Zero-Knowledge Proofs

Max Ostermann

28.05.2019

1 Abstract

Diese Ausarbeitung ist eine Einführung in Zero-Knowledge Proofs. Zuerst wird die Grundidee und Motivation anhand des Beispiels Alibabas Höhle erläutert, um die von der Rundenzahl abhängigen Wahrscheinlichkeiten von Vollständigkeit und Korrektheit zu veranschaulichen, sowie einen ersten Bezug auf die Simulierbarkeit zu nehmen. Anhand des interaktiven Protokolls der quadratischen Reste wird sowohl der Protokollablauf verdeutlicht, als auch die Korrektheit der vorkommenden Formeln exemplarisch behandelt. Daraus folgt auch der Begriff der Simulierbarkeit, welcher für die Fähigkeit steht, ein Transkript der Beweisrunden ohne Kenntnis des Geheimnisses erzeugen zu können, das (fast) nicht von einem echten Transkript zu unterscheiden ist. Vor allem im Rahmen von Signaturen ist es jedoch nicht möglich die Herausforderungen(Challenges) der verifizierenden Partei einzuholen, mit welchen Bedingungen diese generiert werden wird ebenfalls behandelt. Zuletzt werden die möglichen Anwendungen und die damit zusammenhängenden Angriffsvektoren betrachtet. Dabei gilt die größte Aufmerksamkeit der Schwäche gegen Man-in-the-middle Angriffe, die sich durch zeitliche Rahmenbedingungen stark reduzieren lässt. Abschließend wird nochmal veranschaulicht, wieso Zero-Knowledge Proofs sich auf Grund der vorher genannten Punkte besonders als Subprotokoll eignen.

Contents

2 Einführung

Schon im Jahr 1535 fand der italienische Mathematiker Niccolo Tartaglia die erste Verwendung für Zero-Knowledge Proofs. 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 schickte er Briefe an die Kollegen seines Faches, in denen er sie um Aufgaben bat, welche sie ihm wieder zukommen ließen. 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, vom Kenntnis eines Geheimnisses zu überzeugen, ohne dieses preiszugeben.

Um die meisten Eigenschaften von Zero-Knowledge Proofs zu veranschaulichen, stellten Quisquater und Guillou in "How to explain Zero-Knowledge Protocols to your Children"[QG89] das Konzept von Alibabas Höhle vor. Alibabas Höhle hat einen Vorraum, hinter dem ein Rundgang liegt, in dessen Mitte eine magische Tür ist. Diese Tür lässt sich nur durch 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.

3 Grundlagen

4 Protokolle

4.1 Auflistung

4.2 Beispiel: Quadratische Reste

5 Simulierbarkeit

6 Non-interactive Zero-Knowledge Proofs

7 Moderne Anwendungen

8 Angriffsvektoren

9 Fazit

10 Quellenverzeichnis

References

[BM89] Mihir Bellare and Silvio Micali. "Non-interactive oblivious transfer and applicaiions". In: *Advances in Cryptology - CRYPT0 '89* (1989), pp. 547 –560.

[BO+89] Michael Ben-Or et al. "Eficient identification schemes using two prover interactive proofs". In: *Advances in Cryptology - CRYPT0 '89* (1989), pp. 498 –507.

[GMR85] S Goldwasser, S Micali, and S Rackoff. "The knowledge complexity of interactive proof-systems". In: *Proceedings of the seventeenth annual ACM symposium on Theory of computin* (1985), pp. 291 –304.

[GN] Sanjam Garg and 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`.

[GO90] Oded Goldreich and Yair Oren. "Definitions and Properties of Zero-Knowledge Proof Systems". In: *Journal of Cryptography* (1990), pp. 1–32.

[QG89] Jean-Jacques Quisquater and Louis Guillous. "How to explain Zero-Knowledge Protocols to your children". In: *Advances in Cryptology - CRYPT0 '89* (1989), pp. 628 –631.

[RS91] S. Rackoff and D. R. Simon. “Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack”. In: *Advances in Cryptology - CRYPT0 ‘91* (1991), pp. 433 –445.

[Sou19a] Open Source. “Non-interactive Zero-Knowledge Proof”. In: - (2019). URL: https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof.

[Sou19b] Open Source. “Zero-Knowledge Proof”. In: - (2019). URL: https://en.wikipedia.org/wiki/Zero-knowledge_proof.

[ZKV11] Komplexpraktikum Zero-Knowledge-Verfahren. “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.