International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Generation of Private Registration Number Publically

Manoj Kumar
Department of Mathematics, Rashtriya Kishan (P.G.) College Shamli, Choudhary Charan Singh University Meerut, Utter Pradesh, India.

ABSTRACT

The need of Identification is always an essential requirement in our daily life. For example, requirement of registration number for our houses, ration card for public distribution system, registered societies, vehicles etc. This registration number should be unique and authentic. Currently, our government has also decided to allocate a unique registration to every Indian in the form of Aadhaar card. In this paper, we introduced a registration scheme, in which a government authority can generate a unique registration number in such a way that registration number will be unique and cannot be forged and misused. In the proposed scheme, only the number holder can use his registration number and the authenticity of the registration number can verified any time by the government authority.

Keywords: Identity, Registration, authenticity, Public Key Cryptosystem, Secret Key, Private Key.

I. INTRODUCTION

Registrations of various kinds is a common practice in our society, like that of vehicle, shop 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 registration number should be unique and authentic. Currently, our government has also decided to allocate a unique registration to every Indian in the form of Aadhaar card. In this paper, we introduced a registration scheme, in which a government authority can generate a unique registration number in such a way that registration number will be unique and cannot be forged and misused. In the proposed scheme, only the number holder can use his registration number and the authenticity of the registration number can verified any time by the government authority. The proposed scheme is based on public key cryptography and directed signature scheme. A brief detail of these two techniques: public key cryptography and directed signature scheme is given in preliminaries section 2.

1.1. Contribution

This paper proposed a registration scheme to allocate a unique identification number. Our scheme is based on 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.

1.2. Organization

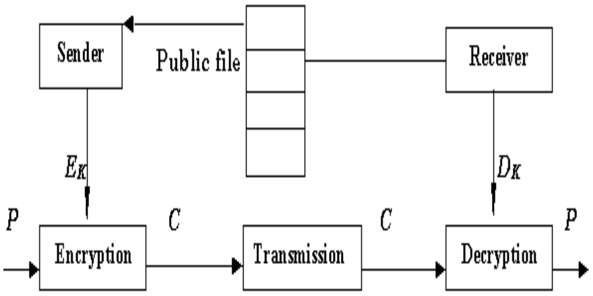
The rest of the paper is organized as follows. Section-2 presents some basic tools. Section-3 presents a registration scheme to allocate a unique registration number. Finally, comes to a conclusion in the section 4.

II. PRELIMINARIES

2.1. Public Key Cryptography

Whitefield Diffie and Martin Hellman proposed in 1976, a new type of cryptosystem which is called now, as *public key cryptosystem* [PKC] [17, 18, 19]. The invention of public key cryptography is the most important event in the field of cryptography and provided answers to all the above problems of key managements and digital signatures. A public key cryptosystem is a pair of families $\{E_K\}$ and $\{D_K\}$, $K \in$ key space K, of algorithms representing invertible transformations $E_K : P \rightarrow C$ and $D_K : C \rightarrow P$

- for every K, E_K is the inverse of D_K .
- for every K, it is easy to compute E_K and D_K
- for almost every K, each easily computed algorithm equivalent to D_K is computationally infeasible to drive from E_K.
- for every K, it is feasible to compute inverse pairs E_K and D_K from K.



Public Key Cryptosystem

Because of the third property, the encryption key E_K of each user can be made public without compromising the security of his private decryption key D_K. The public key cryptographic system is therefore split into two parts, a family of encryption transformations and a family of decryption transformations in such a way that, given a member of one family, it is infeasible to find the corresponding member of the other.

The forth property guarantees that there is a feasible way of computing corresponding pairs of inverse transformations when no constraint is placed on what either the encryption or decryption transformation is to be.

In this cryptosystem, there is no need to send the secret key via secure channel. Every user A in the system has one pair of keys, a *public key* E_{KA} for encryption and a *private key* D_{KA} for decryption. With the help of private key, the user calculates his public key. It is computationally infeasible to recover the private key by using his public key. At first glance, it seems incredible that such cryptosystems could actually exit. Later we shall see that there are indeed successful realizations. The RSA cryptosystem [20] and the ElGamal cryptosystems [21] are such realizations. All public keys are publicly available; they might be stored in public file, as in a phone book. On the other hands, the private keys are kept secret; only the owner knows them. Let us now suppose that we have a public key cryptosystem. Consider the user A wants to send the message m to B. The process works as follows.

- A looks up the public key E_{KB} of B, encrypts the message m as $E_{KB}(m)$ = C and send the cryptotext C to B.
- B is able to decrypt the cryptotext C, since he exclusively knows the key D_{KB}. He gets $m = D_{KB}(E_{KB}(m))$.
- No other user can decipher $E_{KB}(m)$, since no one can recover D_{KB} from E_{KB} and $E_{KB}(m)$.

2.2 ElGamal Cryptosystem

Taher ElGamal [21] proposed a cryptosystem based on the difficulty of finding discrete logarithm. This difficulty of discrete logarithm is applicable not only to the key management, but also to the design of encryption and signature algorithm. To go further, it is necessary to understand the concept of discrete logarithm. Suppose we have a finite field Z_q with group operation of multiplication. With the help of repeated square method anyone can compute b^x for large x such as $y = b^x$, y and $b \in Z_q$. Now it is easy to compute

$$y = b^x$$

for given x and b but for a given b and y ,it becomes infeasible to compute x. Here the value x is said to be the discrete logarithm of y to the base b. For example, let us take Z_{19} and $b = 2$, then we can compute $2^6 = 7$, which is equivalent to saying that the discrete logarithm of 7 to the base 2 is equal to 6. But it is much more difficult to compute the number 6 by using 2 and 7. So for a large x, it is computationally infeasible to recover this x with the known b and y.

In the ElGamal scheme there is a general agreement upon a prime p and an integer g. Every user A select randomly an integer α_A ; $0 < \alpha_A < p - 1$ and compute a public value $\beta = g^{\alpha_A}$ mod p. If we want to send a message m to the user A then we choose random integer k and send to A the pair (g^k ,$m\beta^k$). Now since the user A knows α_A so he can recover the message m from this pair. The user A raises $\alpha_A{}^{th}$ power to the first element of the pair and then divide the second element of the pair to get the plaintext.

2.3 Directed Signature Scheme

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 [6, 8, 9]. 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.

2.4. Schnorr's Signature Scheme

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

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

$$S_A \quad = \quad k_A - x_A \,.\, r_A \bmod p.$$

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

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

III. A REGISTRATION SCHEME TO ALLOCATE A UNIQUE IDENTIFICATION NUMBER

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 key and public key pair as ($x_{o\,,}\, y_o$). 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 third party R whenever necessary. No one other than C can use this registration number because only she can prove its validity. Allocation of registration number, and verifying processes are as follows.

3.1. Allocation of registration number by Y to C

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

$$\mathrm{Wy} \;=\; \mathrm{g}^{\,K_{y_1}\,\text{-}\,K_{y_2}} \bmod p \quad \text{and}$$

$$\mathrm{Zc} \;=\; y_C{}^{K_{y_1}} \bmod p.$$

(b). Y again computes $\mathrm{r_y}$ = h (Zc, Wy, *m*) and

$$S_y = K_{y_2} - \; x_{\mathrm{o}}.r_y \bmod q.$$

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

3.2. Collecting and verification of registration number by C

(a). C collects { $S_{y\,,}$ W_y , $r_{\mathrm{y},}$ *m*} and make this public as her registration number.

(b). C computes

$$\mu \;=\; [\;g^{S_y}(\;y_0{}^{\mathrm{ry}}\;)\,W_y\,] \bmod p,$$

$$Zc \;=\; \mu^{\,x_C} \bmod p$$

and checks the validity of registration by computing

$$r_{\mathrm{y},} \;=\; h\,(Zc,\, W\mathrm{y},\, m).$$

3.3. Verification of registration number by uthority R

(a) C sends to { S_y ,W_y , $r_{\mathrm{y},}$,*m*, µ} to R.

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

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

(c) C in a zero knowledge fashion [3, 4] proves to R that $\log_\mu Z_C \;=\; \log_g y_C$ as follows.

(a) R chooses random *u*, *v* ∈ Z*p* computes

$$w \;=\; \mu^{u}\,.\,g^{v} \bmod p,$$

and sends *w* to C.

(b) C chooses random α ∈ Z*p* computes

$$\beta \;=\; w.\, g^{\alpha} \bmod p, \text{ and}$$

$$\gamma \;=\; \beta^{x_C} \bmod p,$$

and sends β, γ to R.

(c) R sends *u*, *v* to C, by which C can verify that

$$w \;=\; \mu^{u} .\, g^{v} \bmod p.$$

(d) C sends α to R, by which she can verify that

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

$$\gamma \;=\; Z_C^{\;u}\; y_C^{\;v+\alpha} \bmod p.$$

IV. CONCLUSION

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

1. Only the user can use his/her registration number, due to the property of directed signature scheme.
2. The problems of forgery can be solved easily.
3. By using this scheme, we can minimize the possible misuse of the present system.
4. The obvious advantage of our scheme over present system is that the resulting registration number has no meaning to any third person.
5. 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.

V. REFERENCES

[1]. Blakely G.R. (1979). Safeguarding cryptographic keys, Proc. AFIPS 1979 Nat. Computer conf., 48, p.p. 313-317.

[2]. 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.

[3]. Chaum D. (1991). Zero- knowledge undeniable signatures. Advances in Cryptology –Eurocrypt, 90, LNCS # 473,p.p..458-464.

[4]. 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.

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

[6]. 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.

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

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

[9]. 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 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

[10]. 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

[11]. 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

[12]. 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.

[13]. 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.

[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]. 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.

[16]. Diffie W. and Hellman M. (1976). New directions in Cryptography, IEEE Trans. Information Theory - 31, p.p. 644 - 654.

[17]. Diffie W. (1988). The first ten years of Public Key Cryptography, In Contemporary Cryptology: The Science of Information Integrity, Editor, Simmons G.J. IEEE Press, New York. p.p 135-175.

[18]. Hellman M. E. (1979). The mathematics of public key cryptography, Scientific American - 241, p.p. 130-139.

[19]. Rivest, R., Shamir A. and Aldeman L. (1978). A method of obtaining digital signatures and PKCS, Communication of ACM - 21(2), p.p. 120-126.

[20]. ElGamel T. (1985). A PKC and a signature scheme based on discrete logarithm, IEEE trans information theory - 31, p.p. 469 - 472