# Proxy Signatures for Secured Data Sharing

Neha Agarwal
Amity University Uttar Pradesh
agarwalnehajain@gmail.com

Ajay Rana
Amity University Uttar Pradesh
ajay_rana@amity.edu

J.P. Pandey
KNIT Sultanpur
tojppandey@rediffmail.com

*Abstract*—**Digital signatures are used to ensure the integrity, non-repudiation and authencity while communication between the sender and recipient however it cannot be used in some condition so can be used in several forms. Several approaches has been proposed on proxy signatures. In this paper we have given a survey on discrete logarithmic problem, RSA and Bilinear pairing approaches used for proxy signatures.**

Keywords: *Proxy Signature; Discrete Logarithmic Proble; Bilinear pairing; Integer factorization problem.*

## 1. INTRODUCTION

Digital signatures is an asymmetric cryptography which ensures the authenticity of the sender who has send the message. It is an authentication mechanism in which a sender attach a code called signature which is formed by taking hash of a message and then encrypting it using senders secret key, in this way it ensures the integrity of message send. The recipient on receiving the message verify the signatures using senders public key this concept ensures that sender cannot repudiate it later. The main reason to implement digital signature is to ensure authentication, integrity and non repudiation while communicating message between parties. However there are conditions where digital signatures cannot be used as it does not satisfy the requirements, and so they are implemented in several other forms, namely aggregate signatures, ring signatures, multi signatures, proxy signatures, blind signatures etc. Proxy signature is a kind of digital signature in which an original signer(owner) grants his signing rights to another entity called proxy signer who is authorized to sign on his behalf in his absence. Let us consider a case that a senior person in an organization has to go on leave for certain reason in such case he will grant his signing rights to a someone who will be responsible to sign in his absence on his behalf. This paper discuss about recent work done in proxy signatures.

### *A. Classification of proxy signatures*

Based on delegation of rights proxy signature scheme can be classified as full delegation, partial delegation and partial delegation with warrants. In full delegation scheme an owner shares his secret key with proxy signer as a result proxy signer creates signature similar to original signer as a result it becomes difficult to differentiate who has signed the document and this leads to increase in forging. In partial delegation scheme, the original signer generates proxy key using his secret key and gives it to proxy signer. The proxy signer signs on behalf of original signer according to capabilities defined in delegation however there is no restriction on his signing capability, he can even transfer the signing capability to others. Limitations of above mentioned schemes was eliminated by partial delegation with warrants in which original signer specifies identity of both of them, time period of delegation and kind of messages on which proxy signer can sign. Warrants are used by original signer to certify the authenticity of proxy signer.

According to relevant information about proxy secret key known to owner, the proxy signatures are classified as proxy protected or proxy unprotected schemes. In case of proxy protected scheme the proxy secret key is not known to original signer so we can easily discriminate who has create proxy signature and who is original signer. Whereas in proxy unprotected scheme since the original signer is well introduced to the secret proxy key he can easily forge the proxy signer to produce proxy signature.

### *B. BASIC MODEL OF PROXY SIGNATURE*

The basic model comprises of actors and the main actors in the model are:

- An owner who is an original signer and he grants his signing capability partially or fully to a proxy signer to authenticate him to sign in his absence.
- A proxy agent who is also called proxy signer and he has been granted rights and so has an authority to sign the message in absence of the original signer.
- A verifier, who checks for the validity of proxy signature and accordingly decide to accept or reject.

## 2. DESIRED SECURITY PROPERTIES OF PROXY SIGNATURE

Proxy signatures are desired to satisfy certain security properties. Few of expected properties are as follows

- Strong unforgeability: Only a proxy signer who has been delegated by owner(original signer) must be able to create a proxy signature using his private key and no one else not even an original signer can create his signature .
- Strong identifiability: proxy signer must be easily identifiable by anyone from his proxy signature since the proxy signatures are created by his secret key which is personally owned by him.

978-1-4673-8203-8/16/$31.00 ©2016 IEEE

- Strong undeniability: After careting signatures the proxy signer must not be able to repudiate signatures created for the rights delegated to him from the original signer.
- Verifiability: The verifier must be convinced with the agreement signed between the original signer and proxy signature created on signed message.
- Distinguishability: Its important that there must be distinguish ability between signature of original signer and the proxy signature of proxy signer.
- Secrecy: The original signer create a proxy secret key from his private key and send it to proxy agent who uses this proxy secret key and his own private key to generate proxy signature. However the private key of original signer must not be retrieved from any information.

## 3. MODELS OF PROXY SIGNATURE

The three main models discussed in this paper are based on DLP, RSA and Bilinear pairing

### 3.1 Proxy Signature Based On DLP

An owner or original signer selects a private key $Pr_o$ and computes her public key $Pb_o$ as

$Pb_o \leftarrow KG_{dlp}(param, Pr_o)$

A proxy signer selects a private key $Pr_p$ and computes her public key $Pb_p$ as

$Pb_p \leftarrow KG_{dlp}(param, Pr_p)$

- **Generation of delegation capability**

The signature of an owner $\sigma_o$ on warrant ,$\omega$ is generated after taking input as param,chosen parameter of original signer $(k_o, r_o)$, private key of original signer $Pr_o$ and warrant $\omega$.

$\sigma_o \leftarrow S_{dlp}(param,(k_o, r_o), Pr_o, \omega)$

- **Verification of delegation capability**

It takes input as param, public key of original signer $Pb_o$, signature of owner $\sigma_o$ and warrant $\omega$ and Gives Result as valid or invalid

$Result \leftarrow V_{dlp}(param, Pb_o, \sigma_o, \omega)$

- **Generation of proxy Key**

Proxy key $\rho_p$ is generated using parameter param, signature of original signer $\sigma_o$, private key of original signer $Pr_o$, public parameters like signers public key, warrants , random number)

$\rho_p \leftarrow ProxKG_{dlp}(param, \sigma_o, Pr_o, pub\_param)$

- **Generation of Proxy signature**

Proxy key $\sigma p$ on message m is generated using proxy key $\rho p$, message m and parameter param.

$\sigma_p \leftarrow S_{dlp}(param, \rho_p, m)$

- **Verification of Proxy Signature**

It takes as input parameter param, public key of original signer Pbo, public key of proxy signer Pbp, proxy signature of proxy signer $\sigma_p$ and message m and gives result

$Result \leftarrow V_{dlp}(param, (Pbo, Pbp), \sigma_p, m)$

In 1996 first time proxy signatures were introduced by Mambo et al[1].He specified seven properties are needed to be fulfilled in proxy signatures which can be used by proxy signer to sign on behalf of original signer however the limitation with this scheme is that an original signer grants or delegates all his rights to proxy signer as a result he can misuse the unlimited delegation capability and another major weakness is that a proxy signer can transfer delegated rights to others.This limitation was overcome by a scheme proposed by Kim et al.(1997)[2] in which the proxy signer was restricted with partial delegation with warrants but it does not support proxy revocation and at tims it becomes important to revoke rights before warrant expires its time limits..Zhang(2008)[3] proposed Non repudiable proxy signature scheme however Ghodosi et al(1999)[4] find limitation and shortcomings in his scheme which were also find by Lee et al(1998)[5].Petersen and Horster(1997)[6] introduced self certified key for delegating capabilities in proxy signature but the scheme is insecure as the original signer may delegate rights without warrants and the proxy signature has no authentic information about proxy signer he can deny from signature creation. Some more limitation of this scheme are specified by Lee et al.[7,8] like the concept[6] makes use of insecure channel and communication cost is also high, all these limitations are because of lack of formalized security notion. Boldyreva et al(2003)[9] proposed secure signature scheme named triple schnorr proxy signature scheme which is an enhancement of scheme introduced by kim(1997)[2] but the major concern is this scheme do not consider warrants which provides unlimited delegation to proxy signer who can misuse it. Malkin et al.(2004)[10] proposed hierarchical model for proxy signatures with warrants based on Kim scheme. Boldyreva et al. (2012)[11] resolved the problems by formalizing the notion of security for proxy signature scheme. Lu et al. (2006) [12] proposed time stamping services for specifying the delegation with expiry time in warrants and in this way supports revocation.

### 3.2 Proxy Signature based on RSA

An original signer selects a public key $Pb_o$ and computes her private key $Pr_o$ as

$Pr_o \leftarrow KG_{rsa}(param, Pb_o)$

A proxy signer selects a public key $Pb_p$ and computes her private key $Pb_p$

$Pr_p \leftarrow KG_{rsa}(param, Pb_p)$

- **Generation of delegation capability**

The signature of an owner $\sigma_o$ on warrant $\omega$ is generated after taking input as param, private key of original signer $Pr_o$ and warrant $\omega$.

$\sigma_o \leftarrow S_{rsa}(param, Pr_o, \omega)$

- **Verification of delegation capability**

It takes input as param, public key of original signer $Pb_o$, signature of owner $\sigma_o$ and warrant $\omega$ and Gives Result as valid or invalid

$Result \leftarrow V_{rsa}(param, Pb_o, \sigma_o, \omega)$

• **Generation of Proxy signature**

Proxy key $\sigma_p$ on message m is generated using message m, parameter param, signature of original signer $\sigma_o$ and private key of proxy signer Prp.

$\sigma_p \leftarrow S_{rsa}(param, Pr_p,(\sigma_o,m))$

• **Verification of Proxy Signature**

It takes as input parameter param, public key of original signer $Pb_o$ and proxy signer $Pb_p$, proxy signature of proxy signer $\sigma_p$ and message m and gives result

$Result \leftarrow V_{rsa}(param, (Pb_o,Pb_p),\sigma_p,m)$

In 1999 Okamoto et al. [13] was the first to introduce proxy signatures based on RSA that reduced the cost of computation and storage and so was found to be suitable for smart cards but the scheme does not provide strong unforgeability. In 2001 Lee at al. [14] proposed strong non designated proxy signature scheme which was proved as insecure by wang et al. (2003) [15]. In 2002 shum el al.[16] introduced another proxy protected proxy signature scheme.In 2003 Shao[17] introduced proxy signature scheme based on factoring integer problem comprising of RSA and Guillou et al.(1990) [18] there is no formal security proof of this scheme. Later Das et al. (2004) [19] proposed proxy signatures with concept of proxy revocation which is very effective provided proxy signers key length should be less than original signer. Zhou et al. (2005) [20] proposed warrant based proxy signature considering random oracle model however Park et al.(2005) [21] identified the short coming of his work. In 2006, Xue, et al. [22] proposed the normal proxy signature scheme and multi-proxy signature scheme based on the difficulty of factoring of large integers but without giving their formal security proofs. In 2009, Shao [23] proposed proxy- protected signature scheme based on RSA. Recently, in 2012, Yong, et al.[24] proposed provably secure proxy signature scheme from factorization.

3.3 Proxy Signature based on Pairing

The original signer generate his public key $Pb_o = H(ID_o)$ using his identity $ID_o$ and computes private key

$Pr_o \leftarrow KG_{prb}(param, Pb_o)$.

The proxy signer generate his public key $Pb_p = H(ID_p)$using his identity $ID_p$ and computes private key

$Pr_p \leftarrow KG_{prb}(param, Pb_p)$.

• **Generation of delegation capability**

The signature of an owner $\sigma_o$ on warrant $\omega$ is generated after taking input as param, private key of original signer $Pr_o$ and warrant $\omega$.

$\sigma o \leftarrow Sprb(param,(ko,ro,co),Pro,\omega)$

• **Verification of delegation capability**

Delegation capability is verified with input as param, public key of original signer $Pb_o$, signature of owner $\sigma_o$ and warrant $\omega$ and Result is obtained as valid or invalid

$Result \leftarrow V_{prb}(param,(Pb_o,pub_{KGC}), \sigma_o,( c_o,\omega))$

• **Generation of proxy Key**

Proxy key $\rho_p$ is generated using parameter param, signature of original signer $\sigma_o$, private key of original signer $Pr_p$, user parameters like signers public key, warrants , random number.

$\rho_p \leftarrow ProxKG_{prb}(param, \sigma_o, Pr_p, user\_param)$

• **Generation of Proxy signature**

Proxy key $\sigma_p$ on message m is generated using proxy key $\rho_p$, message m and parameter param.

$\sigma p \leftarrow Sprb(param, \rho p,(kp,rp),m)$

• **Verification of Proxy Signature $\rho_p$**

It takes as input parameter param, public key of original signer $Pb_o$ and proxy signer $Pb_p$, proxy signaturer $\sigma_p$ and message m and gives result

$Result \leftarrow V_{prb}(param, (Pbo,Pbp, pub_{KGC}), \sigma_p,(c_p,m,\omega))$

Bilinear pairing was first introduced by Menezes et al. (1993) [25] for elliptical curve cryptography. This concept is used for proxy signatures also. Zhang et al.(2003) [26] proposed proxy signatures base on Hess Id however it need secure channel and suffers from key escrow. Lu et al. (2006) [27] proposed proxy signature scheme with designated verifier which is based on CHDP in random oracle model but it needs secure channel, suffers from key escrow and also takes high computation cost. Das et al. (2007)[28] introduced proxy signature scheme based on Hess signature it provides an efficient user revocation without any need of secure channel and also do not suffers from key escrow.

## 4. CONCLUSION

Proxy signatures is a cryptographic technique which has enabled the owner to delegate his signing authority to proxy signer who will have an authority to sign on documents in his absence. In this paper we have explained full delegation ,partial delegation and partial delegation with warrants and have given a survey on proxy signature based on discrete logarithmic problem, RSA and Bilinear pair. Lots of work can be done in this area in order to enhance the authenticity, integrity and security of data. In future we will explore more on Proxy signature with partial delegation and revocation using bilinear pairing and elliptical curve.

## REFERENCES


1. M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures: Delegation of the Power to Sign Messages," IEICE Transactions Fundamentals, vol. E79-A, no.9, pp. 1338-1353, 1996.
2. S. Kim, S. Park, and D. Won, "Proxy signatures revisited," Proceedings of Information and Communications Security (ICICS' 97), LNCS 1334, Springer-Verlag, pp. 223-232, 1997.
3. K. Zhang, "Nonrepudiable proxy signature schemes," 2008. (http://citeseer.nj.nec.com/360090.html/)
4. H. Ghodosi, and J. Pieprzyk, "Repudiation of cheat- ing and non-repudiation of Zhang's proxy signature schemes," Proceedings of Australasian Conference on Information Security and Privacy (ACISP' 99), LNCS 1587, pp. 129-134, Springer-Verlag, 1999.

5. N. Y. Lee, T. Hwang, and C. H. Wang, "On Zhang's nonrepudiable proxy signature schemes," Proceedings of Australasian Conference on Information Security and Privacy (ACISP' 98), LNCS 1438, pp. 415-422, Springer-Verlag, 1998.
6. H. Petersen, and P. Horster, "Self-certified keys concepts and applications," Proceedings of Conference on Communications and Multimedia Security, pp. 102-116, 1997.
7. B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its applications," Proceedings of Symposium on Cryptography and Information Security, pp. 603-608,2001.
8. J. Lee, J. Cheon, and S. Kim, " An analysis of proxy signatures: Is a secure channel necessary?," Proceed- ings of CT-RSA Conference, LNCS 2612, pp. 68-79, Spconcepts for Springer-Verlag, 2003
9. Boldyreva, A. Palacio, and B. Warinschi, "Secure signature schemes for delegation of signing rights",2003. (http://eprint.iacr.org/2003/96/)
10. T. Malkin, S. Obana, and M. Yung, "The hierarchy of key evolving signatures and a characterization of proxy signatures," Proceedings of Eurocrypt' 04, LNCS 3027,Springer-Verlag, pp. 306-322, 2004.
11. A. Boldyreva, A. Palacio, B. Warinschi, "Secure Proxy Signature for Delegation of Signing Rights", Journal of Cryptography volume 5(1), pp. 57-115,2012
12. E. J. L. Lu, and C. J. Huang, "A time- stamping proxy signature scheme using time-stamping service," International Journal of Network Security, vol.2, no. 1, pp. 43-51, 2006.
13. T. Okamoto, M. Tada, and E. Okamoto, "Extended proxy signaures for smart card" Proceedings of Information Security Workshop'99, LNCS 1729, pp. 247-258, Springer-Verlag, 1999.
14. B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strong non-designated proxy signature," Proceedings of Australasian Conference on Information Security and Privacy (ACISP' 01), LNCS 2119, pp.474-486, Springer-Verlag, 2001.
15. G. Wang, F. Bao, J. Zhou, and R. H. Deng, "Security analysis of some proxy signatures," 2003. (http://eprint.iacr.org/2003/196/)
16. K. Shum and V. K. Wei, "A strong proxy signature scheme with proxy signer privacy protection", In: Proceedings of IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE02), (2002)
17. Z. Shao, "Proxy signature schemes based on factoring," Information Processing Letters, vol. 85, pp.137-143, 2003.
18. L. G. Guillou, and J. J. Quisquater. "A 'paradoxical' identity-based signature scheme resulting from zero- knowledge," Proceedings of Crypto' 88, LNCS 403, pp. 216-231, Springer-Verlag, 1990.
19. M. L. Das, A. Saxena, and V. P. Gulati, "An efficient proxy signature scheme with revocation," Informat- ica, vol. 15, no. 4, pp. 455-464, 2004.
20. Y. Zhou, Z. Cao, and Z. Chai, "An efficient proxy- protected signature scheme based on factoring," Pro- ceedings of ISPA Workshops, LNCS 3759, pp. 332-341, Springer-Verlag, 2005.
21. J. H. Park, B. G. Kang and J. W. Han, "Cryptanalysis of Zhou, et al., proxy-protected signature schemes", Appl. Math Comput., vol. 169, no. 1, (2005), pp. 192-197.
22. Q. Xue and Z. Cao, "Factoring based proxy signature schemes", Journal of Comput Appl Math, vol. 195, (2006), pp. 229-241
23. Z. Shao, "Provably secure proxy-protected signature schemes based on RSA", Comput. Electr. Eng., vol. 35, (2009), pp. 497-505
24. Y. Yong, M. Yi, W. Susilo, Y. Sun and Y. Ji, "Provably secure proxy signature scheme from factorization", Mathematical and Computer Modelling, vol. 55, (2012), pp. 1160-1168
25. A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in finite field," IEEE Transactions on Information Theory, vol. 39, no. 5, pp. 1639-1646, 1993.
26. F. Zhang, and K. Kim, "Efficient ID-based blind signature and proxy signature from bilinear pairings," Proceedings of Australasian Conference on Information Security and Privacy (ACISP'2003), LNCS 2727, pp. 312-323,Springer-Verlag, 2003.
27. R. Lu, Z. Cao, and X. Dong, "Efficient ID- based one-time proxy signature and Its application in E-cheque," Proceedings of Cryptology and Network Security, LNCS 4301,pp.153-167, Springer-Verlag,2006
28. M. L. Das, A. Saxena, and D. B. Phatak, "A proxy signature scheme with revocation using bilinear pair- ings," International Journal of Network Security, vol. 4, no. 3, pp. 312-317, 2007.