Blatt 2
Hashes, Zufallszahlen
Projekt u23

Jan Lühr

October 23, 2015

1 Hashes

1.1 Zweites Urbild

1. Was ist ein Zweites Urbild (second preimage)
2. Wie kann man generisch ein zweites Urbild finden?
3. Wie lange dauert das erwartungsgemäß?

1.2 Bitcoin

Im Bitcoin-Netzwerk suchen Miner mit einer Geschwindigkeit von ingesamt etwa 400 bis 500 PH/s (Peta Hashes pro Sekunde) nach neuen Blöcken. Verwendet wird SHA-256.

1. Wie lange bräuchte das Netzwerk um ein zweites Urbild zu finden, falls alle Miner danach suchen?
2. Nach welcher Zeit fände man mit 50% Wahrscheinlichkeit eine Kollision?

1.3 Merkle–Damgård

Daniel hat gezeigt, wie MD5 aus einem 512-Bit langen Block eine 128-Bit lange Nachricht berechnet.

1. Wie können beliebig lange Nachrichten hashed werden?
2. Ist Verfahren sicher? Welche Probleme treten auf?

1.4 Achilles, sein Freund, das Orakel und die Prüfung // Beweisbar sicherer Pseudo-Zufall

Das Orakel stellt Achilles — dem schnellsten unter den schnellfüßigen — eine Prüfung auf [1]:

> „*Ich werfe eine Münze. Es fällt Kopf oder Zahl:*
>
> - *Fällt Zahl, und schickst mit eine 128-Bit lange Nachricht, dann verschlüssele ich sie korrekt mit AES und gebe Dir den Ciphertext als Antwort. Ich verwende meinen geheimen Schlüssel für alle Deine Nachrichten.*
> - *Fällt Kopf, so bekommst Du nur zufällige Daten zurück.*
>
> *Sage mir, ob ich Kopf- oder Zahl geworfen habe! Du kannst mir beliebige Nachrichten zum Verschlüsseln geben.*“

Die Schildkröte, Achilles treuer Freund hilft ihm bei der Prüfung:

> „*Ich konnte die Prüfung vor vielen Jahren lösen. Damals verwendete das Orakel aber noch AES im Counter-Mode (AES-CTR). Ich kann die Frage beantworten, wenn die Nachrichten mehr als 9 Blöcke lang sind.*“

1. Wie kann Achilles die Aufgabe mit Hilfe seines Freundes lösen?
2. Wir vermuten, dass Achilles die Aufgabe nicht lösen kann, da AES sicher ist. Kann die Schildkröte dann ihre Aufgabe korrekt lösen? Was könnte sie damals getan haben?
3. Argumentiere: AES-CTR ist ein *beweisbar sicherer* PRNG.
4. Cassandra muss die Prüfung auch bestehen und hat keinen Freund (Apollon verlies sie bekanntlich). Das Orakel verschlüsselt bei ihr die Fragen mit AES-CBC.
   Cassandra sendet dem Orakel eine sehr lange Nachricht und besteht die Prüfung. Was hat sie getan?
5. Zeige formal:
   Sei A ein Algorithmus, (d.h. *Left-Or-Right*-Angreifer) mit Erfolgswahrscheinlichkeit ϵ und Laufzeit[2] n auf AES-CTR mit c Blöcken. Dann existiert ein Angreifer A mit Erfolgswahrscheinlichkeit ϵ und Laufzeit n' auf AES. Wie groß ist minimal n'?

[1] Left-Or-Right Security
[2] Vereinfacht: Anzahl der an das Orakel gesendeten Nachrichten