ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 10, pp. 20880-20884, October, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

DIGITAL SIGNATURE SCHEMES: A COMPARATIVE STUDY BETWEEN NUMBER THEORETIC AND LATTICE BASED CRYPTOGRAPHY

Manoj Kumar Misra[1]., Atul Chaturvedi[2] and Tripathi S. P[3]

[1]Department of Computer Science, PSIT, Kanpur, India
[2]Department of Mathematics, PSIT, Kanpur, India
[3]Department of Computer Science, IET, Lucknow, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0810.0978

ARTICLE INFO

Article History:

Received 05th July, 2017
Received in revised form 21st August, 2017
Accepted 06th September, 2017
Published online 28th October, 2017

Key Words:

Digital Signature NTRU, Lattice Based Cryptography, Complexity

ABSTRACT

A digital signature is a mathematical scheme for verifying the authenticity of a digital message or documents. It is used to authenticate the identity of the sender and it confirms the document or message received by the receiver is unaltered. The importance of authentication is increasing due to increase of online transactions over the internet. There is a need to develop a framework for the authentication of computer-based information. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for any electronic transaction like software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. Various asymmetric cryptosystems create and verify digital signatures using different algorithms and procedures. This paper is a survey of various Digital Signature schemes, number theoretic based (RSA, DSA and EIGamal) as well as lattice based cryptography. Lattice-based cryptographic constructions are based on the presumed hardness of lattice problems. The goal of this paper is to make a comparative study between number theoretic and lattice based digital signature schemes.

INTRODUCTION

Digital signature has been the most attractive research field of public key cryptography since it was firstly introduced by Diffie and Hellman [5] in 1976. One of the standard mathematical settings to construct cryptographic algorithms is the discrete logarithm. based on which, a vast variety of signature schemes [24,25,26,28,41] have been presented in literature. The most expensive computational component is Discrete logarithm in the public key cryptography. It increases the computational complexity[38] and dominates the computational cost of public key cryptographic schemes. A lot of work has been done for improving the performance of cryptographic algorithms by reducing the number of exponentiations. Especially, for embedded systems like mobile environment, exponentiation would consume the power the battery which is very limited. Reducing the number of exponentiation will increase battery life. So, the lesser the number of exponentiations [42,43], performance enhances. It is the area where a 20% improvement would be very welcome and a 55-65% improvement would be great achievement. Lattice-based cryptography promises a strong security guarantee and also reduces no of computations [29,30,31,32,39]. Normally all other cryptographic constructions are based on average-case hardness. For instance, breaking a cryptosystem based on factoring might imply the ability to factor some numbers chosen according to a certain distribution, but not the ability to factor all numbers There are currently no known quantum algorithms for solving lattice problems that perform significantly better than the best known classical algorithms.

The rest of this paper is organized as follows. Section 2 introduces number theoretic digital signature schemes. In Section 3, we describe lattice based digital signature schemes. In Section 4, we are giving a comparative advantages of using lattice based signature schemes. Finally, some conclusions are drawn in Section 5.

Digital Signature Schemes: An Overview

Digital signature scheme consist of three phases, key generation algorithm, signing algorithm, sign and verification algorithm. In an public key signature schemes the private-key is used to create it, and the public-key verifies it only the owner (of the private-key) can create the digital signature, hence it can be used to verify who created a message anyone knowing the

Corresponding author:* **Manoj Kumar Misra
Department of Computer Science, PSIT, Kanpur, India

public key can verify the signature Normally whole message is not signed, Here we are going to discuss some well known number theoretic digital signature schemes.

RSA

RSA encryption and decryption are commutative, hence it may be used directly as a digital signature scheme[40]. To sign a message, compute: $S = M^d \pmod{R}$. To verify a signature, compute:

$M = S^e \pmod{R} = M^{ed} \pmod{R} = M \pmod{R}$ .Thus know the message was signed by the owner of the public-key would seem obvious that a message may be encrypted, then signed using RSA without increasing it size but have blocking problem, since it is encrypted using the receivers modulus, but signed using the senders modulus (which may be smaller) several approaches possible to overcome this more commonly use a hash function to create a separate MDC which is then signed

El Gamal Signature Scheme

ElGamal encryption algorithm[24,45] is not commutative, a closely related signature scheme exists In this scheme given prime p, public random number g, private key is x, public key is (y, g, p) .compute $y = g^x \pmod{p}$ .p must be large enough so discrete log is hard. to sign a message M.choose a random number k, $\gcd(k, p-1) = 1$ .compute $a = g^k \pmod{p}$. Extended Euclidean (inverse) algorithm can be used to solve $M = x.a + k.b \pmod{p-1}$. The signature is (a, b) , k must be secret. To verify a signature (a, b) confirm $y^a.a^b \pmod{p} = g^M \pmod{p}$.

DSA (Digital Signature Algorithm)

DSA is a variant on the ElGamal and Schnorr algorithms[45].In DSA $p = 2^L$,a prime number, where L= 512 to 1024 bits and is a multiple of 64 .q is a 160 bit prime factor of $p-1$. $g = h^{(p-1)q}$, where h is any number less than p-1 with $h^{(p-1)q} \pmod{p} > 1$ .x is a number less than $q.y = g^x \pmod{p}$ .to sign a message M .generate random k, $k < q$ Compute $r = (g^k \pmod{p}) \pmod{q}$, $s = k^{-1} sha(M) + x.r \pmod{q}$. signature is (r, s). To verify a signature $w = s^{-1} \pmod{q}$, $u_1 = (SHA(M).w) \pmod{q}$. if $v = r$ then the signature is verified.,

Schnorr Signature scheme: It combines ideas from ElGamal and Fiat-Shamir schemes. It uses exponentiation mod p and mod q. Most of the computation can be completed in a pre-computation phase before signing. For the same level of security, signatures[16,45] are significantly smaller than with RSA.

Digital Signature Schemes (Using Lattice Cryptography)

A lattice is a set of points in n-dimensional space with a periodic structure. Formally a lattice L is defined as $L = \sum_{i=1}^{n} x_i b_i$ where $x_i \in z$ and $b_1, b_2 .. b_n \in R^n$ are linearly independent vectors, known as basis vectors. Lattice cryptography has its roots in a breakthrough discovery of Ajtai [37] which connected the worst-case and average-case complexity of certain lattice problems. As cryptography relies on hard-on-average problems (e.g., when a key is chosen at random, the corresponding cryptographic function should be hard to break), Ajtai's discovery identified lattices as ideal objects to base cryptography on. Initially a subject of mostly complexity theoretical investigations, lattice cryptography is today one of the hottest and fastest moving areas of mathematical cryptography. Two factors recently contributed to bringing lattice cryptography under the spotlight. The increasing number of rich cryptographic primitives [10,16,18,19], encryption secure against key leakage attacks [22,27,28], or even fully homomorphic encryption [17,44]) which can be based on the conjectured hardness of lattice problems, and the potential efficiency and parallelizability of lattice based constructions[35,36], compared to traditional cryptographic primitives based on number theory. Finally, as an added bonus, lattice cryptography appears to be resistant to quantum algorithms, and (in contrast to traditional cryptography based on factoring or elliptic curves) would remain secure even if large scale quantum computers were to be built. Here we are going to give a brief survey of lattice based signature schemes in two phases. First phase includes the signature schemes primarily given and second phase represents the practical lattice based schemes.

First phase lattice based signature schemes The cryptosystems GGH [22] and NTRUEncrypt [28] were among the first, which are based on solving the approximate closest vector problem. NTRUSign [27] was generated by taking the basis of DSS form of GGH cryptosystem. Which combined almost the entire design of GGH but uses the NTRU lattices employed in NTRU Encrypt. Before NTRUSign, NSS [26], was broken by Gentry et al. [21] and NTRUSign was also having the same problem with works by Nguyen and Regev, they recovered the secret-key with around four hundred signatures. So it was clear by the experimental work of Nguyen and Regev that NTRUSign is absolutely insecure [12]. After this Hash-and-Sign Signatures were came in the picture. DSSs based on the hash-and-sign process follow seminal work by Diffie and Hellman [9]. The concept follows the criterion that a message should be hashed before being signed. That is, to sign a message, first hash μ to some point $h = H(\mu)$, which should be in the range of the trapdoor function f. Once the message has been hashed, it is signed $s = f^{-1}(h)$ and a verification algorithm checks that $f(s) = H(\mu)$ to confirm whether (μ, s), is a valid message/signature pair. This results to the first proposal by Gentry et al. [20] (GPV), showing a DSS based on the hardness of lattice problems. Most important part of the scheme is the design of trapdoor functions with the required property that every output value has several pre images, the Gaussian

sampling algorithm and also the use of modular lattices. Another scheme by Micciancio and Peikert [34,36] also follows hash-and-sign, introducing a relatively efficient trapdoor than the one used in GPV. Improvements to the key generation were also made by Alwen and Peikert [4].Another way of constructing a DSS is to first build an identification scheme of a some form, then converting it into a DSS by means of the Fiat-Shamir transformation [1,15] Identification schemes are used between two parties, where one party needs to convince the other party they are whom they claim to be. The technique can be observed by considering Schnorr's protocol, a frequently used proof of knowledge protocol based on the intractability of the discrete logarithm problem. Fiat-Shamir transformations are possible in Lattice-based signature schemes only due to research by Lyubashevsky *et al*. [29,30,31,32]. The procedures in the first publication by Lyubashevsky are shown to be based on SIS, that is, if a solution is found for the DSS then a solution is also found for SIS. The first step taken in this scheme is to first construct a lattice-based identification scheme whereby the challenge is treated as a polynomial in R. The security of the identification scheme is dependent on the hardness of finding the approximate shortest vector in the standard model as well as the random oracle model

Practical Instantiations of Ideal Lattice-Based Fiat-Shamir Signatures This section introduces the ideal lattice-based Fiat-Shamir signature schemes by Guneysu et al. [23] (GLP) and Ducas et al. [11] (BLISS) in more detail, whilst also examining the computational efficiency of each of their components. The reasons for the discussion of GLP and BLISS and common building blocks are that both schemes have been extensively analysed by implementers and currently offer the best trade-off between signature and key sizes as well as security. Thus they are currently considered to be the most practical lattice-based signature schemes.

GLP. The instantiation based on ideal-lattices by Guneysu et al[23].(GLP) follows the signature scheme of Lyubashevsky and specifically targets reconfigurable hardware and constrained devices. This is done by favouring uniformly random distributed noise over Gaussian noise for secret-keys and masking values, and by basing the hardness assumption on an aggressive version of the decisional ring-LWE problem.. The GLP scheme has currently been implemented on reconfigurable hardware , CPUs and microcontrollers..

BLISS. The most efficient instantiation of the BLISS signature scheme [11] is based on ideal-lattices [2,14,33] with the BLISS KeyGen, Sign and Verify algorithms. The rejection sampling has been optimized so that the number of times we need to reject is diminished using a bimodal distribution. The key generation has also been updated to generate the signature using NTRU ideas.

Recently various improvements [2, 3, 14, 33] came over these signature schemes. Practical implementation [46] shows that in future lattice based signature schemes can replace traditional cryptographic schemes and going to play vital role against quantum computers.

Comparative Pros and Cons of Using Lattice Based Cryptography

Working with cipher text: It is clear from Gentry's recent research [17] of a fully homomorphic encryption scheme, that computations can be done on cipher texts without converting them to plaintext. The advantage of this is very clear; suppose we want to search something by submitting a query on search engine then it can be solved by using encrypted query without knowing the actual query. In online services like financial transactions it can play a vital role..

Key randomness. If the secret key is not completely random, it can result to compromise security. The problems based on lattice cryptography works on imperfect keys.so it is robust against key leakage[22].The cryptographers community was trying to find the possibility of imperfect keys from a long time. Now lattice cryptography is enabling this,which can play vital role in the field of cryptography.

Optimized Efficiency. Since Lattice cryptography uses small numbers and matrix multiplication can be done in parallel[31].it can provide remarkable advantage against traditional cryptography in case of basis,which is applicable even for basic encryption or digital signature. Their implementation is also easy both in software or hardware without the use of arbitrary precision arithmetic libraries. Most lattice functions operate on vectors and matrices, which can be executed in parallel

Challenges faced by lattice cryptography. Recent developments[2,14,33] shows that it is a very attractive area that will play vital role in cryptography. But there are different types of challenges also.

- To achieve better security, first important thing is to get understanding of the complexity of current lattice problems. recent research[46] shows there is a gap between theoretical faster algorithms and the reality when implemented practically. Estimation of key sizes is also of great concern to get security up to a appropriate level.
- Lattices are represented by a $n \times n$ matrix .Since only one row of the matrix is required to be stored and other rows can be obtained by various algebraic operations on them. So representations become linear in n. In cryptographic constructions, we can get quadratic or even linear running complexity[6,7,8].To make it practical reality the overhead constants hidden by the asymptotic notations need to be reduced. Thus there is a need to work on algorithms to make effective use of algebraic lattices.

CONCLUSION

Digital signature enhances more security and guarantees efficient and powerful message security mechanism. Today digital signatures are under way and can only be seen as an amendment to traditional procedures. In the future digital signature will get more and more importance to guarantee an efficient action of public authorities. The security standard has to be followed to the computer systems that get increasingly. In this paper we have discussed he concept of digital signature schemes using Cryptography which covers the number theoretic as well as lattice based digital signature schemes of

system based on the kind of key and a few algorithms such as RSA, DSA ,Elgamal and Lattice based schemes.. We studied in detail the mathematical foundations of various algorithms for generation of keys and verification of digital signatures .from this comparative study we found that lattice based signature schemes have a great future specially when quantum computers becomes a reality.

References

1. M. Abdalla, J. H. An, M. Bellare, C. Namprempre. 2002. From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security. In EUROCRYPT. 418-433
2. S.Akleylek,N.Bindel,J.Buchmann,J.Kramer,G.A.Marson .2016.An efficient Lattice based signature scheme with provably secure instantiation.in progress in cryptology Africacrypt 2016 pp-44-60.
3. E. Alkim, N. Bindel, J. Buchmann, and O. Dagdelen. TESLA: tightly-secure efficient signatures from standard lattices. IACR Cryptology ePrint Archive, 2015:755, 2015.
4. J. Alwen, C. Peikert. 2011. Generating Shorter Bases for Hard Random Lattices. Theory Comput. Syst. 48, 3 (2011), 535-553
5. M.Bellare,R.Canetti, H.Krawczyk: Keying hash functions for message authentication. In Advances in Cryptology - CRYPTO'96 (Berlin, New York, Tokyo, 1996) vol. 1109 of Lecture Notes in Computer Science Springer-Verlag.
6. J. Beuchat, N. Sendrier, A. Tisserand, G. Villard, et al. FPGA implementation of a recently published signature scheme. Rapport de Recherche RR LIP 2004-14,2004
7. J. Buchmann, A. May, and U. Vollmer. Perspectives for cryptographic long-term security. Commun. ACM, 49:50{55, September 2006
8. Y. Chen and P. Q. Nguyen. BKZ 2.0: Better lattice security estimates. In ASI-ACRYPT, pages 1-20, 2011.
9. W.Diffie & M.Hellman, New directions in cryptography, IEEE Trans. Inform. Theory,22(6),1976,644-654
10. L.Ducas, V. Lyubashevsky, and T. Prest. Efficient identity-based encryption over NTRU lattices. In Sarkar and Iwata [SI14], pages 22-41.
11. L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. 2013. Lattice Signatures and Bimodal Gaussians. In CRYPTO (1). 40-56. Full version: https://eprint.iacr.org/2013/383.pdf
12. L. Ducas, P. Q. Nguyen. 2012b. Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures. In ASIACRYPT. 433-450.
13. T. Eisenbarth, T. G.uneysu, S. Heyse, and C. Paar. Microeliece: Mceliece for embedded devices. In Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, CHES '09, pages 49-64, Berlin, Heidelberg, 2009.Springer-Verlag.
14. T.Espitau,P.A. Fouque,B. Gerard,M. Tibouchi. Loop abort faults on lattice based Fiat-Shamir & Hash'n sign signatures. https://eprint.iacr.org/2016/449.pdf
15. A.Fiat, A. Shamir. 1986. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In CRYPTO. 186-194.
16. B. A. Forouzan, "Cryptography and Network Security", Special Indian Edition, The McGraw- Hill companies, New Delhi, 2007
17. C. Gentry. Fully homomorphic encryption using ideal lattices. In Proceedings of STOC, pages 169-178,2009.
18. C.Gentry, J. Jonsson, J. Stern, M. Szydlo. 2001. Cryptanalysis of the NTRU Signature Scheme (NSS). In ASIACRYPT. 1-20.
19. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In STOC, pages 197-206, 2008.
20. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions In R. E. Ladner and C. Dwork, editors, *40th ACM STOC*, pages 197-206, Victoria, British Columbia, Canada, May 17-20, 2008. ACM Press. 2
21. C. Gentry, M. Szydlo. 2002. Cryptanalysis of the Revised NTRU Signature Scheme. In EUROCRYPT. 299-320.
22. O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In CRYPTO, pages 112-131, 1997
23. T. Güneysu, V. Lyubashevsky, T. Pöppelmann. 2012. Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems. In CHES. 530-547.
24. R.Haraty, O.Otrok and A.N.El-Kassar,2004.A comparative study of ElGamal based cryptographic algorithm. Proc. Sixth Intl. Conf. Enterprise Information Systems (ICEIS 2004),3:79-84
25. J. Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In L.R. Knudsen, editor, Proc. of Eurocrypt '02, volume 2332 of LNCS, pages 83-107.
26. J. Hoffstein, J. Pipher, J. H. Silverman. NSS: A Lattice-Based Signature Scheme in EUROCRYPT. 211-228.
27. J. Hoffstein, N.H.Graham, J. Pipher, J. H. Silverman, W. Whyte. 2003. NTRUSign: Digital Signatures Using the NTRU Lattice. In CTRSA. 122-140.
28. J.Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In ANTS, pages 267-288, 1998.
29. V. Lyubashevsky. Lattice signatures without trapdoors. In EUROCRYPT, 2012.Full version at http://eprint.iacr.org/2011/537
30. V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In ICALP (2), pages 144-155, 2006
31. V. Lyubashevsky and D. Micciancio. Asymptotically efficient lattice-based digital signatures. In TCC, pages 37-54, 2008
32. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In EUROCRYPT, pages 1-23, 2010.
33. C.A.Melchor, X.Boyen, J.C. Deneuville, P.Gaborit. Sealing the leak on NTRU signatures. M. Mosca(ED): PQ Crypto 2014, LNCS 8772, PP.1-21,2014.

34. D. Micciancio, C. Peikert. 2012. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In EUROCRYPT. 700-718
35. D. Micciancio and O. Regev. Lattice-based cryptography. In D. J. Bernstein, J. Buchmann, and E. Dahmen, editors, Chapter in Post-quantum Cryptography, pages 147-191. Springer, 2009
36. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In EUROCRYPT, 2012. Full version at http://eprint.iacr.org/2011/501
37. Mikl_os Ajtai. Generating hard instances of lattice problems (extended abstract). In Gary L. Miller, editor, STOC, pages 99-108. ACM, 1996
38. Nathanson, Melvyn, B., Elementary Methods in Number Theory, Springer, 2000.
39. P. Nguyen and O. Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology*, 22:139-160, 2009
40. Rivest, R.L., Shamir, A., and Adleman, L.," A method of obtaining Digital Signatures and Public key cryptosystems",Comm.ACM,21,1978
41. M. D. Ryan: Public Key Encryption, Lecture Notes, University of Birmingham (2004).
42. P. Shor. Algorithms for quantum computation: discrete logarithms and factoring In Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, pages 124-134. IEEE, 1994.
43. D. Suzuki. How to maximize the potential of FPGA resources for modular exponentiation. Cryptographic Hardware and Embedded Systems-CHES 2007, pages 272-288, 2007.
44. M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In Proceedings of Eurocrypt, LNCS. Springer, 2010.
45. William Stallings, Cryptography and Network Security: Principles and practice. Tsinghua press, 2002, 253-299.
46. Y.Yuan, C.Cheng, S.Kiyonmoto, Y.Miake, T.Takagi. 2016.portable implementation of Lattice-based cryptography using java script. *International journal of networking and computing*, volume 6, number 2 pages 309-327.

How to cite this article:

Manoj Kumar Misra *et al*.2017, Digital Signature Schemes: A Comparative Study Between Number Theoretic And Lattice Based Cryptography. *Int J Recent Sci Res.* 8(10), pp. 20880-20884. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0810.0978

****