CableWorld

Digital television systems and infocommunication devices

A HUNGARIAN LTD COMPANY FOR DEVELOPING AND MANUFACTURING DIGITAL TELEVISION SYSTEMS

H-1116 Budapest, Kondorfa u. 6/B, Hungary Tel.: +36 1 204 7815 Fax: +36 1 204 7839 www.cableworld.eu cableworld@cableworld.hu

CW-4000

CW-4861, CW-4861 IP, CW-4861 IP Q
TOTALCRYPT PAY TV SCRAMBLER
TCM-061 TOTALCRYPT DESCRAMBLER MODULE

DVB Digital Video Broadcasting

Pay TV allows access to the programs for those only, having paid the due fees. Already in the analogue technology there was a large demand for pay TV systems, but for implementing such systems the digital technology is much more suitable. With introducing digital television technology a sudden rise in paid services is to be expected.

The TOTALCRYPT system developed by CableWorld solves the descrambling function at the receiving side by using the standard Common Interface (CI), thus any set-top box or digital TV set equipped with CI can be used for reception. The gist of the TOTALCRYPT system is converting the receivers (set-top boxes or digital TV sets) into addressable descramblers by inserting TOTALCRYPT descrambler modules in their CI slots. Each TOTALCRYPT descrambler module is equipped with an individual address, and the scrambler in the headend controls the descrambler modules by special data embedded in the transport stream. The descrambler modules receive from the transport stream both the descrambling algorithms and the signals authorizing the subscribed programs, thus both enabling and disabling the reception can be controlled in an easy way.

The CW-4861 TOTALCRYPT PAY TV SCRAMBLER is used in the headend for scrambling the signal going to the QAM modulator. The scrambler is not integrated into the system, thus it can be included or excluded at any time. The scrambler is not bound to CableWorld device environment; it can be used in the headend of any manufacturer. The scrambler does not change the data rate; the space for embedding the control data has to be provided in form of null packets. The quantity of the necessary control data depends on the number of subscribers and the required recovery time of the receivers, and it can be programmed in a wide range.

The TOTALCRYPT descrambler module is DVB and CI compatible however the scrambling is made not according to the standard but in a special system developed by CableWorld, that makes hacking even more difficult. The descrambler modules receive from the transport stream continuous individual control by their identification numbers. The scrambling system provides scrambling up to 64 elementary streams within the transport stream and their individual authorizations.

Main features:

- DVB and CI compatible but not standard scrambling
- Scrambling and individual authorization of up to 64 elementary streams within the transport stream
- Changing of the scrambler algorithm through the transport stream by software
- Maximal number of subscribers 500,000
- Receiver recovery time 0.2 to 2 seconds
- Data update and subscriber/program authorization during operation without disturbing the operation
- Data loading and control with external PC through CW-Net, operation without computer
- 19” × 1 HU frame, 3.3 V supply voltage, low power consumption, continuous service

CW-4861, CW-4861 IP, CW-4861 IP Q TOTALCRYPT PAY TV SCRAMBLER
TCM-061 TOTALCRYPT PAY TV DESCRAMBLER MODULE

CableWorld's product designer team studied in depth the Common Interface standardized for the DVB system and the associated Conditional Access Module (CAM) implementations, identified their weak points, drew a lesson from these and developed an own scrambling system, the **TOTALCRYPT**, *which provides improved security compared with the known widely used systems.*

The TotalCrypt system consists of two main parts: the Pay TV Scrambler in the transmitting side and the TotalCrypt descrambler modules inserted in the subscribers' set-top boxes or digital TV sets at the receiving side. The Pay TV Scrambler scrambles the data of the data stream lead to its input so that receivers (set-top boxes or digital TV sets) without descrambler modules cannot reproduce the picture and sound data streams. The TotalCrypt descrambler modules are equipped with individual identifiers, and they receive the control from the transport stream through the Common Interface (CI) connection. The TotalCrypt descrambler module receives the command about which data streams have to be descrambled and by which algorithm, so that the subscriber can receive the subscribed programs.

The TotalCrypt system fits the DVB system, however the applied scrambling system and the structure of the descrambler module differ from the known systems using smart cards. Deviating from the standard considerably raised the security of the system and greatly decreased the number of those interested in hacking the system because the system deviates from the ones used worldwide. The system permits choosing an own scrambling algorithm for a particular town or cable TV provider so that the TotalCrypt descrambler module transferred to another town or system cannot be used.

The favourable selling price of the TotalCrypt system permits its use even in small systems as in hotels and institutions and moreover, after having purchased the scrambler and the descrambler modules no more fees (e.g. royalties) have to be paid; the user disposes free of the product.

The CW-4861 Pay TV Scrambler scrambles the transport stream according to the pre-programmed algorithms and it replaces the null packets with the data streams controlling the TotalCrypt descrambler modules in the receivers. The amount of data in the controlling data stream is proportional with the number of subscribers and the required recovery time of the system (the time the set-top box or TV set needs for starting to reproduce the descrambled picture after having tuned to the channel). The amount of data necessary for the controlling data stream is not more than 10 % of the data stream even at large systems beyond 100,000 subscribers. The space for the controlling data stream has to be assured in form of null packets in the course of remultiplexing.

The PID values of the data streams to be scrambled, the scrambling algorithm and the subscriber database have to be loaded into the Pay TV Scrambler in form of a PC generated program. The scrambler is equipped with two memory areas; at the same time one of them is in operation, the other can be programmed and refreshed with data. The actual working memory unit is shown with a front panel LED.

The technique of scrambling and the used procedures are not public. The applied technique permits beyond scrambling the picture, sound and teletext data streams also scrambling any data stream complying with the requirements of the DVB system.

The TotalCrypt system permits the subscriber to use always the most up-to date and much liked set-top box or digital TV set; there is one requirement only, it has to be equipped with Common Interface. The TotalCrypt descrambler module is an intelligent sealed unit, which needs no card or other complementary accessory, it is recognised by its individual identification number, and it receives the control data from the transport stream when put in the CI slot. The TotalCrypt descrambler module is shown on the photo in Figure 1.

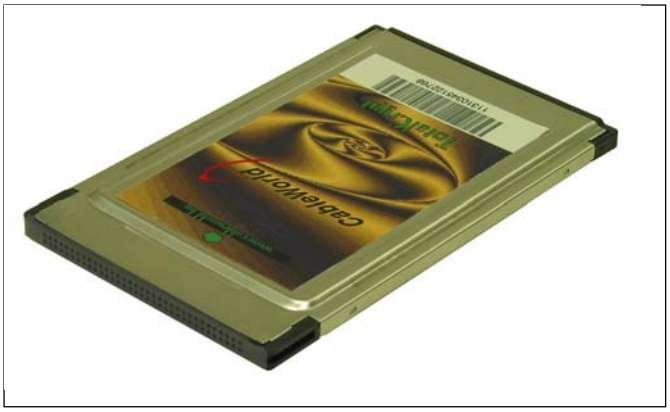

Fig. 1
Photo of the TotalCrypt Descrambler Module used in the CI slot

The Pay TV Scrambler's subscriber handling program is composed of a simple database, thus it can easily be fitted to any invoicing program. The database has to be generated by the invoicing program and submitted in file form to the SW-4861 software, which generates the program to be loaded and performs the loading.

The CW-4861 Pay TV Scrambler is available in three versions:

CW-4861	*ASI input, ASI output*
CW-4861 IP	*IP input, IP output*
CW-4861 IP Q	*4 independent Pay TV Scramblers with IP input and IP output each*

Technical data

Subscriber number	1 to 500,000
Recovery time	0.2 to 2 s + recovery time of the MPEG decoder typically less than 1 sec
Device control and programming	through the CW-Net system
TS input and TS output	
CW-4861	ASI, according to TM 1449 Rec. 1
CW-4861 IP, CW-4861 IP Q	UDP/IP
Data rate	max. 56 Mbps
General characteristics	
CW-4861	see at the CW-48xx series devices
CW-4861 IP, CW-4861 IP Q	see at the CW-49xx series devices

General data

Service period	continuous
Power requirement	90 ~ 264 V AC, 47 ~ 440 Hz
Power consumption	max. 20 VA
Physical dimensions	19" × 1 HU
W × H × D	486 × 43.6 × 473 mm
Mass	max. 3.5 kg