Daniel Pantjuskin-Moos
108013248222
Vincent König
108011232630
Gruppe: D

Abgabe PHYSEC 4

1. Bit Error Rate

Hier Aufgabe 1 bearbeiten.
Nichts muss importiert werden.
Einfach starten wie gewohnt

Abbildung 1: Testbild kann gelöscht werden sobald gesehen

2. Implementierung Quantisierer

Hier Aufgabe 2 bearbeiten

2..1 Implementierung Jana Multibit

2..2 Implementierung Mathur, Suhas

3. Attack Trees

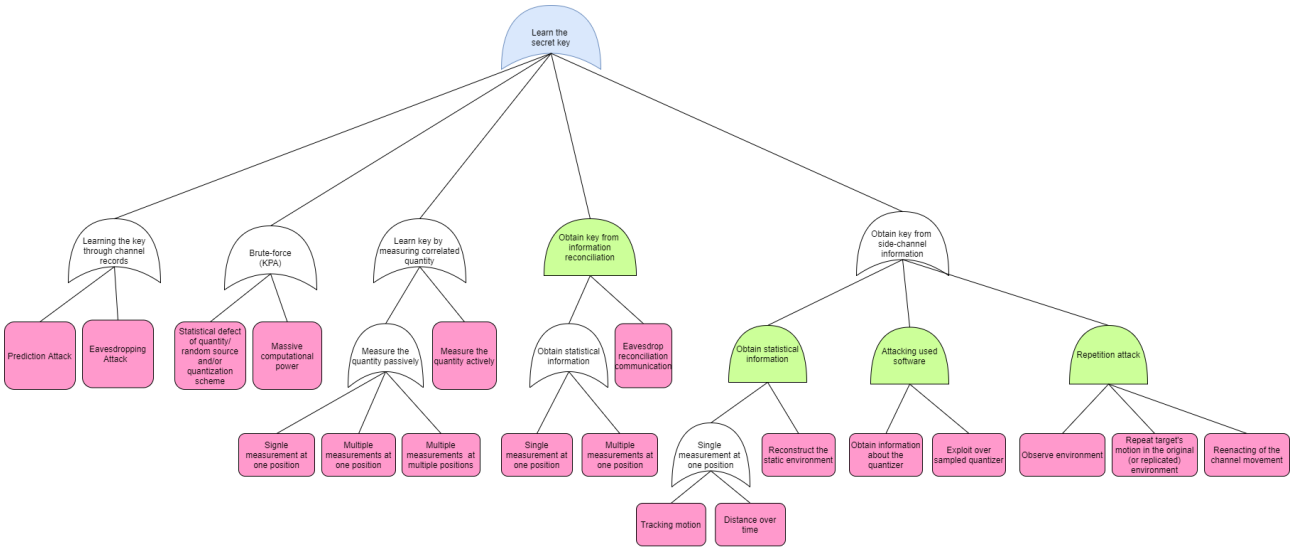

Abbildung 2: Attack tree

4. Angriffe

5. Reading Assignment

5..1 Nennen Sie 5 verschiedene Quellen für Entropie

Physikalische Phänomene

- Radioaktiver Zerfall
- Transmission von Photonen
- Thermisches Rauschen (Johnson-Nyquist-Rauschen)
- Geräusche der Atmosphäre
- Jitter

Mensch-Gerät Interaktion

- Dauer von Tastendrücken und andere Zeitmessungen
- Tasten-und Mausbewegungen
- Bewegungs- und Beschleunigungssensoren

5..2 Wie viele Samples aus einem Smartphone Accelerator benötigen wir um einen 128 bit key zu erstellen?

„Since the recommended security level for almost random bits is $\epsilon = 2^{-80}$. According to the heuristic (1) we need roughly 128/0.125 = 1024 samples to extract a 128-bit key. However taking into account the true error in our Theorem 1 we see that we need at least n $\approx$ 2214 bits!“

Laut dem Paper, welches sie auf Theoreme stützt, braucht man mindestens 1024 Samples. Hinzu kommt allerdings, dass empfohlen wird, ein *n* mit mehr als 2214 Bitlänge zu wählen.

5..3 Wie groß ist der Unterschied an tatsächlich extrahierbarer Entropie und Shannon Entropie?

Corollary 1 (A Signifficant Entropy Loss in the AEP Heuristic Estimate). *In the above setting, the gap between the Shannon entropy and the number of extractable bits ϵ-close to uniform equals at least $\Theta(\sqrt{\log(1/\epsilon)kn})$. In particular, for the recommended security level ($\epsilon = 2^{-80}$) we obtain the loss of $kn - N \approx \sqrt{80kn}$ bits, no matter what an extractor we use.*

Abbildung 3: Auszug aus dem Paper

„In information theory most widely used is Shannon entropy, which quantifies the encoding length of a given distribution. In turn, cryptographers use the more conservative notion called min-entropy, which quantifies unpredictability. In general, there is a large gap between these two measures: the min-entropy of an n-bit string might be only $O(1)$ whereas its Shannon entropy as big as $\Omega(n)$."

Die min-Entropie eines n-bit langen stringes kann konstant sein, wobei gleichzeitig seine Shannon Entropie linear oder größer zu n sein kann.

Von den 2214 bits können nur etwa 128 bits mit nahezu zufällig gleichverteilter Qualität extrahiert werden. Das ist ein Verhältnis von $\frac{128}{2214} \approx 0.0578$ oder anders gesagt: Der Schlüssel hat hier nur die Länge von 5,78% von der Bitlänge des Samples.