logarithm.

References

1. Blake I.F., Van Oorschot P.C., and Vanstone S., (1986). Complexity issues for public key cryptography.In J. K. Skwirzynski, editor, *Performance limits in communication, Theory and Practice, NATO ASI Series E:Applied Science* – Vol # 142,p.p. 75 – 97.Kluwer Academic Publishers.Proceedings of the NATO Advanced Study Institute Ciocco, Castelvecchio Pascoli,Tuscany, Italy.
2. Blakely G.R. (1979). Safeguarding cryptographic keys, *Proc. AFIPS 1979 Nat. Computer conf.,* 48, p.p. 313-317.
3. Boyar, J., Chaum D., Damgard I. and Pederson T., (1991), Convertible undeniable signatures. *Advances in Cryptology – Crypto,* 90, LNCS # 537,p.p.189-205.
4. Bray, Z. (2004). Living Boundaries: Frontiers and Identity in the Basque Country. Brussels: Presses interuniversitaires européenes, Peter Lang.
5. Chaum D. (1991). Zero- knowledge undeniable signatures. *Advances in Cryptology –Eurocrypt, 90,* LNCS # 473,p.p..458-464.
6. Chaum D. (1995). Designated confirmer signatures, *Advances in Cryptology Euro crypt, 94* LNCS # 950,p.p..86-91.
7. Cote, James E. and Charles Levine (2002). *Identity Formation, Agency, and Culture*. New Jersey: Lawrence Erlbaum Associates.
8. Diffie W. and Hellman M. (1976). New directions in Cryptography, *IEEE Trans. Info.Theory.*31.pp. 644 - 654.

9. Guillou, L.C. and Quisquater J.J. (1988), A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory. *"Advances in Cryptology –Eurocrypt, 88,* LNCS # 330, p.p.123 - 128.

10. Jianhong Zhang, Yixian Yang and Xinxin Niu (2009), Efficient Provable Secure ID-Based Directed Signature Scheme without Random Oracle, ISBN: 978-3-642-01512-0, Volume 5553/2009, Springer Berlin / Heidelberg.

11. K.Cameron,"Laws of Identity", (2006) Blog, http://www.identityblog.com/?p=352

12. Lim C.H. and Lee P.J. (1993). Modified Maurer-Yacobi, scheme and its applications. *Advance in cryptology –Auscrypt,* LNCS # 718, p.p. 308 – 323.

13. Lim C.H. and P.J.Lee. (1996). Security Protocol, In Proceedings of International Workshop, (Cambridge, United Kingdom), Springer-Verlag, LNCS # 1189.

14. Lu, R., Lin, X., Cao, Z., Shao, J., and Liang, X. (2008), New (t,n) threshold directed signature scheme with provable security. *Inf. Sci.* 178, 3 (Feb. 2008), 756-765. DOI= http://dx.doi.org/10.1016/j.ins.2007.07.025.

15. Mambo M., Usuda K. and Okamoto E. (1996). Proxy signatures for Delegating signing operation. *Proc.3 rd ACM Conference on computer and communications security.*

16. Meyers, D. T. (2004). Being yourself: essays on identity, action, and social life. Feminist constructions. Lanham, Md: Rowman & Littlefield Publishers. ISBN 0742514781.

17. Mullin R.C., Blake I.F., Fuji – Hara R. and Vanstone S.A. (1985). Computing Logarithms in a finite field of characteristic two. *SIAM J. Alg.Disc.Meth.,* p.p.276 – 285.

18. Odlyzko. A.M. (1984). Discrete logs in a finite field and their cryptographic significance. In N.Cot T.Beth and I.Ingemarsson, editor, *Advances in Cryptology – Eurocrypt, 84,* LNCS # 209, p.p..224 - 314.

19. Okamoto T. (1994). Designated confirmer signatures and public key encryption are equivalent. *Advances in Cryptology – Crypto, 94* LNCS # 839, p.p..61-74.

20. Phil Windley (2005), Digital Identity, ISBN 10: 0-596-00878-3 | ISBN 13: 9780596008789.

21. Rannenberg, Kai; Royer, Denis; Deuker, André, (2009), The Future of Identity in the Information Society: Challenges and Opportunities, , XVI, 508 p. 79 illus., 45 in color., Hardcover ISBN: 978-3-540-88480-4.

22. Schnorr C.P. (1994). Efficient signature generation by smart cards, *Journal of Cryptology,* 4 (3), p.p.161-174.

23. Sunder Lal and Manoj Kumar, A digital signature scheme with threshold generation and verification. http://arXiv.org/ftp/cs/papers/0409/o4090014.pdf

24. Sunder Lal and Manoj Kumar, A directed signature scheme and its applications, in the proceeding of *National conference on Information Security, Sponsored by DRDO*, Jan 8-9 –2003, New Delhi. Also available at http://arXiv.org/ftp/cs/papers/0409/o4090036.pdf

25. Sunder Lal and Manoj Kumar, A directed threshold multi- signature scheme. In the proceeding of INDIA COM – 2008, ISSN 0973-7529 and ISBN 978-81-904526-2-5 serials for international references, http://www.bvicam.ac.in/indiacom/ The full paper is also available on http://arxiv.org/ftp/cs/paper/0409/0409049.pdf

26. Sunder Lal and Manoj Kumar, A directed threshold signature scheme. The full paper is available on http://arxiv.org/ftp/cs/paper/0411/0411005.pdf

27. Sunder Lal and Manoj Kumar, A Directed Threshold signature scheme without SDC, in the proceeding of National Conference on Method and Models in Computing, December 13-14, 2007, School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi. The full paper is also available on http://arxiv.org/ftp/cs/papers/0502/0502002.pdf

28. Woodward, K. (2004). *Questioning Identity: Gender, Class, Ethnicity.* London: Routledge. ISBN 0415329671.

29. Xun Sun1, Jian-hua Li1, Gong-liang Chen and Shu-tang Yang1,(2008),Identity-Based Directed Signature Scheme from Bilinear Pairings, *eprint.iacr.org/2008/305.pdf.*

30. Yen S.M. and Laih C.S. (1993). New digital signature scheme Based on Discrete Logarithm, *Electronic letters,* Vol. 29 No. 12 pp. 1120-1121.

31. Zhang. (1997). Nonrepudiable proxy signature schemes” *Manuscript*.

32. Zheng, Y., Matsummoto T. and Imai H. (1990). Structural properties of one – way hash functions. *Advances in Cryptology – Crypto, 90,* Proceedings, p.p. 285 – 302, Springer Verlag.

33. Zhonghua Shen, Xiuyuan Yu, Qimeng He,(2008), **A Directed-threshold Multi-signature Scheme Based on Modular Secret Sharing,** *International Journal of Computational Science,* 1992-6669 (Print) 1992-6677 (Online) www.gip.hk/ijcs, Vol. 2, No. 6, 806-814.

Manoj Kumar received the B.Sc. degree in mathematics from Meerut University Meerut, in 1993; the M. Sc. in Mathematics (Gold medalist) from C.C.S.University Meerut, in 1995; the M. Phil. (Gold medalist) in Cryptography, from Dr. B. R. A. University Agra, in 1996; the Ph.D. in Cryptography, in 2003. He also qualified the National Eligibility Test (NET), conducted by Council of Scientific and Industrial Research (CSIR), New Delhi- India, in 2000. He also taught applied Mathematics at D. A. V. College, Muzaffarnagar, India from Sep 1999 to March 2001; at S.D. College of Engineering & Technology, Muzaffarnagar- U.P. – INDIA from March 2001 to Nov 2001; at Hindustan College of Science & Technology, Farah, Mathura- U.P. – INDIA, from Nov 2001 to March 2005. In 2005, the Higher Education Commission of U.P. has selected him. Presently, he is working in Department of Mathematics, R. K. College Shamli- Muzaffarnagar- U.P. – INDIA-247776. He is a member of Indian Mathematical Society, Indian Society of Mathematics and Mathematical Science, Ramanujan Mathematical society, and Cryptography Research Society of India. He is working as reviewer for some International peer review Journals: Journal of System and Software, Journal of Computer Security, International Journal of Network Security, The Computer Networks, Computer and Security, The Computer Journal. He is also working a Technical Editor for some International peer review Journals- Asian Journal of Mathematics & Statistics, Asian Journal of Algebra, Trends in Applied Sciences Research, Journal of Applied Sciences. He has published his research works at national and international level. His current research interests include Cryptography and Applied Mathematics.