International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 5, Issue 2, Feb - Mar 2016, 109-122

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

VARIANTS OF BLIND SIGNATURES - A PRACTICAL AUTHENTICATION SCHEME

SANGEETHA JOSE[1] & SUDIN S[2]

[1]Assistant Professor, Department of Information Technology Government Engineering College Idukki, Kerala, India

[2]Head and Assistant Professor, Department of Mathematics Government Engineering College Idukki, Kerala, India

ABSTRACT

Blind signature is a variant of digital signature which helps the user to obtain a signature without giving any information about the message to the signer and the signer cannot tell which session of the signing protocol corresponds to which message. Blind signatures may seem to be a myth; it is a practical reality due to its wide applications in real life like e-coin and e-voting. This paper focuses on the study of variants of blind signatures with its eminent real world applications. It also discuses about future research scope of blind signatures.

KEYWORDS: Blindness, Blind Signature, Unforgeability, Unframeability

I. INTRODUCTION

Data security was a key issue in the ancient era. Data transfer in a secured manner is one of the pivotal tasks in the twenty first century also. Malicious users may eagerly listen to the communication between two entities so that it is very important to ensure security, integrity, authenticity, non-repudiation and privacy of the data. However, when two entities communicate, there is a big risk of this secrecy being violated through leakage of information. Cryptology plays a crucial role to fulfil this security requirement. The fundamental objective of cryptology is the secure communication between sender and receiver through insecure channel. Cryptology is broadly categorised in to cryptography and cryptanalysis. Cryptography is the study of hiding the information which ensures integrity, authenticity and privacy of data. Since perfect security is almost impossible (except for one time pad), cryptanalysis is the study of finding out the weaknesses of the design of existing cryptosystems. Social networks provide abundance of exciting and amazing applications that lead to its rapid growth in this century. Online social networks help to connect to the people and also encourage creating, sharing and collaborating data in an adequate way. However, serious security and privacy problems have prevented the wide adoption of these networks because when secured information falls into a wrong hand that may lead to hazardous situations. Cryptographic measures can overwhelm these concerns to a certain extent. In online social networks a lot of information has to be shared and communicated, while preserving the privacy.

Encryption and digital signatures are the eminent cryptographic primitives which play a crucial role in providing security and authenticity to the data. Encryption provides confidentiality to the transmitted data. Digital signatures are the primitives which sustain authentication and non-repudiation of the data. Digital signature scheme signs documents in such a way that anyone can verify the authenticity of the signature. Due to its relevance, a large number of variants of signature schemes have emerged, like multi-signature [1], ring signature [2], group signature [3], threshold signature [4], aggregate signature [5], proxy signature [6], blind signature [7] etc.

Blind signature is a variant of digital signature that provides assurance of authenticity of a message by the signer

without revealing any information about the signed message. This signature primitive is used in real world applications in which message anonymity is highly important during the signing process, like in e-voting and in digital cash. This motivates us for a detailed study on variants of blind signatures.

This paper is organised as follows. Section II describes the related works with blind signatures. Section III discusses variants of blind signature schemes along with its applications. Section IV concludes with future research scope.

II. RELATED WORKS

The idea of blind signature was put forward by David Chaum (1982) [7]. This is a variant of digital signature in which the content of the message is blinded before it is signed. It also assures the unforgeability property of signature. The provably secure design for blind signature was proposed by Point cheval and Stern [8] in which they defined the security for blind signatures with application to electronic cash. Security arguments for blind signatures are proposed in different papers [9], [10] and [11]. In cryptography, blind signature is a primitive that provides assurance of authenticity of a message by a signer without revealing any information about the message to him. This signature primitive is used in real world applications in which message anonymity is highly important during the signing process, like in e-voting and in digital cash.

Blind signature scheme is a two party protocol between user and signer. Blind signing process has mainly three phases as shown in figure 1.

- Blinding: Blinding process blinds the original message by some random value and outputs blind message. User blinds the message.
- Signing: User sends the blind message to the signer. Signer signs on blinded message and blind signatures are the output after this phase.
- Unblinding: User unblinds the blinded signature and obtains signature on the original message.

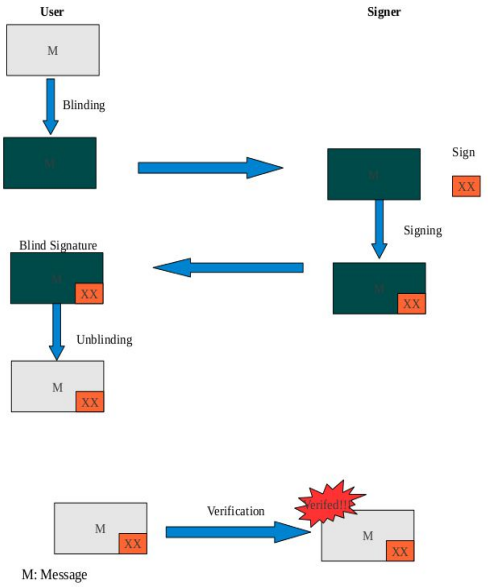

Figure 1: Process of Blind Signature

Blind signature also supports public verification which is similar to the digital signature which ensures the validity of the signature. Blind signature provides unforgeability and blindness properties. Unforgeability ensures that only the signer can make a valid message-signature pair. Blindness shows that signer learns nothing about the content of a message he is helping to sign. Hence the security of blind signature is defined by unforgeability and blindness [[9], [10]].

Blind signatures are widely used in a number of cryptographic applications where signer has to authenticate a message for the user while maintaining privacy of the user's message. Integrity of the e-voting requires that each ballot has to be certified by an election authority without learning voter's selection. Here we need to maintain the anonymity of user's message (i.e., vote) and at the same time it has to be authenticated (signed) by the election authority. This can be achieved with the help of blind signatures because of its blindness and unforgeability properties.

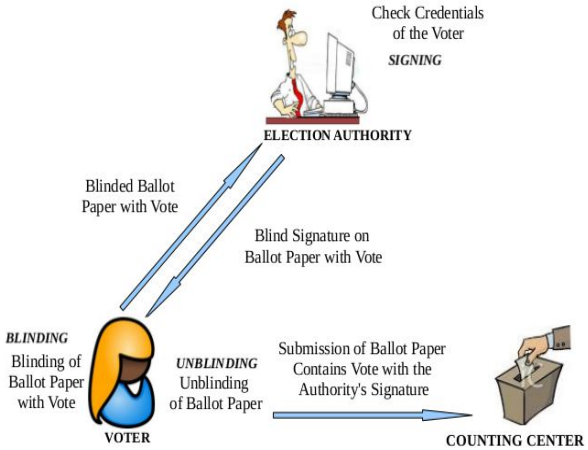

Figure 2: Process of E-Voting

Figure 2 illustrates e-voting process. Voter casts the vote and blinds the vote. Blinded vote will be sent to the election authority. Election authority checks the credentials of the voter and if it is valid then authority signs on the blinded vote. This blinded signature sends back to the voter and voter performs unblinding process and obtains the vote with election authority's signature. Now the voter can submit the valid vote to counting centre. Here each vote is certified by an election authority before it can be accepted for counting and also the authority should not learn anything about the voter's selections.

Chaum [7] introduced the first blind signature scheme based on RSA (Rivest, Shamir and Adleman) signature [12]. Key generation phase is same as that of RSA. As shown in figure 3, p and q are two large prime and N = p x q. ϕ(N) is Euler's totient function which finds the number of positive integers which is smaller and relatively prime to N. Signer's public and secret keys are (N, e) and d respectively where e and d are multiplicative inverses. Blind signing consists of three sub phases blinding, signing and unblinding. Blinding is done with the help of a random value r which produces a blinded message (m'). Signing is done with the help of secret key d of the signer. Signer signs on the blinded message and gives back blind signature (σ') to the user. User unblinds it and obtains the signature (σ) which is the original message with signer's signature. Since d and e are inverses in *modulo* $\phi(N)$, with the help of Euler's Theorem [13] we can easily prove the correctness. In fact, the signature σ obtained in unblinding satisfies

$$\sigma = \sigma' r^{-1} \bmod N$$

$= (m\, r^e \bmod N)^d\, r^{-1} \bmod N$

$= m^d \bmod N$

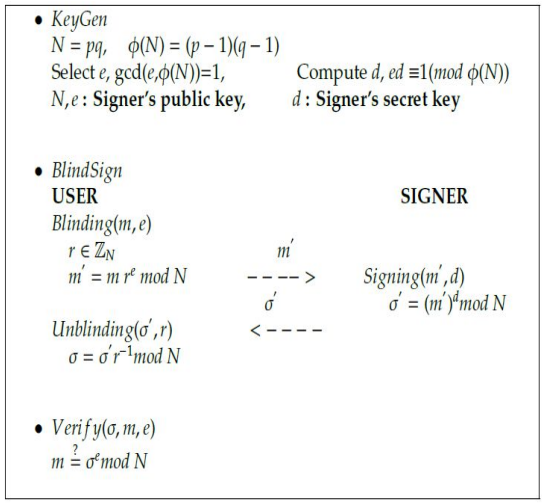

Figure 3: Chaum's Blind Signature Scheme

III. A DETAILED STUDY ON VARIANTS OF BLIND SIGNATURE SCHEMES

Blind signature is a variant of digital signature in which content is blinded before it is signed which is illustrated in Figure 4. That is, signer puts signature on the document without knowing what the document contains and everyone can verify the validity of the signature. It prevents the signer from observing the message it signs.

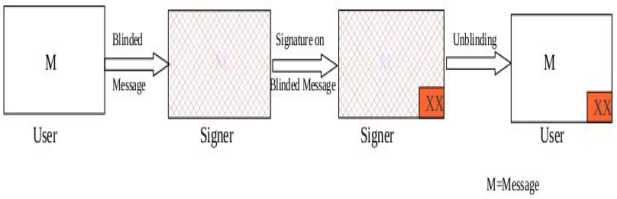

Figure 4: Concept of Blind Signature

As specified in section II Chaum introduced the concept of blind signature which is based on RSA signature with applications in e-voting and payment transactions. Chaum et al. [14] explains the use of blind signature in the scenario of electronic cash and formal proofs for the protocol was left as an open challenge. Two new blind signature schemes based on discrete logarithm problem were designed by Camenisch et al. [15].

A provably secure design for blind signature was elaborated by Point cheval and Stern [8]. They proposed the definition of security for blind signatures with application to electronic cash. They also provided the security proof in random oracle model. Unforgeability of the blind signature was explained with the concept of one-more forgery. Suppose l is an integer which indicates the number of interactions with the signer. After l interactions if user could produce $l + 1$ signature, then there is one-more forgery occurs. They proved that one-more forgery happens only with negligible probability. They had shown that how the witness indistinguishable identification schemes could be converted into blind signature schemes. They also explained Okomoto-Schnorr blind signature and shown its proof of security.

Juels et al. [9] showed that how the security and blindness property for blind digital signatures can be defined by considering an arbitrary one way trapdoor permutation family. They presented the first blind signature scheme with complexity based proof of security. They proved it to be as secure as factoring. They also formally defined the notion of the security of the blind signature scheme. Figure 5 describes the eminent works in blind signatures.

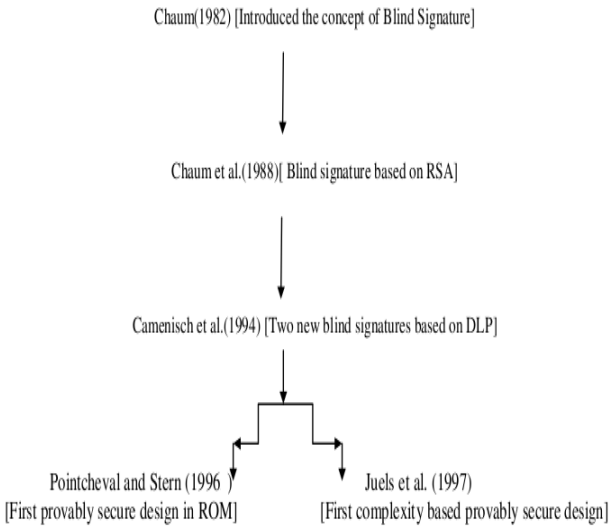

Figure 5: Eminent Works in Blind Signature

Due to extensive use in different applications, different blind signatures and its variants have emerged. Camenisch et al. [16] proposed efficient blind signatures without random oracles. They designed blind signing function as a secure and efficient two-party computation which uses its algebraic properties and paillier encryption scheme. The security of the signature scheme is based on the strong RSA assumption [17] and the hardness of decisional composite residuosity which is commonly used in the proof of the paillier cryptosystems. In short, they elaborated the design of an efficient blind signature scheme which is in standard model.

Okamoto [18] also designed blind and partially blind signatures without random oracles. These signature schemes were secure in the standard model. Okamoto's partially blind signature scheme was the first one which is secure in the standard model. Security proof of these schemes requires the 2SDH (2-variable strong Diffie-Hellman) assumption [19], a stronger variant of the SDH (strong Diffie-Hellman) assumption.

Zhang and Su [20] proposed a short blind signature scheme from bilinear pairings. The size of the signature was short with only half size of the DSA (digital signature algorithm) signature. Since there were no pairings in the blind signing phase and in the verification phase, authors claim that it was more efficient in computation. They also projected out that their scheme was suitable for mobile device and electronic commerce. The security of the scheme was reduced to the computational Diffie Hellman problem in the random oracle model.

There are several Identity (ID) based blind signature schemes in the literature similar to that of public key infrastructure (PKI) based blind signatures. Zhang and Kim [21] proposed the first ID based blind signature scheme which was based on the bilinear pairings. Later Zhang and Kim [22] also proposed an ID based blind signature scheme which was more efficient than Zhang and Kim [21] in computational cost. Galindo et al. [23] explained the generic construction of ID

based blind signature. Gao et al. [24] also proposed a new ID based blind signature scheme based on bilinear pairing. They designed an entirely new scheme which was not based upon any existing ID based signature schemes. The proposed scheme was based on an assumption known as one-more bilinear Diffie-Hellman Inversion (1m-BDHI) assumption. He et al. [25] proposed an identity based blind signature scheme without bilinear pairings.

Lattice-based blind signature is proposed by Rückert [26] by applying hard lattice problems such as the shortest vector problem [27]. Lattice operations are more powerful than modular exponentiation and lattice problems remain hard for quantum and sub exponential time adversaries. Hence, the security proofs based on lattice hard problems has advantages over using the factoring or discrete logarithm problems. They designed a cryptosystem with random oracle model. It was also a blind signature scheme that supports leakage resilience [28].

Over beck [29] proposed a conversion from signature schemes connected to coding theory into blind signature schemes. They explained formal security reductions to combinatorial problems. Author claimed that the blind signature scheme cannot be broken by quantum computers. They presented a blind signature based on syndrome decoding and showed that it was secure against active adversaries as long as some instances of NP (non deterministic polynomial time) hard problems were hard to solve. This blind signature also had two major drawbacks, large signature size and slow blind signature generation.

Partially blind signature was an extension of blind signature schemes which allows a signer to include necessary information in unblinded form like expiration date etc. in the signatures under some agreement with the receiver. There were different partial blind signatures in the literature [[30], [31], [32], [33]]. Partial blind signature can have application with the electronic cash system, which successfully minimises the growth of the bank databases.

Proxy blind signature is a variant form of blind signature which allows delegated signer to generate blind signature on behalf of the original signer [[34], [35], [36]]. It is a combination of proxy signature with blind signature which satisfies the security properties of both proxy and blind signature schemes.

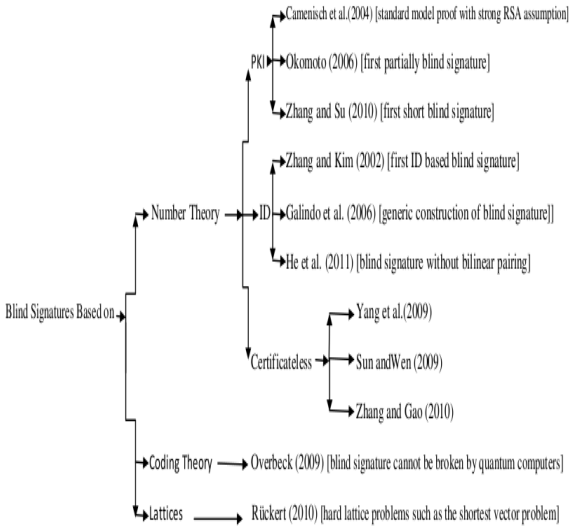

Figure 6: Overview of Different Works in Blind Signature

A blind signature with revocable anonymity and unlink ability is known as fair blind signature. In order to avoid

the misuse of e-cash, an authority or a trustee can link an issuing session to the generated signature and also can trace the signature to the requested user [[37], [38], [39]]. Fuchsbauer and Vergnaud [38] claimed the construction of the first practical fair blind signature scheme and proved its security under standard model.

Blind ring signatures combine properties of both ring signature and blind signature and thus provides a strong notion of anonymity where the privacy of both the identity of the signer and the message is preserved [40]. Blind ring signatures have different applications in multi-authority e-voting and distributed e-cash systems. There are different blind ring signature schemes in the literature [[40], [41], [42]].

Password based signatures are variants of signature scheme in which user's secret signing key is replaced by a password so that it is easy to remember and hence the storage problem can be solved. Gjøsteen and Thuen [43] proposed password based signatures based on RSA [12] and CL (Camenisch and Lysyanskaya) [16] signatures. Since passwords have low entropy, usual password based schemes are vulnerable to offline password attack. Sangeetha Jose et al. [44] proposed a strongly secure password based blind signature (ss-PBBS) that was not susceptible to offline password guessing attack even if the password size is small. Comparison of the strongly secure password based blind signature with other schemes is given in Table 1.

Table 1: Comparison of SS-PBBS with Other Schemes

Scheme	Underlying Signature	Hardness Assumption	Signature Size
Gjøsteen and Thuen (2011) Scheme 1	RSA	RSA known-target inversion	1024 bits
Gjøsteen and Thuen (2011) Scheme 2	CL	es-LRSW	2048 bits
PBBS Scheme Jose *et al.* (2013)	BLS	CDH	170 bits (constraint in password size)
ss-PBBS Scheme	BLS	CDH	170 bits (no constraint in password size)

In identity based encryption (IBE), user gets the secret key from private key generator (PKG). Green and Hohenberger [45] proposed a blind key extraction (BKE) protocol for extracting the secret key of a user in a blinded manner (blinded from PKG). They formalized the above notion as blind IBE which could be used in different applications like privacy preserving delegated keyword search, temporary anonymous identities and so on. Camenisch et al. [46] also designed a committed blind anonymous IBE scheme based on Boyen and Waters [47] anonymous IBE. Lin et al. [48] proposed another BKE protocol for an anonymous IBE by Ducas [49] in which the protocol uses zero knowledge proof of knowledge (ZKPoK) with increased efficiency. Even though there are blind anonymous identity based encryption schemes [[45], [46], [48]], existing systems are complex in their computation and communication cost. Hence Sangeetha Jose et al. [50] proposed a blind anonymous identity based encryption (Π_{BAIBE}) in random oracle model. Comparison of proposed blind anonymous identity based encryption with existing scheme is shown in Table 2.

Table 2: Comparison of Proposed Scheme Π_{BAIBE} with Existing Schemes

Scheme	Number of Secret Key Components	Number of Ciphertext Components	Number of Pairings in Decryption
Camenisch et al. (2009)	5	6	5
Green and Hohenberger (2007)	2	3	2
Lin et al. (2011)	3	4	3
Proposed Scheme (Π_{BAIBE})	2	2	2

The number of cipher text components was less in the proposed scheme. The decryption process also required simple computation as compared with existing schemes.

Certificate less signature scheme overwhelms the drawbacks of public key infrastructure based and identity based signature schemes, since it does not require certificate management as well as it does not possess key escrow problem. Due to its merits, different certificate less blind signatures [[51], [52], [53]] were constructed. Due to the uncertified nature of the public key, an adversary (Type I) in the certificate less system can replace user's public key with another value of his own choice. The second type of adversary (Type II) represents a malicious key generation centre (KGC) who generates partial private key for the users. Yang et al. [51] proposed a certificate less blind signature scheme which is provably secure against Type I and Type II adversaries under random oracle model and claimed that it can be used in e-commerce. Sun and Wen [52] put forwarded two new certificates less blind signature schemes based on Choi et al. [54] certificate less signature scheme. Authors claimed that, these schemes need less computational cost and satisfy the properties of blind signatures. Zhang and Gao [53] also proposed a certificate less blind signature scheme which is proven to be secure in the random oracle model. The security proof was based on computational Diffie-Hellman problem and the bilinear pairing inversion problem (BPI). However these schemes claimed the security without giving detailed mathematical proofs. Hence Sangeetha Jose et al. [55] constructed a new certificate less blind signature scheme (Π_{CLBS}) and proved that it was secure under computational Diffie-Hellman (CDH) and chosen-target CDH assumptions. Comparison of the proposed scheme with existing scheme is shown in Table III.

Table 3: Comparison of Scheme Π_{CLBS} with Existing Schemes

Scheme	Security Proof	Hardness Assumption	Probability (Advantage of the Adversary)
Yang et al. (2009)	Existentially Unforgeable (Only Theorem statement)	Type-1 k-CCA, Type-2 mICDH	No Probability Analysis is given
Sun and Wen (2009) Scheme 1	Unforgeable (similar to Choi et al. (2007)'s CLS scheme)	Type-1 CDH, Type-2 mICDH	No Probability Analysis is given
Sun and Wen (2009) Scheme 2	Unforgeable (similar to Choi et al. (2007)'s CLS scheme)	Type-1 k-CAA, Type-2 mICDH	No Probability Analysis is given
Zhang and Gao (2010)	Unforgeable (Only Theorem statement)	Type-1 q-SDH, Type-2 BPI	No Probability Analysis is given
Scheme(Π_{CLBS})	Strongly Unforgeable (Both Type 1 and 2) Detailed Proof is given	Type-1 CDH and ct-CDH Type-2 ct-CDH	Detailed Probability Analysis is given

IV. CONCLUSIONS AND FUTURE SCOPE

In this paper we explore variants of blind signatures based on number theory, coding theory and lattice based concepts. According to the detailed study, the design of the proposed schemes in the standard model would be a good problem to be work on. Since there is less number of cryptosystems based on lattice concepts, we can also attempt to construct certificate less blind signatures based on lattice based concepts. Even though coding theory assures more efficient cryptosystem, existing coding theory blind signatures has large signature size. It could be a nice solution if we could construct short blind signatures with the help of coding theory. In short, this paper discusses and elaborates variants of blind signatures with its eminent real world applications with future research scope.

REFERENCES

1. Burmester, M., Y. Desmedt, H. Doi, M.Mambo, E. Okamoto, M.Tada, andY.Yoshifuji, "A Structured ElGamal-Type Multisignature Scheme", In H. Imai and Y. Zheng (eds.), Public Key Cryptography, volume 1751 of Lecture Notes in Computer Science(LNCS), Springer 2000, 466–483.
2. Rivest, R. L., A. Shamir, and Y. Tauman, "Howto Leak a Secret", In Advances in Cryptology- ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, volume 2248 of Lecture Notes in Computer Science, Springer, 2001, 552–565.
3. Chaum, D. and E. van Heyst, "Group Signatures", In D. W. Davies (ed.), EUROCRYPT, volume 547 of Lecture Notes in Computer Science, Springer, 1991,257–265.
4. Desmedt, Y. and Y. Frankel, "Threshold Cryptosystems", In G. Brassard (ed.), CRYPTO, volume 435 of Lecture Notes in Computer Science, Springer, 1989, 307–315.
5. Boneh, D., C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps", In EUROCRYPT, In LNCS, volume 2656, 2003, 416–432.
6. Mambo, M., K. Usuda, and E. Okamoto, "Proxy Signatures for Delegating Signing Operation", In L. Gong and J. Stearn (eds.), ACM Conference on Computer and Communications Security, ACM, 1996, 48–57.
7. Chaum, D., "Blind Signatures for Untraceable Payments", In D. Chaum, R. L. Rivest, and A. T. Sherman (eds.), CRYPTO 82. Plenum Press, New York, 1982, 199–203.
8. Pointcheval, D. and J. Stern, "Provably Secure Blind Signature Schemes", In ASIACRYPT, volume 1163 of Lecture Notes in Computer Science, Springer, 1996, 252–265.
9. Juels, A., M. Luby, and R. Ostrovsky, "Security of Blind Digital Signatures (Extended Abstract)", In B. S. K. Jr. (ed.), CRYPTO'97, volume 1294 of Lecture Notes in Computer Science, Springer, 1997, 150–164.
10. Pointcheval, D. and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures", In Journal of Cryptology, volume 13(3), Springer-Verlag, 2000, 361–396.
11. Schröder, D. and D. Unruh, "Security of Blind Signatures Revisited", In M. Fischlin, J. Buchmann, and M. Manulis (eds.), Public Key Cryptography, volume 7293 of Lecture Notes in Computer Science, Springer, 2012, 662–679.

12. Rivest, R. L., A. Shamir, and L.M.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", volume 21, ACM, New York, NY, USA, 1978, 120–126, URL http://doi.acm.org/10.1145/359340.359342.

13. Forouzan, B. A., "Cryptography & Network Security", McGraw-Hill, Inc., New York, USA, 2008, 1st edition, 254–258.

14. Chaum, D., A. Fiat, and M. Naor, "Untraceable electronic cash", In CRYPTO, volume 403 of Lecture Notes in Computer Science, Springer, 1988, 319–327.

15. Camenisch, J., J.-M. Piveteau, and M. Stadler, "Blind signatures based on the discrete logarithm problem", In A. D. Santis (ed.), EUROCRYPT, volume 950 of Lecture Notes in Computer Science, 428-432, Springer, 1994.

16. Camenisch, J. and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps", In Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings, volume 3152 of Lecture Notes in Computer Science, Springer, 2004, 56–72.

17. Bari, N. and B. Pfitzmann, "Collision-free accumulators and fail-stop signature schemes without trees", In W. Fumy (ed.), EUROCRYPT, volume 1233 of Lecture Notes in Computer Science, 480-494, Springer, 1997.

18. Okamoto, T., "Efficient Blind and Partially Blind Signatures Without Random Oracles", In S. Halevi and T. Rabin (eds.), TCC, volume 3876 of Lecture Notes in Computer Science, Springer, 2006, 80–99.

19. Boneh, D. and X. Boyen, "Short signatures without random oracles", In Advances in Cryptology-EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, volume 3027 of LNCS, Springer, 2004, 56–73.

20. Zhang, J. and X. Su, "Another Efficient Blind Signature Scheme Based on Bilinear Map", In 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 2010, 1–4.

21. Zhang, F. and K. Kim, "Id-based blind signature and ring signature from pairings", In Y. Zheng (ed.), ASIACRYPT, volume 2501 of Lecture Notes in Computer Science, 533-547, Springer, 2002.

22. Zhang, F. and K. Kim, "Efficient id-based blind signature and proxy signature from bilinear pairings", In R. Safavi-Naini and J. Seberry (eds.), ACISP, volume 2727 of LNCS, 312-323, Springer, 2003.

23. Galindo, D., J. Herranz, and E. Kiltz, "On the Generic Construction of Identity-Based Signatures with Additional Properties", In X. Lai and K. Chen (eds.), ASIACRYPT, volume 4284 of Lecture Notes in Computer Science, Springer, 2006, 178–193.

24. Gao, W., G. Wang, X. Wang, and F. Li, "One-round id-based blind signature scheme without ros assumption", In S. D. Galbraith and K. G. Paterson (eds.), Pairing, volume 5209 of Lecture Notes in Computer Science, 316-331, Springer, 2008, 316–331.

25. He, D., J. Chen, and R. Zhang, "An efficient identity-based blind signature scheme without bilinear pairings", volume 37, Pergamon Press, Inc., Tarrytown, NewYork, USA, 2011, 444–450.

26. Rückert, M., "Lattice-based blind signatures", In M. Abe (ed.), ASIACRYPT, volume 6477 of Lecture Notes in Computer Science, 413-430, Springer, 2010.
27. Ajtai, M., "The shortest vector problem in l2 is np-hard for randomized reductions(extended abstract)", In Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, STOC '98, ACM, New York, NY, USA, 1998, 10–19.
28. Katz, J. and V. Vaikuntanathan, "Signature schemes with bounded leakage resilience", In M. Matsui (ed.), ASIACRYPT, volume 5912 of Lecture Notes in Computer Science, pages 703-720, Springer, 2009.
29. Overbeck, R., "A step towards QC blind signatures", IACR Cryptology ePrint Archive, 2009, 102.
30. Abe, M. and E. Fujisaki, "How to date blind signatures", In Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, Proceedings, pages 244–251, 1996.
31. Abe, M. and T. Okamoto, "Provably secure partially blind signatures", In Advances in Cryptology - CRYPTO2000, Proceedings of 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000.
32. Chow, S. S. M., L. C. K. Hui, S. Yiu, and K. P. Chow, "Two improved partially blind signature schemes from bilinear pairings", In C. Boyd and J. M. G. Nieto (eds.), Information Security and Privacy, 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Proceedings, pages 316–328, volume 3574 of Lecture Notes in Computer Science, Springer, 2005.
33. Liu, J., Z. Zhang, R. Sun, and K. S. Kwak, "Certificateless partially blind signature", In L. Barolli, T. Enokido, F. Xhafa, and M. Takizawa (eds.), 26th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012, Fukuoka, Japan, March 26-29, pages 128–133, IEEE, 2012.
34. Kar, B., P. Sahoo, and A. Das, "A secure proxy blind signature scheme based on dlp", In International Conference on Multimedia Information Networking and Security (MINES), 2010, 477–480.
35. Tan, Z., Z. Liu, and C. Tang, "Digital proxy blind signature schemes based on dlp and ecdlp", mm research preprints. 2002, 212 – 217.
36. Sun, H. and B. Hsieh, "On the security of some proxy blind signature schemes", In J. M. Hogan, P. Montague, M. K. Purvis, and C. Steketee (eds.), Australasian Information Security Workshop (AISW2004), the Australasian Workshop on Data Mining and Web Intelligence (DMWI2004), and the Australasian Workshop on Software Internationalisation (AWSI2004), pages 75-78, volume 32 of CRPIT, Australian Computer Society, 2004.
37. Stadler, M., J.-M. Piveteau, and J. Camenisch, "Fair blind signatures", In Advances in Cryptology - EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, volume 921 of Lecture Notes in Computer Science. Springer, 1995.
38. Fuchsbauer, G. and D. Vergnaud, "Fair blind signatures without random oracles", In D. J. Bernstein and T. Lange (eds.), Progress in Cryptology - AFRICACRYPT 2010, Third International Conference on Cryptology in Africa, Stellenbosch, South Africa, May 3-6, volume 6055 of Lecture Notes in Computer Science, 16–33, Springer, 2010.

39. Abe, M. and M. Ohkubo, "Provably secure fair blind signatures with tight revocation", In Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, Proceedings, pages 583–602, 2001.

40. Ghadafi, E., "Sub-linear blind ring signatures without random oracles", In M. Stam (ed.), Cryptography and Coding - 14th IMA International Conference, IMACC 2013, Oxford, UK, December 17-19, Proceedings, volume 8308 of LNCS, 304–323, Springer, 2013.

41. Herranz, J. and F. Laguillaumie, "Blind ring signatures secure under the chosen-target cdh assumption", In S. K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, and B. Preneel (eds.), Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings, volume 4176 of Lecture Notes in Computer Science, 117–130, Springer, 2006.

42. Zhang, J., H. Chen, X. Liu, and C. Liu, "An efficient blind ring signature scheme without pairings", In H. T. Shen, J. Pei, M. T. Özsu, L. Zou, J. Lu, T. W. Ling, G. Yu, Y. Zhuang, and J. Shao (eds.), Web-Age Information Management 2010, International Workshops: IWGD 2010, XMLDM 2010, WCMT 2010, Jiuzhaigou Valley, China, July 15-17, 2010, Revised Selected Papers, volume 6185 of Lecture Notes in Computer Science, pages 177-188, Springer, 2010.

43. Gjøsteen, K. and Ø. Thuen, "Password-Based Signatures", In S. Petkova-Nikova, A. Pashalidis, and G. Pernul (eds.), EuroPKI, volume 7163 of Lecture Notes in Computer Science, Springer, 2011, 17–33.

44. Jose, S., P. M. K., and C. P. Rangan, "Strongly Secure Password Based Blind Signature for Real World Applications". Infocommunications Journal, co-sponsored by IEEE Communications Society and IEEE Hungary Section, Volume V, Number 3, Pages 22-29, September 2013.

45. Green, M. and S. Hohenberger, "Blind Identity-Based Encryption and Simulatable Oblivious Transfer", In K. Kurosawa (ed.), ASIACRYPT, volume 4833 of Lecture Notes in Computer Science. Springer, 2007, 265–282.

46. Camenisch, J., M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data", In S. Jarecki and G. Tsudik (eds.), Public Key Cryptography, volume 5443 of Lecture Notes in Computer Science, Springer, 2009, 196–214.

47. Boyen, X. and B.Waters, "Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles)", In Advances in Cryptology—CRYPTO 2006, volume 4117 of Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2006, 290–307.

48. Lin, H., S. S. M. Chow, D. Xing, Y. Fang, and Z. Cao, "Privacy-Preserving Friend Search over Online Social Networks", Cryptology ePrint Archive, Report 2011/445, 2011.

49. Ducas, L., "Anonymity from Asymmetry: New Constructions for Anonymous HIBE", In J. Pieprzyk (ed.), CT-RSA, volume 5985 of Lecture Notes in Computer Science, Springer, 2010, 148–164.

50. Jose, S., P. M. K., and C. P. Rangan, "A Privacy Preserving Profile Searching Protocol in Cloud Networks", Proceedings of International Conference on Cloud Security Management, ICCSM- 2013, Centre for Information Assurance and Cyber Security, University of Washington, Seattle, USA, October 17-18, Pages 99-105, 2013.

51. Yang, X., Z. Liang, P.Wei, and J. Shen, "A provably secure certificateless blind signature scheme", In International Symposium on Information Assurance and Security, volume 2, IEEE Computer Society, Los Alamitos, CA, USA, 2009, 643–646.

52. Sun, S. and Q. Wen, "Novel efficient certificateless blind signature schemes", In International Symposium on Computer Network and Multimedia Technology, CNMT 2009, 2009, 1–5.

53. Zhang, J. and S. Gao, "Efficient provable certificateless blind signature scheme", In Proceedings of International Conference on Networking, Sensing and Control,ICNSC 2010, 2010, 292–297.

54. Choi, K. Y., J. H. Park, J. Y. Hwang, and D. H. Lee, "Efficient certificateless signature schemes", In J. Katz and M. Yung (eds.), Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings, volume 4521 of Lecture Notes in Computer Science, 443–458, Springer, 2007.

55. Jose, S., Gautam, A. and C. P. Rangan, "A New Certificateless Blind Signature Scheme", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Volume 5, Number 1, Pages 122-141, 2014.