SMS1 für MC, FHS Hagenberg
9. Übungsblatt für den 2. Dezember 2004

Zero-Knowledge:

1. Das Authentifizierungsprotokoll von Fiat-Shamir mit Modul $n = 46243$ und $t = 2$: Sie wählen etwa das Geheimnis $s = 9436$ und geben den öffentlichen Schlüssel v bekannt.

   Um sich bei Bob zu identifizieren, wählen Sie $r_1 = 15497$ und schicken den zugehörigen Zeugen an Bob. Der antwortet mit der Herausforderung (challenge) $e = 0$. Was antworten Sie?

   In der zweiten Runde wählen Sie $r_2 = 29054$ und erhalten die Herausforderung $e = 1$. Was sollen Sie antworten?

2. Es seien n, t wie in Aufgabe 1. Alice hat den öffentlichen Schlüssel $v = 5631$ und möchte sich bei Ihnen identifizieren. In der ersten Runde schickt sie den Zeugen $x_1 = 5564$ und antwortet auf die Herausforderung $e = 1$ mit $y_1 = 18360$. In der zweiten Runde schickt sie den Zeugen $x_2 = 40947$ und antwortet auf die Herausforderung $e = 0$ mit $y_2 = 34905$. Was schließen Sie?

3. Wie können Sie beim Fiat-Shamir Protokoll vortäuschen, das Geheimnis s zu kennen, wenn Sie wissen, dass Bob immer die Herausforderung $e = 0$ stellt? Wie, wenn Bob immer $e = 1$ fordert?

4. Recherche: Beschreiben Sie das Authentifizierungsprotokoll nach Schnorr [1, 10.4.4]).

5. Das Authentifizierungsprotokoll von Schnorr für die Parameter $(p, q, \beta) = (10061, 503, 3997)$ und $t = 8$: Sie wählen etwa den privaten Schlüssel $a = 436$ und geben den öffentlichen Schlüssel v bekannt.

   Um sich bei Bob zu identifizieren, wählen Sie $r = 298$ und schicken den zugehörigen Zeugen an Bob. Der gibt die Herausforderung $e = 113$ zurück. Was antworten Sie? Wie überprüft Bob Ihre Antwort?

6. Wie können Sie beim Schnorr-Protokoll vortäuschen, den privaten Schlüssel a zu kennen, wenn Sie vor Beginn des Nachrichtenaustauschs wissen, welche Herausforderung e Bob stellen wird?

Literatur

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography.* CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.