Rambus CRYPTOGRAPHY RESEARCH

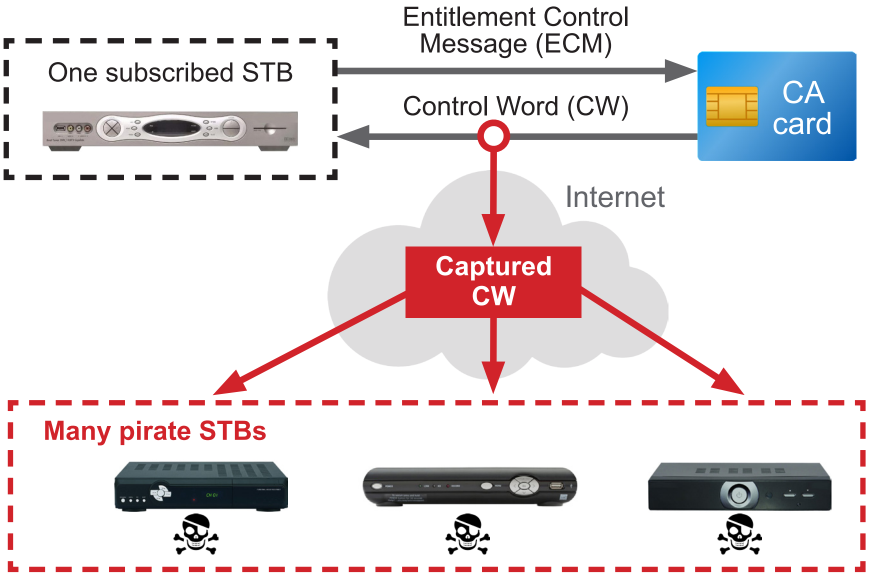
Protecting Pay TV with CryptoFirewall™ Security Cores

Robust security against control word sharing

The advancing capabilities of attackers are driving a new phase in Pay TV signal piracy: pairing keys and control words can be extracted from set-top box (STB) chipsets. These attacks defeat the current defenses against control word sharing and provide access to plaintext control words, enabling illegal access to premium content by non-subscribers. Solving the problem requires improved security in device chipsets, or System-on-Chips (SoCs), including strong hardware security cores.

BACKGROUND

Control word sharing originated about 25 years ago. Pirates have long known that they could obtain control words from the open interface between the STBs and pay TV smart cards. The challenge for pirates was to redistribute captured control words in real-time. Initially, this was done using computer modems, but the Internet enables today's large-scale control word sharing problem.



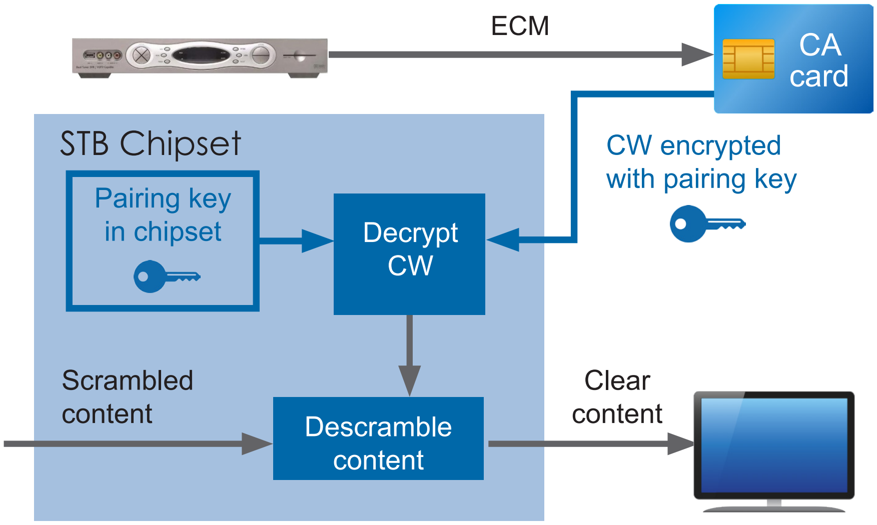
Control word sharing

CryptoFirewall Core Highlights

- Secures video decryption with a separate hardware core within the STB SoC
- Delivers strong, cost-effective security
- Maintains security even if the software and other cryptographic logic is compromised
- Provides complete key management with dedicated high-security root key storage
- Meets operator and studio security requirements
- Supports all main distribution formats—satellite, cable, IPTV and OTT
- Integrates with leading CAS and DRM system providers
- Available now from leading SoC manufacturers (see **cryptography.com/paytv**)

Protecting Pay TV with **CryptoFirewall** Security Cores

To prevent pirates from having direct access to control words, many conditional access systems use a pairing key to encrypt control words in smart cards before transmission to the STB. The STB chipset also knows the pairing key, and uses it to decrypt each control word before using it to descramble the content. For these CA systems, security against control word sharing depends on keeping the pairing key secure.

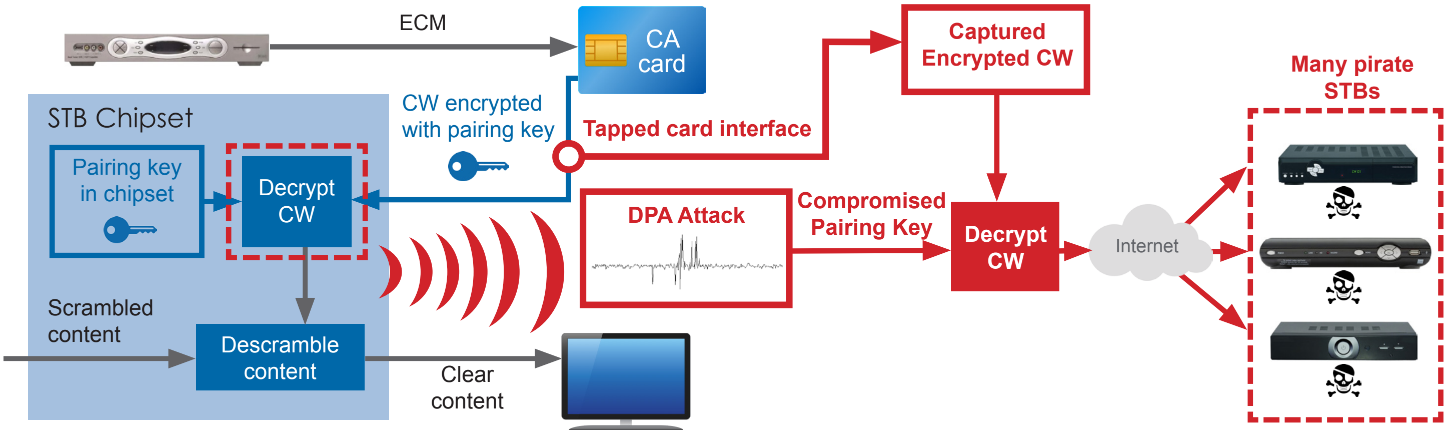


Traditional control word encryption with a pairing key

UNDERSTANDING THE THREAT

The hardware security level of today's STB chipsets varies greatly. While invasively extracting keys from a large SoC is physically difficult, modern attacks are non-invasive and inexpensive. During normal operation, chips leak information through variations in power consumption, timing, and electromagnetic emissions. Attackers can measure these during encryption and decryption, narrow in on the security functions, and apply techniques like differential power analysis (DPA) to obtain secret keys. For example, a simple coil of wire on top of an operating chip can serve as the antenna for a digital radio whose output is analyzed by a computer to find the secret key. Unless chip's security core is specifically hardened, the process is cheap and easy to repeat.

This type of vulnerability is of particular concern for pairing keys, since compromise of a single pairing key can give attackers an ongoing source of control words that can enable many pirate viewers.



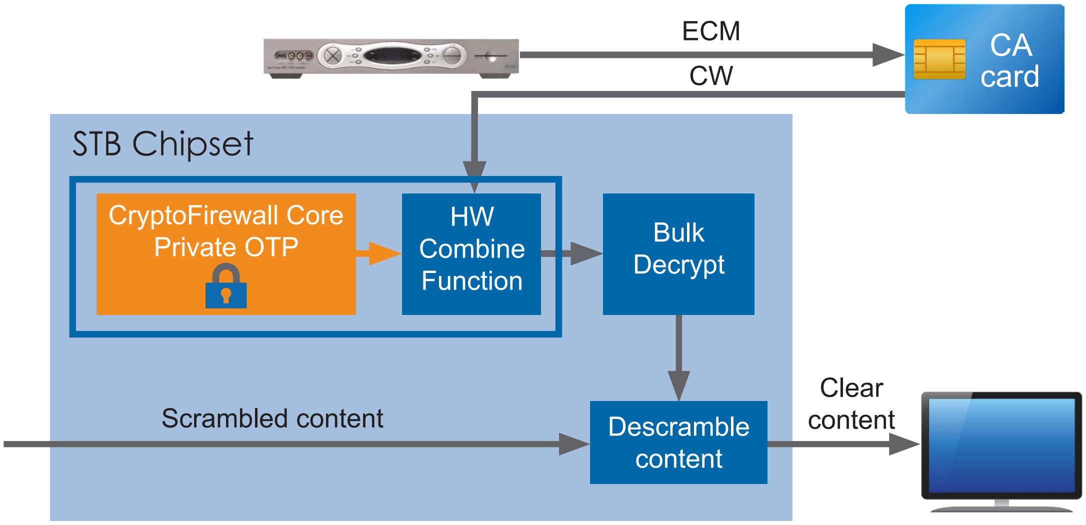
Control word sharing using a pairing key extracted through DPA

Protecting Pay TV with **CryptoFirewall** Security Cores

SOLVING THE PROBLEM

Because pirates can select among the types of STBs in use by the operator, the risk of pairing key extraction (as well as other attacks) reflects the weakest box. As a result, operators' security strategies need to focus on providing a uniformly high level of security across STB models. Operators should give a high priority to deploying STBs with strong hardware security, both in replacements as well as new deployments. Security upgrade strategies should be coordinated with new feature deployments (HD, 4K, 3D, etc.), to ensure that new, high-value features can use the better security. Starting the process sooner saves money in the long term, since the total number of legacy boxes that need to be replaced will decrease over time. The ultimate objective is a system that is future-proofed and hardened against control word sharing.

Available in STB chipsets from leading SoC vendors today, the CryptoFirewall core is specifically designed to deny pirates a source of control words. The CryptoFirewall core provides a separate hardware core within the SoC that manages keys independently from software and maintains security even if the remainder of the chipset is compromised.



Secure content decryption with CryptoFirewall core

The CryptoFirewall core also offers complete key management, with a private bus for key delivery and extra logic for specific conditional access and DRM systems. Unlike traditional pairing key-based approaches, the CryptoFirewall core participates in the forming of the control word, effectively eliminating the vulnerability of control word interception from the smart card interface or software API and removing the need for pairing keys. By providing STB chipsets with uniformly high level of security, CryptoFirewall technology addresses operator needs for broad availability of a cost-effective security solution.

cryptography.com/paytv