Bildunterschriften zu Multimediadatenspeicherung

- **Folie 3**: Verschlüsselung kann direkt auf die Rohdaten, d.h. vor der Kompression (blaues Schloss), im Encoder auf die Zwischendaten während der Kompression (lila Schloss) oder auf die kodierten Daten nach der Kompression (rotes Schloss) angewandt werden.
- **Folie 4**: Bei der selektiven Verschlüsselung (links) wird das gesamte Bild verschlüsselt, aber es sind noch Teile erkennbar (z.B. die Kontur der Person). Bei der Region-of-Interest-Verschlüsselung wird nur ein Teil des Bildes, die so genannte Region of Interest, z.B. ein Gesicht (rechts) verschlüsselt – der Rest des Bildes außerhalb dieser Region bleibt unberührt. Im dargestellten rechten Bild ist eine Kombination aus selektiver und Region-of-Interest-Verschlüsselung abgebildet.
- **Folie 5**: Bei der Verschlüsselung vor der Kompression werden Pixeldaten direkt manipuliert, bevor sie den Encoder erreichen.
- **Folie 6**: Bei der Verschlüsselung während der Kompression werden meist transformierte Daten direkt im Encoder manipuliert, bevor sie als Bitstrom ausgegeben werden.
- **Folie 7**: Bei der Verschlüsselung nach der Kompression werden die Bitstromdaten direkt manipuliert, nachdem sie den Encoder verlassen haben.
- **Folie 8**: Wird ein Makroblock eines kodierten Bildes (links) durch Rauschen ersetzt (rechts, Makroblock links oben unterhalb des Helmes), werden die Daten aller Makroblöcke, die über Intraprädiktion vom geänderten Makroblock abhängen, ebenfalls verändert. Blöcke in der unmittelbaren Umgebung sind dabei durch horizontale bzw. vertikale Intraprädiktion am stärksten betroffen (farbige Streifen in horizontale bzw. vertikale Richtung), während weiter entfernte Blöcke vom sich fortpflanzenden Fehler weniger stark betroffen sind, da sie nicht nur vom geänderten Block, sondern auch von anderen prädizieren.
- **Folie 9**: Wird ein Block einer kodierten Videosequenz (links) in einem einzigen Bild (unten links außen) durch Rauschen ersetzt, pflanzt sich dieser Fehler neben Intraprädiktion im selben Bild auch auf die nachfolgenden Bilder aus. Da bei der Motion Estimation nur die Position und Differenz zum gefundenen Block gespeichert werden, wird der Fehler in alle abhängigen Blöcke weitergetragen. Dabei sind nicht nur Blöcke betroffen, die vom geänderten Block direkt über Motion Estimation abhängen, sondern auch jene, über Motion Estimation von durch örtlichen Drift veränderten Blöcken abhängen. Im Gegensatz zum örtlichen Drift wird zeitlicher Drift meist umso stärker, je weiter ein Frame vom ursprünglichen betroffenen entfernt ist, da sich der Fehler durch mehrfache Motion Compensation addiert. Erst durch einen Szenenwechsel mit I-Blöcken oder ein I-Bild wird die Fehlerausbreitung gestoppt und der zeitliche Drift eliminiert.

- **Folie 12**: Ein Transportstrom wird demuxt, um die senderspezifischen verschlüsselten Schlüssel (S) aus den EMMs an die Smart Card weiterzureichen. Diese entschlüsselt den Schlüssel mit dem benutzerabhängigen, auf der Karte gespeicherten Schlüssel (U) und speichert den entschlüsselten Schlüssel (S) zusammen mit der Information, dass die Karte zur Entschlüsselung des Senders berechtigt ist. Diese Berechtigung kann über andere EMMs wieder entzogen werden, die periodisch im Datenstrom mitgesendet werden und vom Benutzer an die Smart Card weitergereicht werden. Zur Entschlüsselung der Multimediadaten werden die geraden und ungeraden verschlüsselten Schlüssel (O und E) aus den ECMs demuxt und an die Smart Card weitergereicht. Stellt diese fest, dass sie berechtigt ist, entschlüsselt sie die Schlüssel und reicht sie als Control Word über den Demuxer an den Descrambler weiter, der die Multimediadaten damit entschlüsselt.

- **Folie 15**: Im CBC-Modus wird der Klartext des aktuelles Blockes mit dem Schlüsseltext des vorangegangenen Blockes per XOR verknüpft. Der erste Block, der über keinen Vorgänger verfügt, wird mit einem Initialisierungsvektor verknüpft. Für alle Blöcke wird der gleiche Schlüssel verwendet.

- **Folie 16**: Bei der Verschlüsselung von MPEG-TS-Strömen kann entweder der TS-Payload (erste Zeile), der PES-Payload (zweite Zeile) oder das gesamte PES-Paket (dritte Zeile) verschlüsselt werden. Enthält das TS-Paket optionale Headerteile (gelb), bleiben diese unverschlüsselt.

- **Folie 17**: Jede PMT verweist – neben den PIDs für die üblichen Audio-, Video-, und PCR-Daten zusätzlich auf eine senderspezifische PID für ECMs, z.B. ECM 4 (rot) für die PMT zu Sender 4 (rechts oben). Im gesamten Transportstrom werden außerdem für jedes unterstützte Verschlüsselungssystem EMMs mit eigenen PIDs mitgeschickt, die senderunabhängig übertragen werden. Die PID 1 ist für die CAT reserviert, die – analog zur PAT – eine Liste von übertragenen Verschlüsselungssystemen und den jeweils dazugehörigen PIDs speichert.

- **Folie 18**: Auf der Senderseite werden die Audio- und Videosignale durch einen Scrambler verschlüsselt. Die vom Scrambler verwendeten Control Words werden in ECMs gepackt und in den Datenstrom gemuxt, damit sie von der Smart Card beim Empfänger wieder entschlüsselt werden können. Unabhängig davon wird über eine Benutzerverwaltungssoftware der aktuelle Stand berechtigter Smart Cards aktuell gehalten, indem berechtigte Benutzer sowie explizit entzogene Berechtigungen per EMMs signalisiert und in den Datenstrom gemuxt werden.

- **Folie 19**: Die zuvor beschriebene Generierung von EMMs und ECMs bringt einen Datenstrom hervor, der auf der Empfängerseite wieder demuxt werden kann. Die ECMs und EMMs werden an die Smart Card weitergeleitet, die bei entsprechender Berechtigung die verschlüsselten Daten

wieder entschlüsselt. Zusätzlich zur technischen Betrachtungsebene existiert eine logische (dunkelgrau, unten), auf der der Sender (Betreiber) dem Kunden Rechnungen für seine Dienstleistungen stellt und der Kunde diese bezahlt, damit die Berechtigung seiner Smart Card aufrecht bleibt.