Kryptographie & Privatsphäre

Bauhaus Digitalwerkstatt

News Alert

Quiz

- *Was ist* $11^{35} \bmod 12$ *?*

  Ein Beispiel für einen Nullwissenbeweis ist "Wo ist Waldo" mit einer großen Schablone. Erkläre an dem Beispiel die Eigenschaften Completeness, Soundness und Zero
- *Knowledge!*

  Was ist eine
- *Mehrparteienberechnung?*

Restklassen

Berechnen den Ausdruck in $\mathbb{Z}_{23}$:

$$((8+9)*(2-10))^5*(5-6)$$

Lösung

Lösungslink

Knobelei

Statt eine Münze zu werfen, spielen zwei Spieler A und B ein Minispiel gegeneinander. Das Spiel funktioniert folgendermaßen:

Spieler A schreibt auf zwei Zettel jeweils (verdeckt) eine ganze Zahl, beispielsweise -6 auf den einen und 13 auf den anderen. Spieler B kennt also keine der beiden (verschiedenen) Zahlen.

Dann deckt Spieler B eine der beiden Zahlen auf, beispielsweise die 13. Nun muss er raten, ob die bereits aufgedeckte Zahl (13) die größere oder die kleinere der beiden Zahlen ist. Rät er richtig, gewinnt er, rät er falsch, so verliert er den "Münzwurf".

Ist diese Auswahlmethode fair oder kann sie von einem der beiden Spieler zu seinen Gunsten ausgenutzt werden?

Knobelei Lösung

Der ratende Spieler B kann sich einen Vorteil verschaffen, durch den er in gewissen Fällen sicher gewinnt, aber in keinem Fall einen Nachteil erleidet.

Idee: Spieler B sucht sich vor dem Aufdecken der ersten Zahl eine beliebige ganze Zahl aus und addiert dazu 0,5. Mit Hilfe dieser Zahl a hält sich Spieler B nach dem Aufdecken der ersten Zahl an folgende einfache Regel:

Ist die aufgedeckte Zahl kleiner als a, so sagt er, dass die aufgedeckte Zahl die kleinere der beiden Zahlen ist. Ist die aufgedeckte Zahl größer als a, so rät er, dass die aufgedeckte Zahl die größere der beiden Zahlen ist.

Pause

Live Programmieren

Wir bauen uns einen digitalen Würfel!

Verschlüsselung

Wir wollen Nachrichten austauschen, aber den Inhalt geheim halten.

Null-Wissen Beweis

Wir wollen Aussagen beweisen, aber unser Wissen geheim halten.

Mehrparteien-berechnung

Wir wollen Ergebnisse berechnen, aber unsere Variablen geheim halten.

Mehrparteien-berechnung

Es gab 6 frische Muffins. Auf einmal ist der Teller leer. Alle sagen, sie waren es nicht. Wieviele Lügen?

Schritt 1

Jeder hat einen geheimen Summand g_i. 0 für Wahrheit und 1 für Lüge (hat die Muffins wirklich gegessen).

Es ist bekannt eine maximalsumme s_{max} und es wird sich auf einen modulus geeinigt: $s_{max} < m$

Schritt 2

Alle Angeklagten generieren shares ihres summanden:

$$g_1 - z_{1,1} - z_{1,2} = z_{1,3} (\mod m)$$

Schritt 3

Die Shares werden an unterschiedliche Berechner verteilt und somit zu *geteilten Geheimnissen*.

A	B	C	D
$z_{1,1}$	$z_{1,2}$	$z_{1,3}$	$z_{1,4}$
$z_{2,1}$	$z_{2,2}$	$z_{2,3}$	$z_{2,4}$
$z_{3,1}$	$z_{3,2}$	$z_{3,3}$	$z_{3,4}$
$z_{4,1}$	$z_{4,2}$	$z_{4,3}$	$z_{4,4}$

Andere Mehrpateienberechnungen:

- Private set intersection
- Multi-party fair exchange protocol

Exkurs: Entropie in der Thermodynamik

In einem abgeschlossenen System, das sich durch spontane innere Prozesse (wie Wärmeleitung, Vermischung durch Diffusion, Erzeugung von Reibungswärme, chemische Reaktion etc.) dem thermodynamischen Gleichgewicht annähert, steigt die Entropie des Systems durch diese Prozesse an. Der Gleichgewichtszustand ist erreicht, wenn die Entropie den größtmöglichen Wert erreicht, der mit den gegebenen äußeren Parametern des Systems (wie Volumen, Energie, Teilchenzahlen, äußeres Kraftfeld etc.) verträglich ist. --Wikipedia

Ende