

with the associated 500 control words. The method described above in connection with FIG. 8 may be altered to accommodate the 500 ECMs and associated control words.

In some embodiments, the EQAM may have received and cached multiple sets of ECMs (e.g., multiple batches of ECMs). For example, the EQAM may have cached a second set of ECMs prior to losing network connectivity with the ECMG. In such an example, the EQAM may reuse ECMs of the first set of ECMs and ECMs of the second set of ECMs. Particularly, the EQAM may also maintain copies of the second set of ECMs for use with a given set of crypto periods.

In some embodiments, the schedule (generated by the ECMG and sent to the EQAM) may indicate and/or may otherwise provide scheduling information for the reuse of ECMs in the event of a loss of connectivity with the ECMG. For example, the EQAM may schedule and use the copies of the control words for transport encryption and send the copies of the associated ECMs to the downstream client devices based on the schedule.

In some embodiments, the schedule (generated by the ECMG and sent to the EQAM) may indicate and/or may otherwise provide scheduling information for the reuse of ECMs in the event of a loss of connectivity with the ECMG. For example, the EQAM may schedule and use the copy of the last control word (that the EQAM received from the ECMG for the specific service) for transport encryption of the service and send the copy of the associated ECM to the downstream client devices based on the schedule. In such embodiments, no prior indication is given to the EQAM to make copies of the control words and associated ECMs that were used in the previous crypto periods. In the boundary case where a network failure happened and only one control word and associated ECM is left, the EQAM may continue to be use the above schedule.

While the method in FIG. 8 describe a round-robin approach for the reuse of control words and associated ECMs, any number of control word selection preset approaches may be implemented. For example, the EQAM may select the copy of the ECM based on a pseudo-random algorithm. For example, the EQAM may select the copy of the ECM of every third originally scheduled ECM for use with the next crypto period. For example, the EQAM may select the copy of the first ECM for use with next crypto period. The EQAM may then select the copy of the third ECM for use with the following crypto period. In some embodiments, the EQAM may switch from a first approach (e.g., a round robin approach) to a second approach (e.g., the every third ECM approach) after a predetermined period of time and/or number of crypto periods.

In some embodiments, the reuse of control words and associated ECMs might not be in response to a network failure. In such embodiments, controls words and associated ECMs may be reused even if the network connectivity has been maintained (i.e., there has been no loss of network connectivity). For example, the EQAM may reuse control words and associated ECMs when either the EQAM or the ECMG has limited processing capability. For example, the EQAM may reuse control words and associated ECMs when there is network connectivity but that network connectivity is limited either by design or due to network traffic. In such instances, the ECMG by design may supply only a subset of the number of control words and associated ECMs needed as compared to the number required based on the schedule and selected crypto period. For example, in the event the EQAM may use 7,200 control words in total for a two hour movie with a one second crypto period, the ECMG may deliver

only 600 control words and associated ECMs either in one batch or in multiple batches. The EQAM may use each control word and associated ECM 12 times, or reuse each control word eleven additional times on average based on a selected reuse method.

The same methodology is used for supporting multiple simultaneous services. In other words, for each service supported by the EQAM, the EQAM may receive from the ECMG only a subset of control words and associated ECMs typically used to support the service. The EQAM may reuse the subset of control words and associated ECMs for that specific service.

In some embodiments, the EQAM may request and receive a common set of control words and associated ECMs either in one batch or multiple batches. The EQAM may reuse the common set of control words and associated ECMs for each service supported by the EQAM. In some embodiments, the EQAM may use the common set of control words and associated ECMs only during a short preset interval at the beginning of each service. For example, when the EQAM detects a service and before establishing an encryption session with an ECMG, the EQAM may, for a specified time period, use the common set of control words to encrypt the service. After the specified time period, the EQAM may switch over to using a set of control words and associated ECMs specific to the service received from the ECMG. The EQAM may continuously receive and cache new sets of control words and associated ECMs until a full supply of control words and associated ECMs have been received by the EQAM to support the service. Alternatively, in some embodiments, the EQAM may receive only a subset of the control words and associated ECMs used to support the service and may reuse those control words and associated ECMs to support the service until the service is complete.

In some embodiments, multiple successive ECMs received in the transport stream by downstream client devices may be used to derive a control word. In other words, the downstream client devices may derive a first control word based collectively on both a first ECM and a second successive ECM received in the transport stream. For example, the downstream client device may obtain a first portion of information used to derive the first control word from the first ECM and may obtain a second portion of information used to derive the first control word from the second ECM. In some embodiments, in order for the downstream client device to obtain a control word, the information to derive the control word may be divided among more than two successive ECMs.

As illustrated above, various aspects of the disclosure relate to providing control word management functionalities. In other embodiments, however, the concepts discussed herein can be implemented in any other type of computing device (e.g., a desktop computer, a server, a console, a set-top box, etc.). Thus, although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are described as some example implementations of the following claims.

What is claimed is:

1. A method comprising:

caching concurrently, by a computing device, a first set of control words and a first set of entitlement control messages (ECMs) associated with the first set of control words;