Zero Knowledge Compilers

John T. McCall
Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA 56267
mcca0798@morris.umn.edu

ABSTRACT

<Insert Abstract Here>

General Terms

Need to figure this out yet

Keywords

Zero Knowledge Protocols, Compilers

1. INTRODUCTION

I will focus on Zero-Knowledge Compilers which are compilers that automatically generate Zero-Knowledge proofs. This is how I plan to use the following sources:

- I expect [1, 2, 4] to be my core sources, depending on how relevent [4] turns out to be I'll replace it with a better source.
- I will use [3, 5, 6] for background information and examples of Zero-Knowledge Protocols.
- I will need to find some papers for background information on compilers.

As stated above I need to find some sources about compilers. I probably will need to find more papers dealing with ZK-Compilers as well.

1.1 Key Points

2. ZERO KNOWLEDGE PROTOCOLS

2.1 Background

2.2 Examples

3. COMPILERS

3.1 Background

4. ZERO KNOWLEDGE COMPILERS

4.1 Sigma-Protocols

Here I'll talk about Sigma-protocols and
Note to myself: Look into the Fiat-Shamir heuristic

4.2 ZKCrypt

Here I'll talk about

4.3 ZKPDL

5. APPLICATIONS

5.1 Electronic Cash

5.2 Another Application

6. CONCLUSION

7. REFERENCES

[1] J. B. Almeida, M. Barbosa, E. Bangerter, G. Barthe, S. Krenn, and S. Z. Beguelin. Full proof cryptography: verifiable compilation of efficient zero-knowledge protocols. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 488–500, New York, NY, USA, 2012. ACM. *This paper is one of the Core papers. It deals heavily with ZK-Protocols and on ZK-Compilers.*

[2] E. Bangerter, T. Briner, W. Hencecka, S. Krenn, S. Ahmad-Reza, and T. Schneider. Automatic generation of sigma-protocols. In *Proceedings of the 6th European conference on Public key infrastructures, services and applications*, EuroPKI'09, pages 67–82, Berlin, Germany, 2009. Springer-Verlag. *This paper is a core paper and focues on compilers that automatically generate sound and efficient Zero knowledge proofs of knowledge based on sigma-protocols.*

[3] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Advances in Cryptology Proceedings*, CRYPTO' 89, pages 218–229, New York, NY, USA, 1987. ACM. *This paper is referenced by most papers that deal with zero knowledge protocols, but it's old. As such it will be used for backround information and maybe an example.*

UMM CSci Senior Seminar Conference, December 2013 Morris, MN.

[4] S. Meiklejohn, C. C. Erway, A. Kupcu, T. Hinkle, and A. Lysyanskaya. Zkpdl: a language-based system for efficient zero-knowledge proofs and electronic cash. In *USENIX Security'10 Proceedings of the 19th USENIX conference on Security*, Security '10, Berkeley, CA, USA, 2010. USENIX Association. *This is a core paper, it delves into efficient ZK-Proofs and an application dealing with electronic cash.*

[5] A. Mohr. A survey of zero-knowledge proofs with applications to cryptography. *This article is great backround information and has several great examples I can use.*

[6] J.-J. Quisquater, M. Quisquater, M. Quisquater, M. Quisquater, L. C. Guillou, M. A. Guillou, G. Guillou, A. Guillou, G. Guillou, S. Guillou, and T. A. Berson. How to explain zero-knowledge protocols to your children. In *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 628–631. Springer, 1989. *If I use this paper it will primarily be for backround information and and example.*