A Computationally Sound, Symbolic Abstraction for Malleable Zero-knowledge Proofs

Michael Backes
Saarland University
and MPI-SWS
Saarbrücken, Germany
backes@cs.uni-saarland.de

Fabian Bendun
Saarland University
Saarbrücken, Germany
bendun@cs.uni-saarland.de

Matteo Maffei
Saarland University
Saarbrücken, Germany
maffei@cs.uni-saarland.de

Esfandiar Mohammadi
Saarland University
Saarbrücken, Germany
mohammadi@cs.uni-saarland.de

Proofs of security protocols are known to be error-prone and, owing to the distributed-system aspects of multiple interleaved protocol runs, awkward for humans to construct. Hence work towards the automation of such proofs started soon after the first protocols were developed, resulting in so-called symbolic models, following [7], [8], [10]. These models simplify proof construction by freeing proofs from cryptographic details such as computational restrictions, probabilistic behavior, and error probabilities.

While symbolic models traditionally comprised only basic cryptographic operations such as encryption and digital signatures, recent work has started to extend them to more sophisticated primitives with unique security features. These features go far beyond the traditional goal of cryptography to solely offer secrecy and authenticity of communication. Zero-knowledge (ZK) proofs [9] arguably constitute the most prominent such primitive (though not the only one) and have become a central building block for a variety of modern security protocols. A zero-knowledge proof consists of a message or a sequence of messages that combines two seemingly contradictory properties: First, it constitutes a proof of a statement x (e.g, $x =$ "the message within this ciphertext begins with 0") that cannot be forged, i.e., it is impossible, or at least computationally infeasible, to produce a zero-knowledge proof of a wrong statement. Second, a zero-knowledge proof does not reveal any information other than the sole fact that x constitutes a valid statement.

In addition to these core properties, commonly used ZK constructions, such as the Groth-Sahai proof system, offer a novel type of cryptographic flexibility. First, re-randomizing existing ZK proofs, which is a core technique for achieving unlinkability in anonymity protocols. Second, hiding public parts of a ZK proof statement, which is essential for selectively disclosing information of third-party proofs, thereby adhering to individual privacy requirements. Third, logically composing ZK proofs to construct more sophisticated statements, which constitutes a central building block for anonymous credential-based systems. ZK proof systems that permit these transformations are called *malleable*. In addition to offering this functionality, malleable ZK constructions are typically vastly more efficient than their non-malleable counterparts.

Currently existing symbolic abstractions are restricted to non-malleable ZK proofs: they model ZK proofs as monolithic building blocks that cannot be further transformed, i.e., these proofs can only be checked for validity or placed into larger contexts [4]. For such monolithic abstractions computational soundness results have already been established, i.e., it has been shown that a successful symbolic analysis carries over to the corresponding cryptographic ZK realizations [5], [1].

In contrast, for malleable ZK proofs no symbolic abstraction is currently known. Such an abstraction is intrinsically more difficult to handle because the aforelisted transformations are accessible to the adversary as well, which results in a significantly more involved analysis due to a much more comprehensive adversary model. Given the absence of any such abstraction, no computational soundness result for malleable ZK proofs is known either.

A. *Our Contribution*

In this paper, we make the following five contributions to this problem space:[1]

- First, we provide a symbolic abstraction of malleable ZK proofs that is accessible to existing tools for automated verification of security protocols. More precisely, we develop an equational theory that captures the semantics of malleable ZK (MZK) proofs. The main conceptual challenge we faced when devising this abstraction was to identify a finite representation of all possible transformations that an adversary can validly perform to an MZK proof. Roughly, we categorize transformations as *re-randomizing*, as *statement-based* (logically composing and decomposing ZK proofs), and as *modifying the witness* of a proof. We present two variants of our abstraction that only differ in the last category of transformations: the fully MZK (FMZK) abstraction,

[1] Details can be found at: http://www.infsec.cs.uni-saarland.de/~bendun/paper/zk-malle/

which grants the attacker the capability to apply transformations that modify the witnesses of a proof, thereby allowing weaker cryptographic realizations, as well as the controlled MZK (CMZK) abstraction, which excludes this kind of transformations but requires a slightly less efficient cryptographic realization. The CMZK abstraction is accessible to standard reasoning tools for equational theories; reasoning about the FMZK abstraction requires to additionally solve constraints, e.g., by means of a theorem prover.

- Second, we translate our symbolic abstraction to a symbolic F# library, which makes the abstraction accessible to verification tools that support F# such as the type checkers F5 and F7.
- Third, we prove the computational soundness of the FMZK and CMZK abstractions with respect to trace properties. More precisely, we first identify the class of *MZK-safe* protocols, which basically disallows reuse of randomness and revealing signature keys or decryption keys to the adversary. We then establish computational soundness of the FMZK abstraction for all MZK-safe protocols based on standard cryptographic assumptions (non-interactive zero-knowledge arguments of knowledge). Computational soundness of the CMZK abstraction is established for all MZK-safe protocols as well if realized using an appropriate combination of non-interactive zero-knowledge arguments of knowledge and digital signatures. The soundness results are additionally carried over to the F# library.
- Fourth, all our results are given in CoSP [2], a framework for symbolic protocol analysis and computational soundness proofs. CoSP allows for casting computational soundness proofs in a conceptually modular and generic way: proving x cryptographic primitives sound for y calculi only requires $x + y$ proofs (instead of $x \cdot y$ proofs without this framework), and the process of embedding calculi is conceptually decoupled from computational soundness proofs of cryptographic primitives.
- Finally, we illustrate the applicability of our abstraction to the analysis of real-world protocols: we reason about the security properties provided by the Anonymous Web of Trust (AWoT) [3] using our symbolic abstraction and the type checker F7. AWoT essentially realizes anonymous delegatable credentials by means of malleable ZK proofs, and it thus constitutes a suitable candidate for our symbolic abstraction and automated reasoning techniques.

An interesting direction for future work is adopting our computational soundness proof strategy for MZK proofs to observational equivalence properties. Moreover, we aim at showing deduction soundness [6], which would simplify extending our result to a wider range of cryptographic protocols that are used along with MZK proofs. Moreover, in a future work it would be interesting to investigate more efficient methods for achieving controlled-malleability for zero-knowledge proofs.

References

[1] M. Backes, F. Bendun, and D. Unruh, "Computational soundness of symbolic zero-knowledge proofs: Weaker assumptions and mechanized verification," Cryptology ePrint Archive, Report 2012/081, 2012.

[2] M. Backes, D. Hofheinz, and D. Unruh, "Cosp: A general framework for computational soundness proofs," in *ACM CCS 2009*, November 2009, pp. 66–78, preprint on IACR ePrint 2009/080.

[3] M. Backes, S. Lorenz, M. Maffei, and K. Pecina, "Anonymous webs of trust," in *Proceedings of the 10th international conference on Privacy enhancing technologies*, ser. PETS'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 130–148. [Online]. Available: http://dl.acm.org/citation.cfm?id=1881151.1881159

[4] M. Backes, M. Maffei, and D. Unruh, "Zero-knowledge in the applied pi-calculus and automated verification of the direct anonymous attestation protocol," in *IEEE Symposium on Security and Privacy 2008*, May 2008, pp. 158–169.

[5] M. Backes and D. Unruh, "Computational soundness of symbolic zero-knowledge proofs against active attackers," in *21st IEEE Computer Security Foundations Symposium, CSF 2008*, 2008, to appear.

[6] V. Cortier and B. Warinschi, "A composable computational soundness notion. chicago, usa, october 2011. acm press." in *Proc. 18th ACM Conference on Computer and Communications Security*. ACM Press, 2011.

[7] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[8] S. Even and O. Goldreich, "On the security of multi-party ping-pong protocols," in *Proc. 24th IEEE Symposium on Foundations of Computer Science (FOCS)*, 1983, pp. 34–39.

[9] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–207, 1989.

[10] M. Merritt, "Cryptographic protocols," Ph.D. dissertation, Georgia Institute of Technology, 1983.