Grundlagen Informations Sicherheit
Übungsblatt 05

Max Kurz (3265240) Mohamed Barbouchi (3233706)
Daniel Kurtz (3332911)

Problem 1

$$
\begin{aligned}
f_1 \cdot_{\mathbb{F}_{2^8}} f_2 = f_1 \cdot_{\mathbb{Z}_2[x]} f_2 \quad \bmod g &= \\
x^7 + x^5 + x^4 + x^2 + x \cdot_{\mathbb{Z}_2[x]} x^6 + x^4 + x + 1 \quad \bmod g &= \\
x^{13} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^3 + x \quad \bmod g &=
\end{aligned}
$$

Mit der Polynomdivision bildet der entstandene Rest das Ergebnis übertragen nach $\mathbb{Z}_2$:

$$x^5 + x^4 + x^2 + x$$

.

$$
\begin{array}{lllllllllll}
(& x^{13} & + x^{10} & + x^9 & + x^8 & & + x^5 & + x^4 & + x^3 & & + x \big) \div \left(x^8 + x^4 + x^3 + x + 1\right) = x^5 + x^2 + \frac{-2x^6 - x^5 + x^4 - x^2 + x}{x^8 + x^4 + x^3 + x + 1} \\
 & - x^{13} & & - x^9 & - x^8 & - x^6 & - x^5 & & & & \\
\hline
 & & x^{10} & & & - x^6 & & + x^4 & + x^3 & & \\
 & & - x^{10} & & & - x^6 & - x^5 & & - x^3 & - x^2 & \\
\hline
 & & & & & - 2x^6 & - x^5 & + x^4 & & - x^2 &
\end{array}
$$

Problem 2

a) Seien f und p beliebige Polynome. Dann gilt:

$$
\begin{aligned}
\deg(f \cdot p) &= \deg(\sum a_i x^i \cdot \sum a_j x^i) \\
&= \deg(\max\{x^i\} \cdot \max\{x^j\}) \quad \forall a_i, a_j \neq 0 \\
&= \deg(x^i_{\max} \cdot x^j_{\max}) \\
&= \deg(\underbrace{(x_{\max} \cdot \ldots \cdot x_{\max})}_{\text{i-mal}} \cdot \underbrace{(x_{\max} \cdot \ldots \cdot x_{\max})}_{\text{j-mal}}) = \deg(\underbrace{x_{\max} \cdot \ldots \cdot x_{\max}}_{\text{i+j -mal}}) \\
&= \deg(x^{i+j}) = \deg(x^i) + \deg(x^j) \\
&= \deg(f) + \deg(g)
\end{aligned}
$$

$\square$

b)

Abgeschlossenheit unter Addition

Es gilt $\forall i\, a_i + b_i \in F$ und damit $(a_0 + b_0, \ldots) \in F[x]$, da F ein Körper ist und unter Addition abgeschlossen ist.

$$f +_{F[x]} g = (a_0, a_1, \ldots) +_{F[x]} (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

Kommutativität der Addition

$$\begin{aligned} f +_{F[x]} g = (a_0, a_1, \ldots) +_{F[x]} (b_0, b_1, \ldots) &= (a_0 + b_0, a_1 + b_1, \ldots) = (b_0 + a_0, b_1 + a_1, \ldots) \\ &= (b_0, b_1, \ldots) +_{F[x]} (a_0, a_1, \ldots) = g +_{F[x]} f \end{aligned}$$

Assoziativität der Addition

$$\begin{aligned} (f +_{F[x]} g) +_{F[x]} h &= (a_0 + b_0, a_1 + b_1, \ldots) + (c_0, c_1, \ldots) \\ &= ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, \ldots) \\ &= (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), \ldots) = f +_{F[x]} (g +_{F[x]}) \end{aligned}$$

Neutrales Element der Addition

Sei $e_+ = (0, 0, \ldots, 0)$, wobei 0 das neutrale Element von F ist. Dann gilt:

$$\begin{aligned} f +_{F[x]} e_+ &= (a_0 + 0, a_1 + 0, \ldots) = (a_0, a_1, \ldots) = f \\ e_+ +_{F[x]} f &= (0 + a_0, 0 + a_1, \ldots) = (a_0, a_1, \ldots) = f \end{aligned}$$

Nichtleerheit

Es gilt $e_+ \in F[x]$, damit folgt $F[x] \neq \emptyset$.

Existenz des inversen Elemente

Sei a_i^{-1} das inverse Element zu a_i in F für alle $a_i \in F$ und $f^{-1} = (a_0^{-1}, a_1^{-1}, \ldots)$.

$$f +_{F[x]} f^{-1} = (a_0 + a_0^{-1}, a_1 + a_1^{-1}, \ldots) = (0, 0, 0, \ldots) = (a_0^{-1} + a_0, \ldots) = f^{-1} +_{F[x]} f$$

Abgeschlossenheit unter Multiplikation

Da F ein Körper ist, ist F abgeschlossen unter Multiplikation und Addition. Damit ist $(d_0, d_1, \ldots) \in F[x]$ und $f \cdot_{F[x]} g = (d_0, d_1, \ldots)$ mit $d_i = \sum_{j \leq i} a_j \cdot b_{i-j}$ und $d_i \in F$

Kommutativität der Multiplikation

$$\begin{aligned} f \cdot_{F[x]} g &= (\sum_{j \leq 0} a_j \cdot b_{0-j}, \sum_{j \leq 1} a_j \cdot b_{1-j}, \ldots) \\ &= (\sum_{j \leq 0} b_j \cdot a_{0-j}, \sum_{j \leq 1} b_j \cdot a_{1-j}, \ldots) \\ &= g \cdot_{F[x]} f \end{aligned}$$

Distributivgesetze

$$\begin{aligned} (f +_{F[x]} g) \cdot_{F[x]} h = (a_0 + b_0, a_1 + b_1, \ldots) \cdot_{F[x]} (c_0, c_1, \ldots) &= (\sum_{j \leq 0} (a_0 + b_0) \cdot c_{0-j}, \ldots) \\ &= (\sum_{j \leq 0} a_0 \cdot c_{0-j} + b_0 \cdot c_{0-j}, \ldots) \\ &= (\sum_{j \leq 0} a_0 \cdot c_{0-j} + \sum_{j \leq 0} b_0 \cdot c_{0-j}, \ldots) \\ &= (f \cdot_{F[x]} h +_{F[x]} (g \cdot_{F[x]} h) \end{aligned}$$

$$\begin{aligned} f \cdot_{F[x]} (g +_{F[x]} h) = f \cdot_{F[x]} (b_0 + c_0, b_1 + c_1, \ldots) &= (\sum_{j \leq 0} a_0 \cdot (b_{0-j} + c_{0-j}), \ldots) \\ &= (\sum_{j \leq 0} a_0 \cdot b_{0-j} + a_0 \cdot c_{0-j}, \ldots) \\ &= (\sum_{j \leq 0} a_0 \cdot b_{0-j} + \sum_{j \leq 0} a_0 \cdot c_{0-j}, \ldots) \\ &= (f \cdot_{F[x]} g) +_{F[x]} (f \cdot_{F[x]} h) \end{aligned}$$

$\square$

Problem 3

Sei x und x' unterschiedlich aber es gilt $h_n(x) = h_n(x')$.

Algorithm 1

```
Generate Keypair ((n, e), (n, d))
send(x)
receive(s) und s = PKCS-sig(x, (n, d)) = h_n(x)^d mod n
output(x', s)
```

Der Angreifer hat einen Vorteil von 1.
$V'(x', s, (n, e)) = V(h_n(x'), s, (n, e)) =$ `vaild`, da:

$$\begin{aligned} h_n(x') &= h_n(x) \text{ und} \\ s^e &= h_n(x)^{de} \mod n = h_n(x) \end{aligned}$$

Das bedeutet also dass der Angreifer ohne das Orakel mit dieser Message zubefragen, einen `valid`-Tag gefunden hat und somit immer das Game gewinnt.

Problem 4

a)

1. Data link (Source MAC = aa:aa:aa:aa:aa:aa, Dest. MAC = ff:ff:ff:ff:ff:ff) /
ARP (Who has 10.0.0.1 ?)
2. Data link (Source MAC = 01:01:01:01:01:01, Dest. MAC = aa:aa:aa:aa:aa:aa) /
ARP (I have 10.0.0.1)
3. Data link (Source MAC = aa:aa:aa:aa:aa:aa, Dest. MAC = 01:01:01:01:01:01) /
IP (Source IP = 10.0.0.2, Dest. IP = 10.0.0.1) /
UDP (Source Port = 16000 , Dest. Port = 53) /
DNS (Transaction ID = 0x0000, query = "www.example.com, type A, class IN")
4. IP (Source IP = 19.19.19.19, Dest. IP = 4.0.0.1) /
UDP (Source Port = 16001 , Dest. Port = 53) /
DNS (Transaction ID = 0x0001, query = "www.example.com, type A, class IN")
5. IP (Source IP = 4.0.0.1, Dest. IP = 19.19.19.19) /
UDP (Source Port = 53 , Dest. Port = 16001) /
DNS (answer = "dont know, ask 4.0.0.2", Transaction ID = 0x0001, response for ="www.example.com, type A, class IN")
6. IP (Source IP = 19.19.19.19, Dest. IP = 4.0.0.2) /
UDP (Source Port = 16002 , Dest. Port = 53) /
DNS (Transaction ID = 0x0002, query = "www.example.com, type A, class IN")
7. IP (Source IP = 4.0.0.2, Dest. IP = 19.19.19.19) /
UDP (Source Port = 53 , Dest. Port = 16002) /
DNS (answer = "dont know, ask 4.0.0.3", Transaction ID = 0x0002, response for ="www.example.com, type A, class IN")
8. IP (Source IP = 19.19.19.19, Dest. IP = 4.0.0.3) /
UDP (Source Port = 16003 , Dest. Port = 53) /
DNS (Transaction ID = 0x0003, query = "www.example.com, type A, class IN")
9. IP (Source IP = 4.0.0.3, Dest. IP = 19.19.19.19) /
UDP (Source Port = 53 , Dest. Port = 16003) /
DNS (answer = "www.example.com, type A, class IN, 1.2.3.4", Transaction ID = 0x0003, response for ="www.example.com, type A, class IN")
10. Data link (Source MAC = 01:01:01:01:01:01, Dest. MAC = aa:aa:aa:aa:aa:aa) /
IP (Source IP = 10.0.0.1 , Dest. IP = 10.0.0.2) /
UDP (Source Port = 16000 , Dest. Port = 53) /
DNS (answer = "www.example.com, type A, class IN, 1.2.3.4", Transaction ID = 0x0000, response for ="www.example.com, type A, class IN")
11. Data link (Source MAC = aa:aa:aa:aa:aa:aa, Dest. MAC = 01:01:01:01:01:01) /
IP (Source IP = 10.0.0.2, Dest. IP = 1.2.3.4) /
TCP (SYN, Source Port = 17000 , Dest. Port = 80, Seq = 1)
12. IP (Source IP = 19.19.19.19, Dest. IP = 1.2.3.4) /
TCP (SYN, Source Port = 17001 , Dest. Port = 80, Seq = 1)

13. IP (Source IP = 1.2.3.4, Dest. IP = 19.19.19.19) /
    TCP (SYN-ACK, Source Port = 80 , Dest. Port = 17001, Seq = 10, ACK = 2)
14. Data link (Source MAC = 01:01:01:01:01:01, Dest. MAC = aa:aa:aa:aa:aa:aa) /
    IP (Source IP = 1.2.3.4, Dest. IP = 10.0.0.2) /
    TCP (SYN-ACK, Source Port = 80 , Dest. Port = 17000, Seq = 10, ACK = 2)
15. Data link (Source MAC = aa:aa:aa:aa:aa:aa, Dest. MAC = 01:01:01:01:01:01) /
    IP (Source IP = 10.0.0.2, Dest. IP = 1.2.3.4) /
    TCP (ACK, Source Port = 17000 , Dest. Port = 80, Seq = 2, ACK = 11)
16. IP (Source IP = 19.19.19.19, Dest. IP = 1.2.3.4) /
    TCP (ACK, Source Port = 17001 , Dest. Port = 80, Seq = 2, ACK = 11)
17. Data link (Source MAC = aa:aa:aa:aa:aa:aa, Dest. MAC = 01:01:01:01:01:01) /
    IP (Source IP = 10.0.0.2, Dest. IP = 1.2.3.4) /
    TCP (Message, Source Port = 17000 , Dest. Port = 80, Seq = 3) /
    HTTP (GET / HTTP1.1, HOST = www.example.com)
18. IP (Source IP = 19.19.19.19, Dest. IP = 1.2.3.4) /
    TCP (ACK, Source Port = 17001 , Dest. Port = 80, Seq = 3) /
    HTTP (GET / HTTP/1.1, HOST = www.example.com)
19. IP (Source IP = 1.2.3.4, Dest. IP = 19.19.19.19) /
    TCP (Message, Source Port = 80 , Dest. Port = 17001, Seq = 11, ACK = 4) /
    HTTP (HTTP/1.1 200 OK, Content-Length: ..., Content = <html>...</html>)
20. Data link (Source MAC = 01:01:01:01:01:01, Dest. MAC = aa:aa:aa:aa:aa:aa) /
    IP (Source IP = 1.2.3.4, Dest. IP = 10.0.0.2) /
    TCP (Message, Source Port = 80 , Dest. Port = 17000, Seq = 11, ACK = 4) /
    HTTP (HTTP/1.1 200 OK, Content-Length: ..., Content = <html>...</html>)
21. Data link (Source MAC = aa:aa:aa:aa:aa:aa, Dest. MAC = 01:01:01:01:01:01) /
    IP (Source IP = 10.0.0.2, Dest. IP = 1.2.3.4) /
    TCP (FIN, Source Port = 17000 , Dest. Port = 80, Seq = 4, ACK = 12)
22. IP (Source IP = 19.19.19.19, Dest. IP = 1.2.3.4) /
    TCP (FIN, Source Port = 17001 , Dest. Port = 80, Seq = 4, ACK = 12)
23. IP (Source IP = 1.2.3.4, Dest. IP = 19.19.19.19) /
    TCP (FIN, Source Port = 80 , Dest. Port = 17001, Seq = 12, ACK = 5)
24. Data link (Source MAC = 01:01:01:01:01:01, Dest. MAC = aa:aa:aa:aa:aa:aa) /
    IP (Source IP = 1.2.3.4, Dest. IP = 10.0.0.2) /
    TCP (FIN, Source Port = 80 , Dest. Port = 17000, Seq = 12, ACK = 5)
25. Data link (Source MAC = aa:aa:aa:aa:aa:aa, Dest. MAC = 01:01:01:01:01:01) /
    IP (Source IP = 10.0.0.2, Dest. IP = 1.2.3.4) /
    TCP (ACK, Source Port = 17000 , Dest. Port = 80, Seq = 5, ACK = 13)
26. IP (Source IP = 19.19.19.19, Dest. IP = 1.2.3.4) /
    TCP (ACK, Source Port = 17001 , Dest. Port = 80, Seq = 5, ACK = 13)

Problem 5

a) Wir müssen die TXID und den UDP Source Port raten. Dies sind 2^{16} Werte jeweils, also insgesamt 2^{32} Werte. Die Wahrscheinlichkeit beim ersten Versuch richtig zu raten liegt also bei $P = 2^{-32}$

b) Wie bereits in oben beschrieben gibt es 2^{32} mögliche Werte, also muss eine Angreifer durchschnittlich $\frac{2^{32}}{2}$ verschiendene Werte raten um erfolgreich zu sein.

Geht man von 2000 Versuchen pro Runde und 0,1 Sekunden pro Runde aus, kann man die Durchschnittliche Zeit in Sekunden berechnen:

$$\begin{aligned}
&= \frac{2^{31}\ \text{value}}{\frac{2000\frac{\text{value}}{\text{round}}}{0,1\frac{\text{second}}{\text{round}}}} \\
&= \frac{2^{31}\text{value}}{20000\frac{\text{value}}{\mathit{second}}} \\
&= 107374,182 \text{ seconds } \mathrel{\widehat{=}} 1,243 \ \text{ days}
\end{aligned}$$