# Zero-Knowledge Proofs

Max Ostermann

28.05.2019

# 1 Abstract

Diese Ausarbeitung ist eine Einführung in Zero-Knowledge Proofs. Nach der Einführung anhand von Alibabas Höhle und der Erklärung der grundlegenden Definitionen werden die Protokolle von Zero-Knowledge Proofs untersucht. Bei dieser Betrachtung stellt man zum Einen fest, dass die arithmetischen Operationen für ehrliche Beweisteilnehmer einen sehr geringen Rechenaufwand haben und zum Anderen, dass für alle Sprachen in NP ein Zero-Knowledge Proof existiert [Gol94]. Trotzdem fällt auf, dass selbst bei leicht berechenbaren Operationen die reine Anzahl an Interaktionen ein potentielle Limitierung von Protokollen darstellen. Anhand der zusätzlichen Möglichkeiten, die sich durch non-interactive Zero-Knowledge Proofs bieten, werden mögliche Anwendungen in modernen kryptographischen Systemen untersucht. Unter Berücksichtigung der Schwächen, wie zum Beispiel der „man-in-the-middle“ Attacke, stellt sich heraus, dass Zero-Knowledge Proofs am Besten als Teilprotokolle verwendbar sind. Dies zeigt sich unter Anderem in neuen Blockchain Anwendungen, bei denen die Integrität der einzelnen Transaktionen durch ein eigenes Protokoll sichergestellt wird und Zero-Knowledge Proofs nur zum Schutz der Privatsphäre der Nutzer dienen.

# Inhaltsverzeichnis

# 2 Einführung

In der Kryptographie geht es häufig darum, eine geheime Botschaft sicher zu übermitteln, ohne dass Dritte Zugriff auf ihren Inhalt haben. Möchte man aber stattdessen nur beweisen, dass man dieses Geheimnis kennt, ohne Informationen preiszugeben, bieten sich Zero-Knowledge Proofs an. Mit Zero-Knowledge Proofs beweist ein Beweiser einer verifizierenden Person sein Wissen über ein Geheimnis, ohne dass diese zusätzliche Informationen über das Geheimnis erlangen kann.
Dies wird im Laufe dieses Kapitels anhand zweier Beispielen verdeutlicht. Anschließend werden die grundlegenden Definitionen(3) und mit Hilfe derer der Begriff der Simulierbarkeit(4) erklärt. Darauf folgt eine kurze Übersicht über einige Protokolle und es wird die Existenz von Zero-Knowledge Proofs zu Sprachen in NP gezeigt. Unter Betrachtung der neuen Möglichkeiten, die sich mit non-interactive Zero-Knowledge Proofs(6) bieten , werden die aktuellen Anwendungen(7) von Zero-Knowledge Proofs erläutert und abschließend noch deren Schwächen betrachtet.

Schon im Jahr 1535 fand der italienische Mathematiker Niccolo Tartaglia die erste Verwendung für Zero-Knowledge Proofs[BSW06]. Er entdeckte eine Lösungsformel für Polynome 3. Grades und wollte dies beweisen, ohne, aus Furcht ein anderer Mathematiker würde es als seine Entdeckung verkaufen, diese Formel preiszugeben. Dazu bat er einen Kollegen seines Fachs um Aufgaben, welche er ihm wieder zukommen ließ. Mit seiner Lösungsformel konnte er die Aufgaben korrekt lösen, so beweisen, dass er im Besitz der korrekten Formel war und anschließend als seine Entdeckung vermarkten.

Wie man hier erkennen kann, dienen Zero-Knowledge Proofs dazu, als Beweiser, auch Prover/ P genannt, eine verifizierende Person, auch Verifier/ V genannt, von der Kenntnis eines Geheimnisses zu überzeugen, ohne dieses preiszugeben.

Um die meisten Eigenschaften von Zero-Knowledge Proofs zu veranschaulichen, stellten Quisquater und Guillous in „How to explain Zero-Knowledge Protocols to your Children“[QG90] das Konzept von Alibabas Höhle vor. Alibabas Höhle hat einen Vorraum, hinter dem ein Rundgang liegt. In der Mitte dieses Ganges ist eine magische Tür. Diese Tür lässt sich nur mit Kenntnis der geheimen Passphrase öffnen, Alice kennt dieses Geheimnis, Bob jedoch nicht. Nun möchte Alice Bob beweisen, dass sie dieses Geheimnis kennt, ohne Bob eben jenes zu offenbaren. Also befiehlt sie Bob vor der Höhle zu warten, während sie selbst in einen der beiden Eingänge des Rundgangs hineingeht. Bob betritt daraufhin den Vorraum und ruft aus welcher Seite Alice den Rundgang verlassen soll. Wenn Alice den Gang durch diese Seite betreten hat, dreht sie um und kommt zu dieser Seite wieder heraus. Hat sie jedoch den Gang von der anderen Seite betreten, muss sie nun die Passphrase verwenden, um durch die Tür gehen zu können und in dem von Bob gewünschten Ausgang zu erscheinen. Nach

einer einzigen Durchführung dieses Spiels ist Bob zurecht noch nicht von Alice Wissen überzeugt, da es sich um Zufall handeln könnte. Doch vertraut er Alice nach jeder neuen Runde etwas mehr und ist nach einigen Runden überzeugt, dass Alice die geheime Passphrase kennt, ohne dass Bob neue Informationen über die Passphrase erhalten hat.

Nun möchte Bob dieses Phänomen mit der Welt teilen und zeichnet seine Sicht mit einer Kamera auf. Doch stellt er fest, dass niemand ihm glauben würde, da er das Video auch einfach selber fälschen könnte, indem er sich entweder mit einem Freund abspricht, in welcher Reihenfolge er die Ausgänge ausruft oder die fehlerhaften Ergebnisse einfach aus dem Video herausschneidet. Stellt man die Videos, die Alice oder Bobs Freunde zeigen, nun gegenüber, zeigt sich, dass sich diese kaum voneinander unterscheiden und ein Beobachter dieser Videos keine Möglichkeit hat abzuwägen, von wem er denn das Geheimnis erlangen kann. Diese Eigenschaft wird unter „Simulierbarkeit“(5) näher betrachtet und Alibabas Höhle wird in den danach folgenden Abschnitten zur Veranschaulichung entsprechend erweitert.

# 10 Quellenverzeichnis

## Literatur


[BM89] Mihir Bellare und Silvio Micali. „Non-interactive oblivious transfer and applicaiions“. In: *Advances in Cryptology - CRYPT0 ‘89*. Springer-Verlag, 1989, 547–560.

[BSW06] Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. *Moderne Verfahren der Kryptographie*. sixth. Vieweg Verlag, 2006.

[GMR85] S Goldwasser, S Micali und C Rackoff. „The Knowledge Complexity of Interactive Proof-systems“. In: *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*. STOC ’85. ACM, 1985, S. 291–304. URL: http://doi.acm.org/10.1145/22145.22178.

[GN] Sanjam Garg und Preetum Nakkiran. „Lecture 10: Non-Interactive Zero-Knowledge (NIZK) and the Hidden-Bit Model“. In: *CS 276 – Cryptography* (). URL: https://people.eecs.berkeley.edu/~sanjamg/classes/cs276-fall14/scribe/lec10.pdf (besucht am 13. 05. 2019).

[Gol94] Yair Goldreich Odedand Oren. „Definitions and properties of zero-knowledge proof systems“. In: *Journal of Cryptology* 7.1 (1994), S. 1–32. URL: https://doi.org/10.1007/BF00195207.

[Hop+19] Daira Hopwood u. a. „Zcash Protocol Specification“. In: (2019). URL: https://github.com/zcash/zips/blob/master/protocol/protocol.pdf (besucht am 14. 05. 2019).

[QG90] Jean-Jacques Quisquater und Louis Guillous. „How to Explain Zero-Knowledge Protocols to Your Children“. In: *Advances in Cryptology — CRYPTO’ 89 Proceedings*. Hrsg. von Gilles Brassard. Springer New York, 1990, S. 628–631.

[RS92] Charles Rackoff und Daniel R. Simon. „Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack“. In: *Advances in Cryptology — CRYPTO ’91*. Hrsg. von Joan Feigenbaum. Springer Berlin Heidelberg, 1992, S. 433–444.

[TD11] Lehrstuhl Datenschutz und Datensicherheit TU Dresden Fakultät Informatik. „Zero-Knowledge-Verfahren“. In: *Komplexpraktikum* (2011). URL: https://tu-dresden.de/ing/informatik/sya/ps/ressourcen/dateien/studium/materialien/mat_kp_datensicherheit/v11_doku.pdf?lang=de (besucht am 18. 05. 2019).