Protokolli turvalisus

Protokoll on turvaline, kui ründaja vaade on sõltumatu salajasest teatest M. See tähendab:

1. Protokoll töötab. Ka ründaja tegutseb.
2. Peale protokolli töö lõppu visatakse münti.
3. Kui tuli kull, siis antakse ründajale salajane teade M.
4. Kui tuli kiri, siis antakse ründajale teade M', mis on
   - M-st sõltumatu;
   - sama jaotusega kui M.
5. Ründaja püüab ära arvata mündiviske tulemust.

Protokoll on *turvaline*, kui äraarvamise tõenäosus pole oluliselt suurem kui $1/2$.

Interpretatsioon

- Generate^l key x

$$I(x) = \underline{key}(l)$$

- Generate^l random x

$$I(x) = \underline{random}(l)$$

- $x := (x_1, \ldots, x_k)$

$$I(x) = \underline{tuple^k}(I(x_1), \ldots, I(x_k))$$

- $x := \pi_i^{(k)}(y)$

$$I(x) = \underline{\pi_i^k}(I(y))$$

- $x := encr_k^l(y)$

$$I(x) = \underline{encr}(l, I(k), I(y))$$

- $x := decr_k(y)$

$$I(x) = \underline{decr}(I(k), I(y))$$

- Receive^l x

$$I(x) = \underline{input}(l)$$

Seejuures peaks ka lihtsustama.

- Check if $x = y$

1. Kontrolli, kas $I(x) = I(y)$ on üldse võimalik. Eeldame, et on.
2. Tee kindlaks, kumb termidest $I(x)$ ja $I(y)$ on „lihtsam“.
   * $\underline{key}(l)$, $\underline{random}(l)$ on lihtsaimad.
   * $\underline{input}(l)$-e sisaldavad termid on keerulisimad.
   * $\underline{input}(\textsf{hilisem})$ on keerulisem kui $\underline{input}(\textsf{varasem})$

   Loeme, et $I(x)$ on lihtsam.
3. Kirjuta üle: $I(y) := I(x)$.
4. Ka $I(z)$-des asenda alamterm $I(y)$ termiga $I(x)$.

- $z := \mathit{case}\ w\ \mathit{of}$

$$
\begin{aligned}
& x_1 \to y_1 \\
& \cdots\cdots\cdots \\
& x_n \to y_n
\end{aligned}
$$

See asenda lausetega

$$
\begin{aligned}
& \text{Check if } w = x_i \\
& z := y_i
\end{aligned}
$$

Siin $i \in \{1, \ldots, n\}$ on valitud „mittedeterministlikult“.