Lattice-Based Simulatable VRFs: Challenges and Future Directions

Carlo Brunetta, Bei Liang, and Aikaterini Mitrokotsa

Chalmers University of Technology, Gothenburg, Sweden
{brunetta,lbei,aikmitr}@chalmers.se

Abstract Lattice-based cryptography is evolving rapidly and is often employed to design cryptographic primitives that hold a great promise for being post-quantum resistant and can be employed in multiple applications such as: e-cash, unique digital signatures, non-interactive lottery and others. In such application scenarios, a user is often required to prove non-interactively the correct computation of a pseudo-random function $F_k(x)$ without revealing the secret key k used. Commitment schemes are also useful in such application settings to commit to a chosen value, while keeping it hidden to others but being able to reveal the committed value later. In this short paper, we provide our insights on constructing a *lattice-based simulatable verifiable random function (sVRF)* and point out the main challenges that need to be addressed in order to achieve it.

Keywords: Dual-Mode Commitment Scheme, Lattice-based Cryptography, Non Interactive Zero Knowledge Arguments, Pseudo Random Functions, Verifiable Random Functions

1 Introduction

Zero-knowledge (ZK) proofs [14] are employed to prove the knowledge of secret information while preserving provers privacy with respect to a NP language. Depending on whether the zero-knowledge proof is performed interactively or not, we may have *interactive* or *non-interactive* protocols; while the latter are more efficient regarding communication costs.

Pseudo-random functions (PRFs) [10] are a very useful cryptographic primitive that is often employed in combination with *zero-knowledge* proofs in multiple application scenarios. Let us consider a general scenario: a prover $\mathcal{P}$ wants to prove to a verifier $\mathcal{V}$ the knowledge of a secret $\boldsymbol{w}$ and the correct computation of a PRF $F_{\boldsymbol{w}}$ on the input x, *i.e.,* $F_{\boldsymbol{w}}(x)$. A rather important question is:

How may $\mathcal{P}$ prove to $\mathcal{V}$ the correct evaluation of the PRF $F_{\boldsymbol{w}}(x)$ without leaking any information about $\mathbf{w}$, just by providing a proof π?

We consider the case where the communication between $\mathcal{P}$ and $\mathcal{V}$ should be **non**-interactive, *i.e.,* $\mathcal{P}$ needs to provide $\mathcal{V}$ all the necessary information to verify the correct computations in a single step.

The above stated question can be solved by employing a *verifiable random function* (VRF) [16]. A VRF is a PRF with two additional algorithms; one algorithm that is able to generate a proof π of the correct computation of the PRF $F_{\boldsymbol{w}}(x)$ as well as a *verification* algorithm.

Recent papers [11,8] use the VRF into a *blockchain* context in order to either define a *fair and verifiable lottery* in which the winner will publish the next block, or as a way to generate a *"common and shared random string"* which can be seen as an equivalent of the CRS model.

Finding these study cases is extremely important to motivate the community to research and further develop primitives that allows scenarios where *verification* or *providing a proof* is a mandatory step.

Although algebraic pseudo-random functions and ZK proofs are well studied primitives, they have received limited attention in lattice settings; furthermore, to the best of our knowledge, *building lattice-based VRFs is an open problem.*

Lattice-based cryptographic primitives [1,18], mainly rely on the *learning with errors* (LWE) and the *short integer solution* (SIS) problems; they are quite promising for providing post-quantum resistance guarantees, while also offering simpler arithmetic operations and thus, important efficiency guarantees.

Designing a lattice-based VRF is a challenging and currently open problem since it requires a non-interactive proof in the standard model. As a step towards this direction, in this short paper, we provide our insights on designing a lattice-based *simulatable VRF* (sVRF), originally introduced by Chase and Lysyanskaya [6]. Informally, an sVRF is a VRF defined in a public parameter model, such as the *common random string* (CRS) model, which implies the existence of honest common parameters on the top of the standard VRF system. More precisely, besides the usual algorithms in a VRF there is an additional parameter generation algorithm which takes as input the security parameters and output the public parametrs pp. Both the input domain and output range of the sVRF depend on pp. Meanwhile, pp is included in the inputs for all the algorithms KeyGen, Eval, Prove and Verify. Moreover, except of the uniqueness and pseudorandomness properties, sVRFs should also satisfy *simulatability* which is a novel property making them different from VRFs. Simulatability states that there exists a simulator that is able to simulate the common parameters such that, corresponding to a verification key, for any x, y, it is possible to produce a proof π that $F(sk, x) = y$. The simulated transcription is required to be indistinguishable from the values computed from the parameters that are generated honestly. In this paper, we describe our insights on constructing an sVRF when relying on Libert *et al.*'s [14] method to prove zero-knowledge arguments for lattice-based PRFs. Furthermore, we describe the main challenges that need to be addressed in order to construct a lattice-based sVRF using this method.

1.1 A Roadmap to Lattice-based sVRFs

Chase and Lysyanskaya's [6] provided a general construction of sVRFs from a perfectly binding computational hiding non-interactive commitment scheme and an unconditionally-sound multi-theorem NIZK for NP. Their main idea is to use a multi-theorem NIZK to generate the proof for a statement that the public verification key is a commitment of the secret key and the function value is the correct result on the input applied to the secret-keyed PRF, *i.e.*, $\mathsf{pk} = \mathsf{Com}(\mathsf{sk}; r) \wedge y = F(\mathsf{sk}, x)$. However, such solution is based on a general assumption, in order to come up with a lattice-based sVRF, we should specify a lattice-based PRF scheme.

Fortunately, thanks to the very recent significant results of Boneh *et al.* [4] who proposed a LWE-based key homomorphic PRFs as well as Libert *et al.*'s [14] three round zero-knowledge arguments of correct evaluation for the LWE-based PRF Boneh *et al.* [4] w.r.t committed keys and inputs, it is possible to obtain a non-interactive solution of $y = F(\mathsf{sk}, x)$ as the correct evaluation of a PRF for a secret input x and a committed key sk, and yielding a sVRF furthermore.

Libert *et al.* have significant contributions [14,12,13] in the area of designing efficient zero-knowledge proofs for lattice-related language. For instance, Libert *et al.* [12] considered how to construct zero-knowledge arguments of knowledge of a secret matrix X and vectors $\boldsymbol{s}, \boldsymbol{e}$ such that for a public vector $\boldsymbol{b}$ it holds $\boldsymbol{b} = \boldsymbol{X} \cdot \boldsymbol{s} + \boldsymbol{e} \bmod q$. Libert *et al.* [13] also investigated in the lattice setting how to design zero-knowledge arguments for the statement that c_x, c_y and c_z are the commitments to the polynomial-size bit-strings x, y and z which are the binary representations of large integers X, Y, Z satisfying certain algebraic relations such as $Z = X + Y$ and $Z = X \cdot Y$.

In order to obtain zero-knowledge arguments for the correct evaluation of key-homomorphic PRF [1] of Boneh *et al.* [4] , Libert *et al.* [14] presented an useful abstraction of Stern's protocol [19] and they modified the Boneh *et al.*'s lattice PRF [4] in order to efficiently prove the correct computation of the PRF interactively, while providing zero-knowledge guarantees.

As stated in their paper, it is possible to obtain the first non-interactive lattice-based zero-knowledge protocol by directly applying the Fiat-Shamir transformation [9]. The main issue with this choice is that the Fiat-Shamir transformation is secure in the *Random Oracle Model* (ROM) which is against the original sVRF definition [6].

Thus, our main research objective is to find an appropriate transformation from ZK to NIZK, defined over lattices, not relying on the ROM. In Figure 1, we depict two different strategies in order to obtain a lattice-based sVRF: either by directly transforming Libert *et al.*'s ZK argument or by providing a different lattice-based ZK PRF proof system and applying a ZK to NIZK transformation and then the Chase-Lysyanskaya's transformation from NIZK to sVRF.

$$\begin{tikzcd}
\text{Libert's ZK} \arrow[rrd, bend left, "\textbf{Transf.}"] & & \\
\text{Lattice ZK} \arrow[r, "\textbf{Transf.}"] & \text{Lattice NIZK} \arrow[r, "\text{Chase \textit{et. al} [6]}"] & \text{Lattice sVRF}
\end{tikzcd}$$

Figure 1. Roadmap to lattice-based sVRF. In **bold**, this paper's main research focus.

[1] Namely demonstrating knowledge of a committed secret key $\boldsymbol{k}$, a secret input $\boldsymbol{J}$ and an output $\boldsymbol{y}$ satisfying $\boldsymbol{y} = F_{\boldsymbol{k}}(\boldsymbol{J})$

2 Applying Lindell's Tranformation

In this section we provide our finding when defining a sVRF based on Libert's ZK argument and the Lindell's transformation [15]. We explain our discoveries and challenges.

We considered Lindell's transformation [15] from any sigma-protocol into a corresponding NIZK protocol. In contrast to Fiat-Shamir's transformation [9], Lindell's transformation does not require the random oracle model; more precisely, in Lindell's transformation the *zero-knowledge* property holds in the *common reference string* (CRS) model, while in order to achieve *soundness*, the used hash function is modeled as a *non-programmable* random oracle [17].

In order to adopt Lindell's transformation an important requirement is that of a *dual-mode* commitment scheme.

The main concept of a commitment scheme is that it is possible to secretly fix some message m that it is used in a protocol and in a second phase, open the commitment and therefore prove the correct knowledge or possession of the specific message m. Designing lattice-based commitment schemes has already received some attention in the literature [3,2].

The *dual-mode* represents the possibility to sample a statement in a language L via a bit b and use the commitment scheme in a *binding* way, *i.e.*, a commitment c can be decommitted in a *unique* message m, or in a *"trapdoor"* way, *i.e.,* that with some secret witness $\boldsymbol{w}$, it is possible to decommit c to any message m'.

Therefore, the main property required for a dual-mode commitment scheme is that it is impossible to distinguish how the bit b is selected and therefore impossible to know if we are decommitting to the original message or we are using the trapdoor to decommit to an arbitrary message.

A *dual-mode commitment scheme* represents a specific type of commitment schemes that are equivalently defined by Catalano and Visconti as *hybrid commitment schemes* [5].

As described in [15], in order to define a dual-mode commitment scheme, Lindell requires a *membership-hard efficient-sampling language* defined as:

Definition 1 (Membership-hard with Efficient Sampling [15]). *Let L be a language. L is* membership-hard with efficient sampling *(MHES) if there exists a probabilistic polynomial-time sampler S_L such that for every probabilistic polynomial-time distinguisher D there exists a negligible function $\mu(\cdot)$ such that:*

$$|\mathsf{Pr}(D(S_L^x(0,1^n),1^n)=1)-\mathsf{Pr}(D(S_L(1,1^n),1^n)=1)|\leq\mu(n)$$

where $S_L(b,\cdot)$ is a sampler that returns an instance in the language L if $b=0$ and an instance not in the language L if $b=1$. S_L^x denotes only the instance without the witness.

In a nutshell, the MHES language L is a language in which it is hard to distinguish if an efficient sampling algorithm S_L sampled the statement x in the language L or not: it is hard to decide the membership of $x \in L$ but it is easy to sample x in the language (or not).

In summary, in order to build an sVRF while employing the Lindell's transformation, the main building blocks required are depicted in Figure 2.

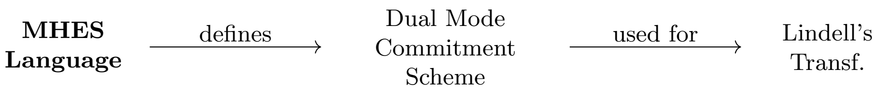

Figure 2. Roadmap to Lindell's transformation.

By assuming the hardness of the *inhomogeneous short integer solution* (ISIS) problem, if we follow the idea and structure of the DDH language construction proposed by Lindell [15] in order to define the language L_{IS} of Eq. (1), the result is unfortunately not MHES for common lattice security parameters.

$$L_{\mathsf{IS}} \coloneqq \{(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{u}, \boldsymbol{v}) \mid \boldsymbol{A}, \boldsymbol{B} \in {\mathbb{Z}_p}^{n\times m}, \tilde{\boldsymbol{w}} \in \{0,1\}^m, \boldsymbol{u} = \boldsymbol{A}\tilde{\boldsymbol{w}}, \boldsymbol{v} = \boldsymbol{B}\tilde{\boldsymbol{w}}\}. \qquad (1)$$

This is the case since whenever we provide a statement not in the language $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{u}, \boldsymbol{v}) \notin L_{\mathsf{IS}}$, it exists in fact a statement $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{A}\tilde{\boldsymbol{w}}', \boldsymbol{A}\tilde{\boldsymbol{w}}') \in L_{\mathsf{IS}}$ in the language for some $\tilde{\boldsymbol{w}}'$. Therefore it cannot be used to define a dual-mode commitment scheme mainly because the commitment scheme will not be perfectly binding, which is a necessary condition in order to use Lindell's transformation.

3 Challenges and Future Directions

In this section we will briefly discuss and collect our conjectures and/or our future research directions by dividing them into into two major classes: a first class of questions related to *transformations* from ZK to NIZK and a second class of challenges regarding *lattice languages*.

3.1 ZK Transformations

Choosing Lindell's transformation is not optimal for the final goal of constructing an sVRF since the transformation is defined in the non-programmable ROM.

Ciampi *et al.* [7] modified and improved Lindell's transformation: the transformation does not require the non-programmable random oracle *nor* a perfectly binding commitment scheme at the cost of a more specific language. By using Ciampi *et al.*'s transformation, it might be possible to obtain a ZK to NIZK transformation not based on the ROM.

Challenge 1 *Is it possible to use Ciampi* et al. *transformation in our sVRF construction-idea? The main challenge of this approach is to check if any lattice-based language can be defined in order to fulfil the transformation hypothesis and requirement.*

With the same spirit, we find an additional challenge of more general interest: a ZK to NIZK transformation that is not defined in the random oracle model (or any similar ones). Therefore, we state as a general challenge for future investigation:

Challenge 2 *Are there any other transformations in the literature that can be used for our construction-idea? Are they efficient? How do they compare among themselves or with respect to the Fiat-Shamir's transformation?*

3.2 Lattice Languages

When considering the Lindell's transformation, the language L_{IS} is ill-defined and therefore cannot be used in order to build a dual-mode commitment scheme. Furthermore, the language challenge of defining a membership-hard language can be seen as of perpendicular interest.

Challenge 3 *Is there a way to define a lattice-based membership-hard efficient sampling language L that can be used to define a dual-mode commitment scheme?*

Generally speaking and quite informally, the main obstacle is finding *"good"*-languages that have a *"unique-witness"*. This means that it would be incredibly useful to find a lattice-language L in which the witness of a statement $x \in L$ is unique. Solving this problem will open new direction in lattice based cryptography.

Challenge 4 *Find a lattice-based language L in which every statement $x \in L$ has a unique witness w.*

As a different but related problem, if we consider a different ZK PRF proof system, the ZK language used for our construction-idea requires an additional property in order to be used by the Chase-Lysyanskaya's transformation. The ZK system has to be able to prove the correct computation of the PRF **and** the correctness of an additional commitment. It has to be defined over lattices **and**, after transforming it with the best ZK to NIZK transformation possible, the obtained NIZK has to be multi-theorem.

Challenge 5 *Given the best ZK transformation, find a ZK PRF argument/proof system that can be used for the Chase-Lysyanskaya's transformation.*

Acknowledgement. We really thank the anonymous reviewers for their insightful comments, suggestions, discussions and the new literature-direction that we can now explore. This work was supported by the the Swedish Research Council (Vetenskapsrådet) through the grant PRECIS (621-2014-4845).

References

1. Ajtai, M.: Generating Hard Instances of Lattice Problems (Extended Abstract). In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. pp. 99–108. STOC '96, ACM, New York, NY, USA (1996), http://doi.acm.org/10.1145/237814.237838
2. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More Efficient Commitments from Structured Lattice Assumptions. Tech. Rep. 997 (2016), https://eprint.iacr.org/2016/997
3. Benhamouda, F., Krenn, S., Lyubashevsky, V., Pietrzak, K.: Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings. In: Proceedings, Part I, of the 20th European Symposium on Computer Security – ESORICS 2015 - Volume 9326. pp. 305–325. Springer-Verlag New York, Inc., New York, NY, USA (2015), http://dx.doi.org/10.1007/978-3-319-24174-6_16
4. Boneh, D., Lewi, K., Montgomery, H., Raghunathan, A.: Key Homomorphic PRFs and Their Applications. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013. pp. 410–428. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
5. Catalano, D., Visconti, I.: Hybrid Commitments and Their Applications to Zero-knowledge Proof Systems. Theor. Comput. Sci. 374(1-3), 229–260 (Apr 2007), http://dx.doi.org/10.1016/j.tcs.2007.01.007
6. Chase, M., Lysyanskaya, A.: Simulatable VRFs with Applications to Multi-theorem NIZK. In: Advances in Cryptology - CRYPTO 2007. pp. 303–322. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg (Aug 2007), https://link.springer.com/chapter/10.1007/978-3-540-74143-5_17
7. Ciampi, M., Persiano, G., Siniscalchi, L., Visconti, I.: A Transform for NIZK Almost as Efficient and General as the Fiat-Shamir Transform Without Programmable Random Oracles. In: Kushilevitz, E., Malkin, T. (eds.) Theory of Cryptography. pp. 83–111. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
8. David, B., Gaži, P., Kiayias, A., Russell, A.: Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018. pp. 66–98. Lecture Notes in Computer Science, Springer International Publishing (2018)
9. Fiat, A., Shamir, A.: How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology — CRYPTO' 86, vol. 263, pp. 186–194. Springer Berlin Heidelberg, Berlin, Heidelberg (2006), http://link.springer.com/10.1007/3-540-47721-7_12
10. Goldreich, O., Goldwasser, S., Micali, S.: How to Construct Random Functions. J. ACM 33(4), 792–807 (Aug 1986), http://doi.acm.org/10.1145/6490.6503
11. Li, W., Andreina, S., Bohli, J.M., Karame, G.: Securing Proof-of-Stake Blockchain Protocols. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology, vol. 10436, pp. 297–315. Springer International Publishing, Cham (2017), http://link.springer.com/10.1007/978-3-319-67816-0_17
12. Libert, B., Ling, S., Mouhartem, F., Nguyen, K., Wang, H.: Zero-knowledge arguments for matrix-vector relations and lattice-based group encryption. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 101–131. Springer (2016)
13. Libert, B., Ling, S., Nguyen, K., Wang, H.: Lattice-based zero-knowledge arguments for integer relations. In: Annual International Cryptology Conference. pp. 700–732. Springer (2018)

14. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash. In: Asiacrypt 2017. LNCS, Springer, Hong Kong, China (Dec 2017), https://hal.inria.fr/hal-01621027
15. Lindell, Y.: An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-programmable Random Oracle. In: Dodis, Y., Nielsen, J.B. (eds.) Theory of Cryptography, vol. 9014, pp. 93–109. Springer Berlin Heidelberg, Berlin, Heidelberg (2015), http://link.springer.com/10.1007/978-3-662-46494-6_5
16. Micali, S., Rabin, M., Vadhan, S.: Verifiable random functions. In: 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039). pp. 120–130 (1999)
17. Nielsen, J.B.: Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case. In: Goos, G., Hartmanis, J., van Leeuwen, J., Yung, M. (eds.) Advances in Cryptology — CRYPTO 2002, vol. 2442, pp. 111–126. Springer Berlin Heidelberg, Berlin, Heidelberg (2002), http://link.springer.com/10.1007/3-540-45708-9_8
18. Peikert, C.: A Decade of Lattice Cryptography. Foundations and Trends® in Theoretical Computer Science 10(4), 283–424 (2016), http://www.nowpublishers.com/article/Details/TCS-074
19. Stern, J.: A new paradigm for public key identification. IEEE Transactions on Information Theory 42(6), 1757–1768 (Nov 1996)