

1.1

Annahme π PFS $\Rightarrow US[M=m|C=c] = US[M=m]$

$$US[M=m|C=c] = \frac{US[C=c|M=m] \cdot US[M=m]}{US[C=c]}$$

1.2

$$US[C=c|M=m] \cdot US[M=m] = \frac{1}{2} \text{ da PFS } \text{f}$$

$$= \frac{US[C=c|M=m] \cdot US[M=m] + US[C=c|M=m'] \cdot US[M=m']}{\text{f}}$$

$$= \frac{US[C=c|M=m] \cdot \frac{1}{2}}{\frac{1}{2} (US[C=c|M=m] + US[C=c|M=m'])}$$

$US[C=c] + US[C=c]$

$$= \frac{US[C=c|M=m]}{2 US[C=c]} = \frac{1}{2} \Rightarrow \pi \text{ PFS}$$

1.3

1.4

Annahme $US[M=m] \neq US[M=m'] \Rightarrow \pi$ nicht PFS

$$US[M=m|C=c] = \frac{US[C=c|M=m] \cdot US[M=m]}{US[C=c]}$$

$$US[C=c] = US[C=c|M=m] \cdot US[M=m] + US[C=c|M=m'] \cdot US[M=m']$$

$$US[C=c|M=m] \cdot US[M=m] = US[C=c|M=m'] \cdot US[M=m']$$

$$US[C=c|M=m] \cdot US[M=m] = US[C=c] \cdot US[M=m]$$

$$US[C=c] \cdot US[M=m] = US[C=c] \cdot US[M=m']$$

$$\frac{US[C=c]}{US[C=c]} \cdot \underline{US[M=m] = US[M=m']}$$

Annahme verletzt \Rightarrow TT muss PFS sein.

2.1



Daniel Benford	108	019	210	217
Sergej Mamberger	108	019	231	345
Max Randhuhn	108	019	211	207

UG AF

Index der Kommentare

- 1.1 PFS ist eine etwas unglückliche Abkürzung, da diese für Perfect Forward Secrecy steht
- 1.2 nein, dass gilt i.A. nicht für perfekte Sicherheit!
- 1.3 Ihr habt hier versucht zu zeigen, dass wenn PI perfekt sicher ist, dass dann auch PI perfekt sicher ist.
- 1.4 es existieren perfekt sichere Verschlüsselungsverfahren bei denen $Ws[M=m] \neq Ws[M=m']$
- 2.1 das war nicht das was ihr zeigen oder widerlegen solltet.