Practical Lattice-based Digital Signature Schemes

J. Howe[1], T. Pöppelmann[2], M. O'Neill[1], E. O'Sullivan[1], T. Güneysu[2]
[1] Centre for Secure Information Technologies (CSIT), Queen's University Belfast, UK
[2]Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany

Abstract: Among the various post-quantum techniques that exist (such as multivariate, code or hash-based), the most promising is lattice-based cryptography, which has become a very viable alternative to number-theoretic cryptography. Its main advantage is that it allows for extended functionality and is, at the same time, more efficient for the basic primitives of public-key encryption and digital signatures. The focus of this presentation will be to survey recent developments in lattice-based digital signature schemes and in particular practical schemes that have been shown to improve upon the performance of equivalent RSA designs. Propositions for future research areas that are essential for the continued development of lattice-based cryptography will also be discussed.

1 Introduction

With the onset of quantum computers ever looming, the computational power it could provide would cause instant insecurity to many of today's universally used cryptographic schemes by virtue of Shor's [1] algorithm. Specifically, schemes based on the discrete-logarithm problem or number-theoretic hard problems, which subsume almost all public-key encryption schemes used on the Internet, including elliptic-curve cryptography (ECC), RSA and DSA would be vulnerable. Accordingly, this has motivated the post-quantum era of cryptography, which refers to the construction of cryptographic algorithms to withstand quantum reductions. Amongst many important areas in post-quantum research (such as multivariate, code or hash-based) lattice-based cryptography is disputably the most auspicious. Lattice-based cryptographic primitives can be utilised to form more advanced schemes, while digital signatures and public-key encryption based on lattices are now more practical than RSA-based equivalent schemes. Computational problems that exist within the lattice environment, such as finding the shortest vector (SVP) or finding the closest vector (CVP) are thought to be immune to quantum reductions [2,3] which imply its conjectured intractability. Such properties show promise, with regards to security and practicability, for replacing current encryption schemes that would be susceptible to attacks in a post-quantum world.

In recent years there has been a tremendous growth in lattice-based cryptography as a research field. As a result, concepts such as functional encryption [4], identity-based encryption [5, 6], attribute-based encryption [7], group signature schemes [8-10] and fully homomorphic encryption [11, 12] have been developed. On the practical front, some constructions of public-key encryption schemes and digital signature schemes based on lattice problems are now more practical than traditional schemes based on RSA. The most recent implementation of a lattice-based encryption scheme in hardware is shown by Roy et al. [13] with results outperforming those of RSA. More specifically, the scheme shows performances an order of magnitude faster in comparison to RSA, for a higher security level, and with the added properties of consuming less resources and greater adaptability for scaling. With regards to digital signature schemes, the two most notable are by Güneysu et al. [14] and Pöppelmann et al. [15] with the former implementation resulting in a 1.5x speed improvement compared to an equivalent RSA design, and the latter scheme being faster, consuming less resources, needing less iterations and attaining a higher security level (80-bit vs. 128-bit) in comparison to the former scheme. The first use of lattices as a cryptographic primitive is due to Ajtai [16], proposing a problem now known as the Short Integer Solution (SIS) problem. The concept remained purely academic until recently due to its limited capabilities and inefficiencies; lattice-based cryptography has now become available as a future alternative to number-theoretic cryptography. Recent research allows virtually any cryptographic primitive, such as those already discussed as well as collision resistant hash functions and oblivious transfers, to be built on the hardness of lattice problems. Also, there has been a transition into a particular class of lattices, predominantly ideal lattices, as a source of computational hardness. Although the robustness of this hardness assumption, in comparison to general lattices, has not been explicitly proven, it is generally considered that most problems still remain hard using ideal lattices [17, 18]. Additionally, using ideal lattices offers a significant speed-up and reduction in key sizes for almost all cryptographic protocols, in particular, in encryption schemes and digital signatures. However, it will be some time before lattice-based crypto schemes

begin to replace current public-key cryptography and their integration into practical applications needs to be explored. For example, ECC was proposed independently by Miller [19] and Koblitz [20] in 1986/1987, but it took 20 years until it appeared in actual security systems. Even with relatively little cryptanalysis and low confidence in parameters sets, the most critical issue to date with lattice-based cryptography is its practicability, and it is clear that in order for it to replace widely used number-theoretic primitives, its constructions must be shown to be similarly efficient on many of the embedded platforms existing in today's digital and pervasive environment.

The proposed presentation will evaluate lattice-based digital signature schemes (DSSs), which are an essential component of any cryptosystem.

2 Lattice-based Digital Signature Schemes

DSSs based on the hardness of lattice problems generally fall into three categories: 1) GGH/NTRUSign signatures; 2) Hash-and-sign signatures; and 3) Fiat- Shamir signatures.

2.1 GGH/NTRUSign signatures

The GGH [21] and NTRUEncrypt [22] cryptosystems were among the first shown to be based on the hardness of lattice problems, specifically based on solving the approximate closest vector problem. The difference between these schemes is that the latter can be viewed as a special instantiation of the former. The GGH cryptosystem included a DSS, in turn forming the basis of NTRUSign [23] which combined almost the entire design of GGH but uses the NTRU lattices employed in NTRUEncrypt. The predecessor to NTRUSign, NSS [24], was broken by Gentry et al. [25, 26] and incidently NTRUSign suffered the same fate with works by Nguyen and Regev [27], which shows experimental results recovering the secret-key with 400 signatures. Since Nguyen and Regev categorically show NTRUSign (without perturbation) to be absolutely insecure and further countermeasures and a version with perturbations have also been broken [28], this scheme will not be covered as implementation results currently do not have practical applications. However, recent research such as Melchor et al. [29] hold some promise for the future of this form of DSS, such that someday the security and efficiency issues of NTRUSign may be amended.

2.2 Hash-and-sign signatures

DSSs based on the hash-and-sign paradigm follow seminal work by Diffie and Hellman [30]. The concept follows the criterion that a message, μ, should be hashed before being signed. That is, to sign a message, first hash μ to some point h = $H(\mu)$, which must be in the range of the trapdoor function f, the then acclaimed RSA being such a function. Once the message has been hashed, it is signed $\sigma = f^{1}(h)$ and a verification algorithm checks that $f(\sigma) = H(\mu)$ to confirm whether (σ,μ) is a valid message/signature pair. This theory became the foundation for full-domain hash (FDH) [31], with the hash function $H(\cdot)$ being modelled on a random oracle. Where f is a trapdoor permutation, the scheme is shown to be existentially unforgeable under a chosen-message attack. The relation lattices have to hash-and-sign signatures is the intuition that a short basis for a lattice could provide such a trapdoor function. This led to the first proposal by Gentry et al. [32] (GPV), showing a DSS based on the hardness of lattice problems. Central to the scheme is the construction of trapdoor functions with the necessary property that every output value has several preimages, the Gaussian sampling algorithm and also the use of modular lattices. A more recent scheme by Micciancio and Peikert [33] also adopts hash-and-sign, introducing a more efficient trapdoor than the one used in GPV. Improvements to the key generation were also made by Alwen and Peikert [34].

2.3 Fiat-Shamir Signatures

An alternative way of constructing a DSS is to first build an identification scheme of a certain form, then converting it into a DSS by means of the Fiat-Shamir transformation [35, 36]. Lattice-based signature schemes which use the Fiat-Shamir transformation are mainly due to research by Lyubashevsky et al. [14, 37-41]. The procedures in the first publication by Lyubashevsky [37] are shown to be based on the short integer solution problem (SIS), that is, if a solution is found for the DSS then a solution is also found for SIS. The initial 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 based on the hardness of finding the approximate shortest vector in the standard model as well as the random oracle model. The identification scheme is then transformed into a DSS where optimisations are made to the tight parameter settings improving elements such as the length of the signature and

making it computationally infeasible to find collisions in the hash function family *H.* The security of the scheme is dependent on the hardness of finding collisions in certain hash function families. An adversary who is able to forge a signature can then use this to find a collision in a hash function chosen randomly from H. Therefore, forging a signature and furthermore finding a collision in a randomly chosen $h \leftarrow H$ is equivalent to finding short vectors in a lattice over R, that is, the ring-SIS problem.

The subsequent improvements made by Lyubashevsky [38] (LYU) were twofold. The most significant change is that of the hardness assumption used, adapting from ring-SIS to ring-LWE, which is shown to significantly decrease the sizes of the signature and the keys, thereby improving efficiency. The second improvement is during the signing procedure, which involves asymptotically shorter signatures. This stage requires more complicated rejection sampling, so that the signatures are independent from the secret-key, and sampling from the normal distribution, wherein highly accurate computations are needed [38]. The scheme, as in the previous scheme, is shown to be strongly unforgeable and is based on the worst-case hardness of finding short vectors in a lattice.

The current state-of-the-art in lattice-based DSSs is the proposed scheme by Ducas et al. [41] named BLISS. The main contribution of this work is the significant improvement in the rejection sampling stage. As a consequence, this scheme presents an important bridge between theoretical and practical lattice-based DSSs.

3 Evaluation of Hardware and Software Implementations of Lattice-based Digital Signature Schemes

As previously discussed, there are currently no practical instantiations of the GGH [21] signature schemes and implementations of NTRUSign such as [42] are vulnerable to cryptanalysis, so they are not considered in this evaluation. Lattice-based schemes investigated here for which implementation results are available are GPV [32, 33], LYU [38], GLP [14] and BLISS [41]. For a quick overview, all schemes considered for evaluation, their secret-key, public-key and signatures sizes as well as available software (CPU) results are summarised in Table I, however since these benchmarks are not all on the same platform they are not all directly comparable (similarly in Table II). The fastest scheme with regard to signing and also with the smallest signature (5.6 kb) is currently BLISS (implemented in C) due to the low amount of rejections, fast Gaussian sampling using a large cumulative distribution table (CDT), and small parameters for the dimension, n and the modulus, q. The structural disadvantage of GLP (more rejections, larger n and q) is almost compensated by the optimised implementation by Güneysu et al. [2013] using assembly optimisation and vectorisation (i.e. AVX extensions). As verification almost only requires polynomial multiplication, the vectorised GLP implementation is twice as fast as BLISS.

Thus in the future, it is expected that BLISS could be further improved by applying the vectorisation ideas of Güneysu et al. [43]. Moreover, for the signing procedure of BLISS, the impact of higher security levels on performance is moderate as n and q stay the same, with the significant changes being in the Gaussian sampler and number of rejections. As Gaussian sampling is not needed for verification, the runtime of verification is basically independent of the security level. The LYU implementation by Weiden et al. [44] is not competitive, mainly due to larger parameters and also because the implementation uses slow rejection sampling and relies on the NTL library for basic arithmetic. For GPV [32], initial outputs and key sizes were many megabits long and even with improvements by Bansarkhani and Buchmann [45], signature and key sizes are still large in practice, around 250 kb for security of around 100-bits. With the improvements proposed by Micciancio and Peikert [33], their scheme alleviates the sizes of the signatures and keys to roughly 100 kb, a drastic improvement over GPV; however for practical applications this is still significantly large and the implementation cannot compete with GLP or BLISS. Regarding those implementations on constrained devices or microcontrollers; Oder et al. [46] target an ARM Cortex-M4F microcontroller, which compares different samplers (Bernoulli, Knuth-Yao and Discrete Ziggurat) and running at 168 MHz; the device produces 28 signing, 167 verification and 0.46 key generation operations per second. Boorghany et al. [47] and Boorghany and Jalili [48] provide an implementation of GLP and BLISS used as an identification scheme on 8-bit architectures (Atmega and ATxmega), showing that lattice-based DSSs perform well even on very constrained devices. The Gaussian sampler is based on the CDT and the table currently fills a large part of the flash. However, the ideas of Pöppelmann et al. [15] should be directly applicable to reduce the table size with a hopefully moderate impact on runtime. As the signature schemes are implemented as identification schemes their runtimes are not discussed.

Table I: A summary of lattice-based DSSs and schemes based on classical assumptions.

Scheme	Security	Sign. Size	*sk* Size	*pk* Size	Sign./s	Ver./s
GPV	100-bits	240 kb	191 kb	300 kb	48	370
LYU	100-bits	103 kb	103 kb	65 kb	36	260
GLP-I	80-bits	9.5 kb	2 kb	12 kb	5300	75500
Bliss-I	128-bits	5.6 kb	2 kb	7 kb	8000	33000
Bliss-II	128-bits	5 kb	2 kb	7 kb	2000	33000
Bliss-III	160-bits	6 kb	3 kb	7 kb	5000	32000
Bliss-IV	192-bits	6.5 kb	3 kb	7 kb	2500	31000
RSA-2048	112-bits	2 kb	2 kb	2 kb	800	27000
RSA-4096	128-bits	4 kb	4 kb	4 kb	100	7500
ECDSA-256	128-bits	0.5 kb	0.25 kb	0.25 kb	9500	2500
ECDSA-384	192-bits	0.75 kb	0.37 kb	0.37 kb	5000	100

* Most results are benchmarked on an Intel Core i7 at 3.4 GHz, 32GB RAM with OpenSSL 1.0.1c. [41]
The GLP-I, LYU, GPV performances have been scaled to 3.4 GHz based on cycle counts.

Table II: A summary of hardware instantiations of DSSs on Virtex-5 and Spartan- 6 FPGAs

Scheme	Security	Description	Device	Resources	Ops/s
GLP-I (Sign)	80-bits	q = 8383489, n = 512	S6 LX16	7465 LUTs; 8993 FF; 28 DSP; 29.5 BRAM18	931
GLP-I (Ver)	80-bits	q = 8383489, n = 512	S6 LX16	6225 LUTs; 6663 FF; 8 DSP; 15 BRAM18	998
Bliss-I (Sign)	128-bits	CDT Sampler	S6 LX25	7491 LUTs; 7033 FF; 6 DSP; 7.5 BRAM18	7958
Bliss-I (Sign)	128-bits	Bernoulli Sampler	S6 LX25	9029 LUTs; 8562 FF; 8 DSP; 6.5 BRAM18	8081
Bliss-I (Ver)	128-bits	-	S6 LX25	5275 LUTs; 4488 FF; 3 DSP; 4.5 BRAM18	14438
RSA (Sign)	103-bits	RSA-2048; private key	V5 LX30	3237 LS; 17 DSP;	89
ECDSA (Sign)	128-bits	Full ECDSA; secp256r1	V5 LX110	32299 LUT/FF pairs	139
ECDSA (Ver)	128-bits	Full ECDSA; secp256r1	V5 LX110	32299 LUT/FF pairs	100

For reconfigurable hardware, results are available for GLP and BLISS and are summarised in Table II. While the speed of the GLP implementation, with roughly 1000 signing and verification operations per second, is good in comparison with classical schemes, the implementation in [14] and particularly the usage of schoolbook multiplication is suboptimal given works on fast multiplication such as [13]. The BLISS implementation by Pöppelmann et al. [15] uses the Number Theoretic Transform (NTT) multiplier proposed by Pöppelmann and Güneysu [49] and achieves high throughput for signing and verification. The resource consumption is also reasonable and the design fits on low-cost Spartan-6 devices. Usage of the improved NTT multiplier design by Roy et al. [13] might give a further reduction of the resource consumption. For BLISS, two variants are given; one implementing the improved CDT approach and another one using the Bernoulli techniques of Ducas et al. [41].

4 Conclusion and Future Work

Due to the favourable results shown by Fiat-Shamir signatures and in particular the recent instantiations of BLISS on FPGAs by Pöppelmann et al. [15] (≈ 8000 signatures per second) and on microcontrollers by Oder et al. [46] (28 signatures per second), in both instances outperforming RSA and ECC for comparable security levels, lattice-based digital signature schemes are now at a stage where they can be feasibly considered for real-world applications. One of the main areas of future research in lattice-based DSSs is further optimisation and implementation of schemes based on the Fiat-Shamir model. In particular, BLISS, which shows very good performance, is a candidate for integration into other constrained systems and devices like smart cards and microcontrollers. Integrating the scheme with respect to highly-optimised software is also a possible area for future work. Additionally, further research is needed into the parameters (and security analyses) of these schemes. This would build upon research such as [50], which would mean parameter selection becoming much more explicit in lattice-based cryptography.

One of the most time consuming components for hardware implementations of lattice-based cryptography is currently polynomial multiplication. Making this stage efficient has been well studied. However, optimising such a stage is arguably the most critical in hardware due to the computationally intensive operations; as such, this is still an important focus for research for implementations on both large and lightweight devices. Another module pertaining to one of the more computationally expensive in hardware is the Gaussian sampling stage. Dwarakanath and Galbraith [51] and Roy et al. [52] look into different approaches to efficiently compute such a stage for constrained devices. As shown by [15] and [46] the CDT approach is best suited for larger devices with the Bernoulli approach showing efficiencies on smaller devices. Due to its computational importance, further research into making this stage more efficient could result in significant improvements overall. As lattice-based DSSs become more practical and publicly available, further attack vectors like side-channel analysis (SCA) [53] have to be considered. Timing and fault injection attacks, power, electro-magnetic analysis and advanced machine learning-based attacks are serious threats to many real-world implementations. Recent work has shown that SCA attacks are applicable in real-world situations [54]. There has been very little research conducted on the vulnerabilities of lattice-based cryptographic implementations to physical attacks. It is anticipated that there may be a particular vulnerability with respect to algorithmic parts with variable runtime, for instance Gaussian and rejection sampling, which are major components of many lattice-based algorithms.

An interesting area of theoretical research looks into the security of DSSs in the quantum world, specifically relating to the DSSs that use random oracle constructions and whether they are still secure to a quantum adversary. Although making the DSSs less efficient, schemes by Gentry et al. [32] and Lyubashevsky [38] are respectively shown by Boneh and Zhandry [55] and Dagdelen et al. [56] to be secure to such an adversary, creating the quantum random oracle model. This could also motivate an important area for future research, such as proving security for more DSSs to a quantum adversary or possibly creating a generic technique, which could turn a DSS secure in the random oracle model to that in the quantum random oracle model.

References

1. P.W.Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26, 5 (Oct. 1997), 1484–1509.
2. M. Ajtai, R. Kumar, D. Sivakumar. 2001. A Sieve Algorithm for the Shortest Lattice Vector Problem. In STOC. 601–610.
3. I. Dinur, G. Kindler, R. Raz, S. Safra. 2003. Approximating CVP to Within Almost-Polynomial Factors is NP-Hard. Combinatorica 23, 2 (April 2003), 205–243
4. D. Boneh, A. Sahai, B. Waters. 2011. Functional Encryption: Definitions and Challenges. In TCC. Vol. 6597.
5. S. Agrawal, D. Boneh, X. Boyen. 2010. Efficient Lattice (H)IBE in the Standard Model. In EUROCRYPT. 553–572.
6. L. Ducas, V. Lyubashevsky, T. Prest. 2014. Efficient Identity-Based Encryption over NTRU Lattices. IACR Cryptology ePrint Archive 2014 (2014), 794
7. X. Boyen. 2013. Attribute-Based Functional Encryption on Lattices. In TCC. 122–142.
8. S. D.Gordon, J. Katz, V. Vaikuntanathan. 2010. A Group Signature Scheme from Lattice Assumptions. In ASIACRYPT. 395–412
9. J.Camenisch, G. Neven, M. Ruckert. 2012. Fully Anonymous Attribute Tokens from Lattices. In SCN. 57–75.
10. F. Laguillaumie, A. Langlois, B. Libert, D. Stehlé. 2013. Lattice-Based Group Signatures with Logarithmic Signature Size. In ASIACRYPT (2). 41–61.
11. C. Gentry. 2009a. A Fully Homomorphic Encryption Scheme. Ph.D. Dissertation. Stanford University.
12. C. Gentry. 2009b. Fully homomorphic encryption using ideal lattices. In STOC. 169–178.
13. S. S. Roy, F. Vercauteren, N. Mentens, D. D.Chen, I. Verbauwhede. 2014. Compact Hardware Implementation of Ring-LWE Cryptosystems. In CHES. 371–391.
14. T. Güneysu, V. Lyubashevsky, T. Pöppelmann. 2012. Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems. In CHES. 530–547
15. T. Pöppelmann, T. Güneysu. 2014. Area Optimization of Lightweight Lattice-Based Encryption on Reconfigurable Hardware. In ISCAS. 2796–2799
16. M. Ajtai. 1996. Generating Hard Instances of Lattice Problems (Extended Abstract). In STOC. 99–108.
17. A. Langlois D. Stehlé. 2014. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography (2014).
18. V.Lyubashevsky, C. Peikert, O. Regev. 2010. On Ideal Lattices and Learning with Errors over Rings. In EUROCRYPT. 1–23.
19. V. S. Miller. 1986. Use of Elliptic Curves in Cryptography. In CRYPTO. 417–426.
20. N. Koblitz. 1987. Elliptic Curve Cryptosystems. Math. Comp. (1987).
21. O. Goldreich, S. Goldwasser, S. Halevi. 1996. Public-Key Cryptosystems from Lattice Reduction Problems. Electronic Colloquium on Computational Complexity (ECCC) 3, 56 (1996).
22. J. Hoffstein, J. Pipher, J.H. Silverman. 1998. NTRU: A Ring-Based Public Key Cryptosystem. In ANTS. 267–288
23. J. Hoffstein, N.Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte. 2003. NTRUSign: Digital Signatures Using the NTRU Lattice. In CT-RSA. 122–140.
24. J. Hoffstein, J.Pipher, J.H. Silverman. 2001. NSS: An NTRU Lattice-Based Signature Scheme. In EUROCRYPT. 211–228.
25. C.Gentry, J. Jonsson, J. Stern, M. Szydlo. 2001. Cryptanalysis of the NTRU Signature Scheme (NSS). In ASIACRYPT. 1–20.

26. C. Gentry, M. Szydlo. 2002. Cryptanalysis of the Revised NTRU Signature Scheme. In EUROCRYPT. 299–320.
27. P. Q. Nguyen, O.Regev. 2009. Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures. J. Cryptology 22, 2 (2009), 139–160.
28. L. Ducas, P. Q. Nguyen. 2012b. Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures. In ASIACRYPT. 433–450
29. C. A. Melchor, X. Boyen, J-C. Deneuville, P. Gaborit. 2014. Sealing the Leak on Classical NTRU Signatures. In PQCrypto 2014. 1–21.
30. W. Diffie, and M.E. Hellman. 1976. New directions in cryptography. IEEE Transactions on Information Theory 22, 6 (1976), 644–654
31. M.Bellare, P. Rogaway. 1993. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In ACM CCS. 62–73.
32. C. Gentry, C. Peikert, V.Vaikuntanathan. 2008. Trapdoors For Hard Lattices And New Cryptographic Constructions. In STOC. 197–206
33. D. Micciancio, C. Peikert. 2012. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In EUROCRYPT. 700–718
34. J. Alwen, C. Peikert. 2011. Generating Shorter Bases for Hard Random Lattices. Theory Comput. Syst. 48, 3 (2011), 535–553
35. A.Fiat, A. Shamir. 1986. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In CRYPTO. 186–194
36. M. Abdalla, J. Hea 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
37. V. Lyubashevsky. 2009. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. In ASIACRYPT. 598–616.
38. V. Lyubashevsky. 2012. Lattice Signatures without Trapdoors. In EUROCRYPT. 738–755.
39. M. Abdalla, P-A Fouque, V. Lyubashevsky, M. Tibouchi. 2012. Tightly-Secure Signatures from Lossy Identification Schemes. In EUROCRYPT. 572–590
40. S. Bai and S. D. Galbraith. 2014. An Improved Compression Technique for Signatures Based on Learning with Errors. In CT-RSA. 28–47
41. 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.
42. B. Driessen, A. Poschmann,C. Paar. 2008. Comparison of innovative signature algorithms for WSNs. In WISEC. 30–35.
43. T. Guneysu, T. Oder, T. Poppelmann, P. Schwabe. 2013. Software Speed Records for Lattice-Based Signatures. In PQCrypto. 67–82
44. P. Weiden, A. Hulsing, D. Cabarcas, J. Buchmann. 2013. Instantiating Treeless Signature Schemes. IACR Cryptology ePrint Archive 2013.
45. R. El Bansarkhani, J. Buchmann. 2013. Improvement and Efficient Implementation of a Lattice-Based Signature Scheme. In Selected Areas in Cryptography. 48–67.
46. T. Oder, T. Poppelmann, T. Guneysu. 2014. Beyond ECDSA and RSA: Lattice-based Digital Signatures on Constrained Devices. In DAC. 1–6.
47. A. Boorghany, S. Bayat Sarmadi, R. Jalili. 2014. On Constrained Implementation of Lattice-based Cryptographic Primitives and Schemes on Smart Cards. IACR Cryptology ePrint Archive 2014 (2014), 514.
48. A. Boorghany, R. Jalili. 2014. Implementation and Comparison of Lattice-based Identification Protocols on Smart Cards and Microcontrollers. IACR Cryptology ePrint Archive 2014 (2014), 78.
49. T. Poppelmann, T. Guneysu. 2012. Towards Efficient Arithmetic for Lattice-Based Cryptography on Reconfigurable Hardware. In LATINCRYPT. 139–158
50. M. Ruckert, M. Schneider. 2010. Estimating the Security of Lattice-based Cryptosystems. IACR Cryptology ePrint Archive 2010 (2010), 137.
51. N. Dwarakanath. S. D. Galbraith. 2014. Sampling from discrete Gaussians for lattice-based cryptography on a constrained device. 159–180.
52. S. S. Roy, F. Vercauteren, I. Verbauwhede. 2013. High Precision Discrete Gaussian Sampling on FPGAs. Selected Areas in Crypto. 1–39.
53. P.C. Kocher, J. Jaffe, and B. Jun. 1999. Differential Power Analysis. In CRYPTO. 388–397.
54. T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, M. T. Manzuri Shalmani. 2008. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoqCode Hopping Scheme. In CRYPTO. 203–220
55. D. Boneh , M. Zhandry. 2013. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World. In CRYPTO (2). 361–379
56. O. Dagdelen, M.Fischlin, T. Gagliardoni. 2013. The Fiat-Shamir Transformation in a Quantum World. In ASIACRYPT (2). 62–81.