Technische Universität Braunschweig

Institut für Theoretische Informatik

Dr. Jürgen Koslowski

# Cryptologie 3

Aufgabenblatt 1, 2017-04-27

## Übungsaufgabe 1

Führen Sie das *Feige-Fiat-Shamir-Verfahren* (Protokoll 11.2) zur Identifikation durch. Verwenden sie dabei zunächst Algorithmus 11.3 zur Bestimmung der Identifikationsinformationen. Als Parameter werden durch das "Vertrauenszentrum" die Werte $n = 23 \cdot 31 = 713$ und $k = 3$ gewählt. Außerdem wird $ID(\text{Alice}) = 42$ sowie $t = 2$ festgelegt. Die Zufallszahlen bzw. Zufallsbits entnehmen Sie in dieser Reihenfolge (!) bitte den "zufälligen" Folgen

$$(111, 222, 333, 555, 444) \qquad \text{bzw.} \qquad (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$$

*Lösungsvorschlag:*

Algorithmus 11.3:

(1) $p = 23$ und $q = 31$ erfüllen

$$p \bmod 4 = q \bmod 4 = 3$$

$k = 3$ war ebenfalls gegeben.

(2) Alice wählt wie vorgegeben

$$s_0 = 111 \quad , \quad s_1 = 222 \quad \text{sowie} \quad s_2 = 333$$

mit

$$111^{-1} \bmod 713 = 546 \quad , \quad 222^{-1} \bmod 713 = 273 \quad \text{sowie} \quad 333^{-1} \bmod 713 = 182$$

(3) Alice wählt wie vorgegeben

$$(c_0, c_1, c_2) = (0, 1, 1)$$

(4) Alice berechnet

$$\begin{aligned} w_0 &= (-1)^0 111^{-2} \bmod 713 = 82 \\ w_1 &= (-1)^1 222^{-2} \bmod 713 = -273^2 \bmod 713 = 336 \\ w_2 &= (-1)^1 333^{-2} \bmod 713 = -182^2 \bmod 713 = 387 \end{aligned}$$

(5) Das "Vertrauenszentrum" erhält $(w_0, w_1, w_2)$ und überprüft $ID(\text{Alice}) = 42$. Weiterhin ist zu überprüfen, ob $\pm w_i \in R_n$ gilt für $i < 3$:

$$82^{11} \bmod 23 = 1 \quad \text{und} \quad 82^{15} \bmod 31 = 1$$

impliziert

$$(82 \bmod 23, 82 \bmod 31) = (13, 20) \in R_{23} \times R_{31} \cong R_{713}$$

Analog erhalten wir

$$336^{11} \bmod 23 = -1 \quad \text{und} \quad 336^{15} \bmod 31 = -1$$

impliziert

$$(-336 \bmod 23, -336 \bmod 31) = (9,5) \in R_{23} \times R_{31} \cong R_{713}$$

sowie

$$387^{11} \bmod 23 = -1 \quad \text{und} \quad 387^{15} \bmod 31 = -1$$

impliziert

$$(-387 \bmod 23, -387 \bmod 31) = (4,16) \in R_{23} \times R_{31} \cong R_{713}$$

Veröffentlicht wird das Tupel $(42, 82, 336, 387)$.

Protokoll 11.2 (Identifikation von Alice bei Bob mit $t = 2$):

(1) Alice sendet $ID(\text{Alice}) = 42$ an Bob.

(2) Bob besorgt sich $(w_0, w_1, w_2) = (82, 336, 387)$.

i=0 (3) Alice wählt $r_0 = 555$ und $b_0 = 1$, und sendet

$$v_0 = (-1)^{b_0} r_0^2 \bmod n = -555^2 \bmod 713 = -9 \bmod 713 = 704$$

an Bob.

(4) Bob sendet den Zufallsvektor $(b_{11}, b_{12}, b_{13}) = (1,0,1)$ an Alice.

(5) Alice antwortet mit

$$u_0 = r_0 \cdot s_0 \cdot s_2 \bmod 713 = 555 \cdot 111 \cdot 333 \bmod 713 = 29$$

(6) Bob berechnet

$$v_0' = u_0^2 \cdot w_0 \cdot w_2 \bmod n = 29^2 \cdot 82 \cdot 387 \bmod 713 = 704$$

und überprüft $v_0 \in \{v_0', -v_0' \bmod n\}$. In der Tat gilt hier

$$v_0 = v_0' = 704$$

i=1 (3) Alice wählt $r_1 = 444$ und $b_1 = 0$, und sendet

$$v_1 = (-1)^{b_0} r_0^2 \bmod n = 444^2 \bmod 713 = 348$$

an Bob.

(4) Bob sendet den Zufallsvektor $(b_{21}, b_{22}, b_{23}) = (1,1,0)$ an Alice.

(5) Alice antwortet mit

$$u_1 = r_1 \cdot s_0 \cdot s_1 \bmod 713 = 444 \cdot 111 \cdot 222 \bmod 713 = 63$$

(6) Bob berechnet

$$v_1' = u_1^2 \cdot w_0 \cdot w_1 \bmod n = 63^2 \cdot 82 \cdot 336 \bmod 713 = 365$$

und überprüft $v_1 \in \{v_1', -v_1' \bmod n\}$. In der Tat gilt hier

$$v_1 = 348 = (-365) \bmod 713 = -v_0' \bmod 713$$

(7) Bob akzeptiert die Identifizierung.

### Übungsaufgabe 2

Eine Variante des Fiat-Shamir-Signaturverfahrens gemäß Ong und Schnorr (1991):

Die TA wählt große Zufallsprimzahlen $p$ und $q$, zwei Sicheheitsparameter $k, t \in \mathbb{N}$ und eine Hash-Funktion $h$ mit Werten der Länge (mindestens) $tk$. Weiter verfügt sie über ein asymmetrisches Chiffrierverfahren $\langle E_{\text{TA}}, D_{\text{TA}} \rangle$. Die Werte $n = p \cdot q$, $h$, $k$, $t$ und der öffentliche Schlüssel $e_{\text{TA}}$ werden veröffentlicht.

Jeder Nutzer $A$ wählt einen geheimen Schlüssel $\vec{s}_A \in (\mathbb{Z}_n^*)^k$. Der zugehörige öffentliche Schlüssel $\vec{v}_A \in (\mathbb{Z}_n^*)^k$ hat die Komponenten $(v_A)_i = (s_A)_s^{-2^t}$, $i < k$.

Die TA registriert den Nutzer $X$, indem sie seine Identität überprüft und das Paar $\langle I\!D(X), \vec{v}_X \rangle$ signiert, was ein Zertifikat $Z(X) = \langle I\!D(X), \vec{v}_X, D_{\mathrm{TA}}\langle I\!D(X), \vec{v}_X \rangle\rangle$ liefert (vergl. Kapitel 8.2 im Buch/Skript).

Das Protokoll in Diagrammform, im Vergleich zu Protokoll 11.1:

$$\begin{tikzcd}
A \arrow[d, "r \in \mathbb{Z}_n^*"'] & \\
A \arrow[d, "\vec{e} := h(M \| r^{2^t} \bmod n)"'] & \\
A \arrow[r, "{Z(A),\, M}", "{\vec{e},\, y := r \prod_{j<k} s_j^{\sum_{i<t} e_{i,j} \cdot 2^i} \bmod n}"'] & B \arrow[d, "\text{teste } Z(A)"] \\
& B \arrow[d, "h(M \| y^{2^t} \prod_{j<k} v_j^{\sum_{i<t} e_{i,j} \cdot 2^i} \bmod n) \stackrel{?}{=} \vec{e}"] \\
& B
\end{tikzcd}$$

Untersuchen Sie dieses Verfahren auf seine Vollständigkeit und Sicherheit. Welche Vor- oder Nachteile bestehen im Vergleich zum Fiat-Shamir Signaturverfahren?

*Lösungsvorschlag:*

Wir verweisen auf den Originalartikel in den Materialien, und beschränken uns ansonsten auf den Nachweis der Vollständigkeit:

Dazu ist nachzuweisen, dass der zweite Teil des Arguments, das von Bob gehasht wird, mit $r^{2^t} \bmod n$ übereinstimmt:

$$\begin{aligned}
y^{2^t} \prod_{j<k} v_j^{\sum_{i<t} e_{i,j} \cdot 2^i} \bmod n &= r^{2^t} \left( \prod_{j<k} s_j^{\sum_{i<t} e_{i,j} \cdot 2^i} \right)^{2^t} \left( \prod_{j<k} v_j^{\sum_{i<t} e_{i,j} \cdot 2^i} \right) \bmod n \\
r &=^{2^t} \left( \prod_{j<k} s_j^{2^t \cdot \sum_{i<t} e_{i,j} \cdot 2^i} \right) \left( \prod_{j<k} s_j^{-2^t \cdot \sum_{i<t} e_{i,j} \cdot 2^i} \right) \bmod n \\
&= r^{2^t} \left( \prod_{j<k} s_j^{0 \cdot \sum_{i<t} e_{i,j} \cdot 2^i} \right) \bmod n \\
&= r^{2^t} \bmod n
\end{aligned}$$

Anmerkung: Warum kann man nicht den Exponenten $2$ anstelle von $2^t$ verwenden? Warum steigt durch wiederholtes Quadrieren die Sicherheit?