CT 10G-EPON Systems Churning requirement

(Note: This segment will be inserted into Chapter 11 of <CTC EPON technical Specification V2.1> after being finalized, behind the requirements for 1G Churning. And for the other same contents, please refer to Chapter 11.1.1 to 11.1.4 of the V2.1 spec.)

1 Churning and Dechurning functions for 10G-EPON System

10G-EPON System should implement the churning algorithm per LLID, and each LLID should have its own independent encryption key. The churning should start from destination MAC address of the Ethernet frame, and end at FCS field. And the system should complete both MPCP Discovery and OAM Discovery before exchanging the encryption key. And then, after the key exchanging, all the downlink data, MAC Control and OAM frames of that ONU should be churned. Please refer to below Figure1 for the implementation of 10G EPON churning.

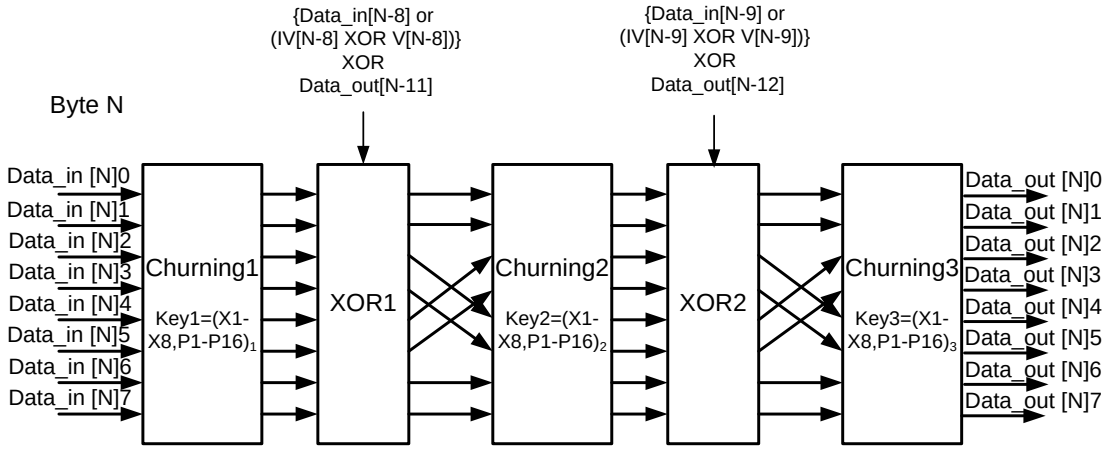

Figure1 10G-EPON churning solution

As above figure, the churning system shall support 3 cascade churning engines, and each shall carry out the specified single churning. And the churning used every time shall be absolutely different. And the 24 bits encryption key shall be $(X1\text{-}X8, P1\text{-}P16)_1$ for the 1st engine, and $(X1\text{-}X8, P1\text{-}P16)_2$ for the 2nd one, and $(X1\text{-}X8, P1\text{-}P16)_3$ for the 3rd one. And the churning key shall be the result from the Exclusive OR (XOR) operation between three 3-bytes random data and the three 3-bytes data extracted from the ONU upstream.

The output from the 1st engine (Churning1) shall XOR with two 8-bits vectors bit by bit: the first vector shall be the input bytes Data_in[N-8] before the 8th byte. When encryption data are the first 8 bytes in one frame, it should be denoted as IV[N-8] XOR V[N-8]. And the vector IV[N-8] of each LLID should relate with the encryption key of that LLID, as below:

IV[-9] is the $(X1 \sim X8)_1$ of Key1

IV[-8]is the $(P1 \sim P8)_1$ of Key1

IV[-7] is the $(P9 \sim P16)_1$ of Key1

IV[-6] is the $(X1 \sim X8)_2$ of Key2

IV[-5] is the $(P1 \sim P8)_2$ of Key2

IV[-4] is the $(P9 \sim P16)_2$ of Key2

IV[-3] is the $(X1 \sim X8)_3$ of Key3

IV[-2] is the $(P1 \sim P8)_3$ of Key3

IV[-1] is the $(P9 \sim P16)_3$ of Key3

The vector V[-9] ~ V[-1] of each LLID should derive from the last 4 bytes (M_1, M_2, M_3 and M_4) of the previous frame of that LLID, i.e. M_1 is the last byte of that encryption frame, and M_2, M_3 and M_4 are corresponding to the No.2, No.3 and No.4 byte from the end. Thus the vector V[-9] ~ V[-1] of each LLID should be as below:

$V[-1] = M_1$

$V[-2] = M_2$

$V[-3] = M_3$

$V[-4] = M_4$

$V[-5] = M_1$

$V[-6] = M_2$

$V[-7] = M_3$

$V[-8] = M_4$

$V[-9] = M_1$

When OLT encrypts the 1st frame of each LLID, the vector V[N-8] should be all “0”. And OLT should maintain the M_i and encryption key for every LLID in the process. And when one ONU disconnects, and then reconnects to the OLT, the vector V[N-8] should be all “0” for the 1st frame.

The second vector shall be the output Data_out[N-11] before the 11th byte after the churning. And for the first 9 bytes of each frame, “0” should be used to replace Data_out[N-11], i.e. Data_out [-11] to Data_out [-3] are all “0”. Also, M_2 should be used to replace Data_out[-2], and M_3 for Data_out[-1].

The input of Churning2 shall come from the output of XOR1 through bit shift, and the shifting rule as below: swap bit2 and 4, swap bit3 and 5, and keep the positions of bit0, 1, 6 and 7. As shown in Figure1.

Also, the output from the 2nd engine (Churning2) shall XOR with two vectors bit by bit: the first vector shall be the input Data_in [N-9] before the 9th byte. When encryption data are the first 9 bytes in one frame, it should be denoted as IV[N-9] XOR V[N-9]. And please refer to above description to get the values of IV[N-9] and V[N-9].

The second vector shall be the output Data_out[N-12] before the 12th byte after the churning. And for the first 10 bytes of each frame, “0” should be used to replace Data_out[N-12], i.e. Data_out [-12] to Data_out [-3] are all “0”. Also, M_2 should be used to replace Data_out[-2], and M_3 for Data_out[-1].

Also, the input of Churning3 shall come from the output of XOR2 through bit shift, and the shifting rule is same as above.

In the 10G EPON churning solution, the relevance between the input and output of the 1st 15 bytes in each frame is shown as Figure2.

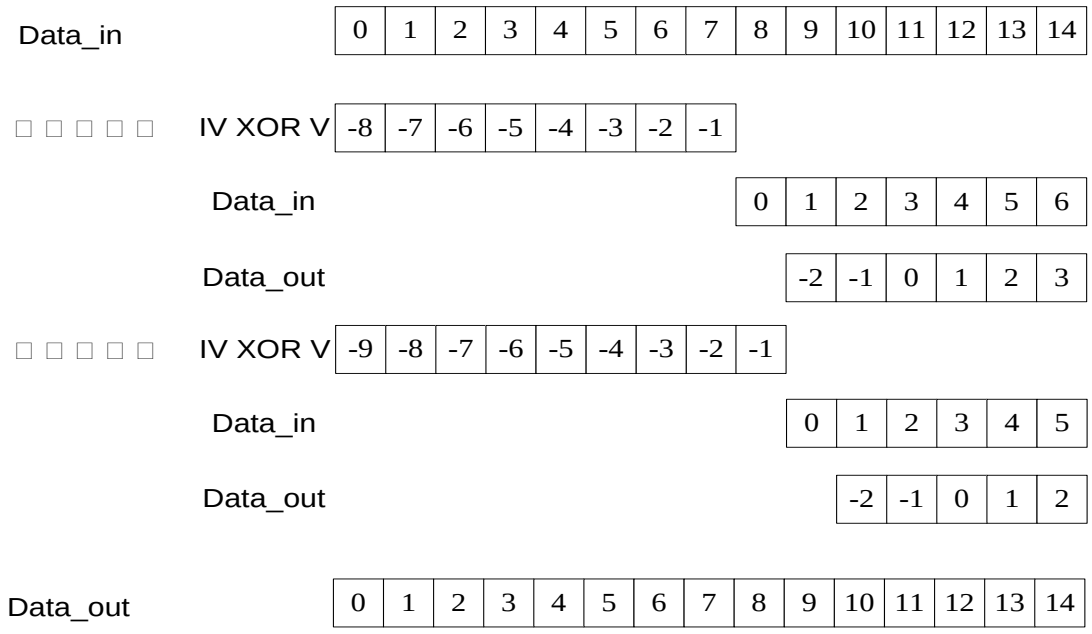

Figure2 The relevance between the input and output of the 1st 15 bytes in each frame

The dechurning of 10G EPON is the simple mirror of churning function，and the implementation is shown as Figure3.

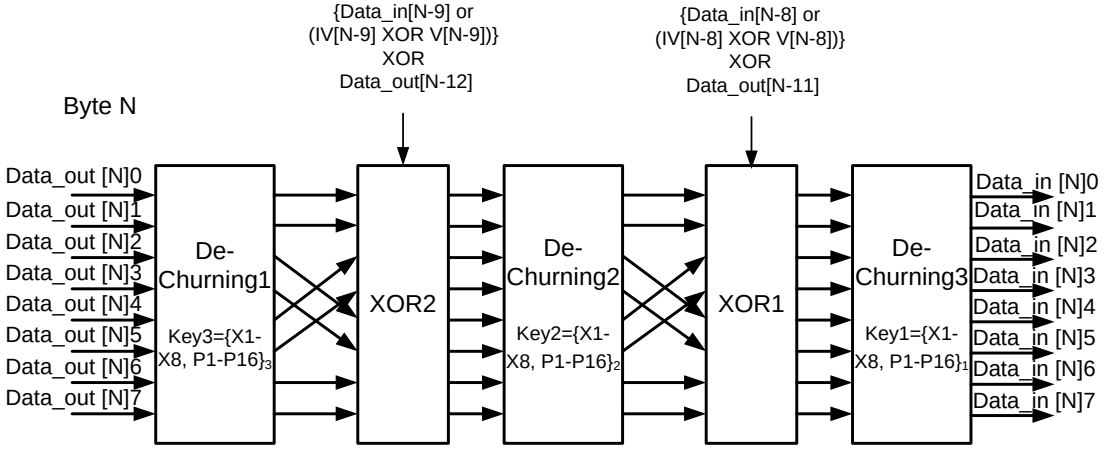

Figure 3 10G-EPON Dechurning Solution

Please refer to Chapter 11.1.2 of CTC V2.1 spec for the process to update and synchronize the churning key of 10G EPON solution. And the update period of the key should be configurable, and the default value should be 10s.

10G-EPON system shall use two kinds of messages to exchange the keys, which are new key requesting frame (new_key_request) and new key notification frame (new_churning_key). And please refer to Chapter 11.1.4 of CTC V2.1 spec for the format of new key requesting frame.

The definition of new key notification frame is shown as Figure4. Churning_code="0x01". And the lowest bit of New_Key_Index byte shall be used to denote the sequence ID of the delivery key ("0" or "1"), and the other bits are all "0". And the churning key field (3 bytes) includes the new key that shall be replaced in Churning1, and the delivery sequence should be [(MSB)X1,X2,…,X8,P1,P2,…,P16(LSB)]. And then, the next two churning Key fields (both 3 bytes) shall include the new replaced keys for Churning2 and Churning3 separately, and the delivery sequence shall be [(MSB)X1,X2,…,X8,P1,P2,…,P16(LSB)]. And then it is the PAD.

6	Destination Address=01-80-c2-00-00-02
6	Source Address
2	Length/Type=0x8809[Slow Protocol]
1	Subtype=0x03[OAM]
2	Flags
1	Code=0xFE
3	OUI
1	Ext. Opcode=0x09
1	Churning code=0x01(new_churning_key)
1	New_Key_Index
3	Churning Key1(X1, ..., X8, P1,...,P16)$_1$
3	Churning Key2(X1, ..., X8, P1,...,P16)$_2$
3	Churning Key3(X1, ..., X8, P1,...,P16)$_3$
27	Pad
4	FCS

Figure4 frame format of new_churning_key message