HARRIS CUSTOMIZABLE CRYPTOGRAPHIC ARCHITECTURE

Michael Kurdziel
Harris Corp., RF Communications Div.
Rochester, New York 14610

Robert Clements
Harris Corp., RF Communications Div.
Rochester, New York 14610

ABSTRACT

The need for protection of information has dramatically increased in recent years as equipment that can be used for interception of sensitive data has become more readily available. The need to secure non-DOD sensitive data in both the government and private sectors has required the development of very robust, high grade information security solutions that can be tailored to meet specific security needs. Harris has made a long term R & D investment into developing a robust information security architecture, that can be used in applications where Type 1 security is not required. The architecture is based on Harris’s proprietary cryptographic algorithm technology. It supports Sensitive But Unclassified (SBU) requirements and international markets requiring customer unique encryption. It is an ideal solution for the protection of defense and other national level interests, and provides state-of-the-art protection for both domestic and international users over any of the media used in modern communications. The first embedment of this architecture is the CITADEL™ integrated circuit. CITADEL™ is Harris’ prime export encryption solution for all of its new products requiring security, such as the FALCON II HF, VHF, and Multi-band radio platforms. This paper presents an overview of the Harris Customizable Cryptographic Architecture and discusses various applications in which the CITADEL™ can be used.

1. INTRODUCTION

Information Security has become a major concern for the export, non-US DOD, and US SBU communities. International customers desire information security (INFOSEC) solutions that offer features traditionally available in Type 1 INFOSEC applications. These are introduced in the following paragraphs.

1.1 Security Autonomy

Unlike the commercial INFOSEC community, domestic and foreign DOD and Government users require Security Autonomy. That is, they require that their INFOSEC algorithms be unique and not publicly disclosed. Many countries even have a need for several unique algorithms. This allows network separation to be guaranteed without relying on an elaborate key management plan.

1.2 High Cryptographic Strength

In the past, the availability of intercept and decode technology was limited. For this reason, the tactical environment often allowed the use of a wider range of INFOSEC solutions. The dissemination of technology makes prediction of an adversary’s cryptanalysis capability increasingly difficult. Users now require that an INFOSEC solution be secure against all known cryptanalytic techniques.

Many providers of INFOSEC solutions have focused on specifications such as key length to demonstrate the quality of their products. In reality, key length is only one component of a high quality INFOSEC solution. Few will dispute that a very strong cryptographic algorithm will be of little value if it uses a 20 bit key. However, it is also true that a weak algorithm which supports a 128 bit key is also of limited utility. Sophisticated customers will not accept key length as verification of an algorithm’s strength.

1.3 Functional Requirements

In addition to the previously described requirements, it is desirable for an INFOSEC architecture to include the features discussed below. These features will allow the architecture to support a wide range of applications.

A cryptographic algorithm is only part of a core INFOSEC architecture. An additional layer of the architecture controls the feedback structure for the algorithm and performs other simple mathematical operations. The algorithm defines the cryptographic strength of the architecture, but the traffic mode defines the ability of an architecture to recover from channel errors. Several traffic mode options should be available to allow the architecture to be configured for specific channel conditions. These modes allow the architecture to recover in the presence of both toggled bit errors and bit synchronization (dropped or added bits) errors.

It is desirable to include a separate mode to be used only for traffic key wrapping (encryption) and unwrapping (decryption). A separate mode guarantees functional separation between traffic functions and key management functions. This will eliminate the possibility of logical paths existing between key I/O and traffic I/O in embedments of the architecture.

Another desirable feature is that the architecture have a scalable key length. This is particularly important in the application of the architecture to exportable embedments. By using an architecture with a scalable key length, new embedments will be able to accommodate changes in export policy without drastic changes to the INFOSEC core. This will allow compatibility with legacy equipment to be maintained.
It is equally desirable to allow key length to be scaled in response to advances in cryptanalysis tools and technology. Lastly, the architecture's interface should meet the requirements of a wide range of applications. It should support both encryption and decryption in addition to serial and parallel traffic processing. Logical separation between plaintext, ciphertext and key spaces should be provided. Finally, the architecture should be scalable from low complexity to full featured applications.

2. ARCHITECTURE DESCRIPTION

2.1 Block Diagram

Harris Secure Products group has developed an INFOSEC architecture that meets all the requirements discussed in the previous section. A block diagram of the architecture is shown in Figure 1. The basis of the architecture is a Harris proprietary cryptographic algorithm (patent pending) [1]. This algorithm has been evaluated and verified by an independent third party for cryptographic strength. Detailed discussion of its design is beyond the scope of this paper. However, the following high level description is provided.

It is observed that the algorithm is secure, by design, against the benchmark "Differential" and "Linear" Cryptanalysis techniques. It is a 64 bit block cipher. The algorithm is not iterative and can not be segmented into "rounds" for analysis. It consists of a series of operations or sub-blocks having at least 64 bit I/O spaces. Many of these can not be segmented into lower level operations. The algorithm consists of non-linear mapping functions, mixed-mode arithmetic, a non-linear mixing function and a non-invertable transform. These operations prevent differential characteristics or a significantly biased linear approximation from existing between the algorithm's input, output and key spaces. The interested reader is directed to [2] for an excellent tutorial on cryptanalysis.

2.1.1 Security Autonomy

The requirement for security autonomy was addressed in two ways. These are described in the following paragraphs.

2.1.1.1 Full Architecture Customization

To allow full customization of the architecture, the design specification of the Harris algorithm was modified, (refer to Figure 1). This allows Block 3 and several functions in Block 9 to be uniquely specified.

Block 3 is a customizable Substitution/Expansion block providing a custom non-linear operation with inputs W2 and Zj[24:31] and output W1. This powerful feature allows custom variants of the architecture to be designed and provided. The structure of Block 3 is not arbitrary and must meet the requirements of secure cipher design [2]. Custom Substitution/Expansion unit designs are disclosed only to the intended end user.

Block 9 is the key scheduling unit. It is composed of sub-blocks' f, g, h, shift register R128 and a mod 2 add logic gate. The key scheduling unit processes "Key Variable" Zs to produce variables Zq and Zs. These variables are used during encryption and decryption. Zs which is a deterministic function, h, of "Key Variable" Zs is input to R128. R128 is shifted to the right one bit at a time until its contents have been completely re-circulated. With each shift, the least significant bit in R128 is mod 2 added to the output of f. The result is moved into the most significant bit position of R128. When the contents of R128 have been completely processed, it is output as variable Zq. Zq is input to function g to produce variable Zs.

Function f is a custom non-linear function. It maps at least 6 one bit inputs to a single one bit output. Each of the inputs to f is a "tap" connected to an individual bit position in R128. The tap locations can be arbitrarily chosen with the following constraint. No tap can be connected to either the least significant or to the most significant bit positions on R128. Custom f block designs are disclosed only to the intended end user. Function g performs a bit-wise mod 2 add without carry of the higher and lower order halves of Zq to produce Zs. Function h performs a bit-wise mod 2 add without carry of variable Zs and custom bit pattern of equal length to produce variable Zs. The value of the custom bit pattern is disclosed only to the intended end user.

2.1.1.2 Architecture Field Modification

To allow the structure of the architecture to be modified in the field, blocks 1, 2 and 4 were added and the operation in Block 5 was slightly modified.

The Block 1 operation is a modulo 2 addition of primary traffic input X1 with variable Z1 resulting in output W1.

Blocks 2 and 4 are "nibble swapping" blocks. These blocks allow the structure of the algorithm to be changed based on an externally applied input, Z1. For Block 2, W1 is segmented into 8 pairs of 4 bit values called nibbles. Bits Z1[0:7] determine the re-ordering of each pair of nibbles from W1 into W2. For example, when the value of bit "0" in Z1 is equal to a binary "1" then the order of the nibble pair "0" will be transposed. Likewise, if bit "0" is equal to binary "0" then the order is left unchanged. The order of each pair will be determined by the value of the corresponding bit in Z1. The value of bit 0 will affect nibble pair 0, the value of bit 1 will affect nibble pair 1 continuing through to bit 7 which will affect nibble pair 7. The re-ordered output is designated as W2 in Figure 1.

Block 4 is another "Nibble Swap" operation. Here, W3 is segmented into 16 pairs of nibbles. Z1[8:23], determines the re-ordering of each pair of nibbles from W3 into W4. This is done in a slightly different manner than in Block 2. For example, when the value of bit "8" in Z1 is equal to a binary "0" then the first nibble in the pair will be written to the first position in the high order segment of W4 and the second nibble will be written to first position in the low order segment of W4. When the value of bit "8" in Z1 is equal to a binary "1"
then the two nibbles will be transposed before being written to \( W_4 \). As with Block 2, the re-ordering of each nibble pair will be determined by the corresponding bit in \( Z_1 \).

Block 5 is a modular addition operation. \( W_4 \) and \( Z_7 \) are operands of this stage. \( W_4 \) is the output of this block and \( Z_7 \) is an output from the Key Scheduler. The modulus, \( q \), of the operation is determined using \( Z_1[32:63] \) by the following relation:

\[
q = 2^{128} - Z_1[32:63] \tag{1}
\]

2.1.2 High Cryptographic Strength

As previously stated, users require that an INFOSEC solution be secure against all known cryptanalytic techniques. The Harris Customizable Cryptographic Architecture is based on independently verified cryptographic algorithm technology. It uses a "secure by design" philosophy that insures strength against benchmark cryptanalytic techniques.

Architecture variants provided through the methods described in Section 2.1.1.1 will be re-verified to insure strength against the benchmark cryptanalysis techniques. In addition, modification of the architecture’s structure via the method described in Section 2.1.1.2 can not result in degenerate modes of operation [1].
2.1.3 Functional Requirements

To meet the functional requirements outlined in Section 1.3, the architecture can be configured into several traffic modes. Figure 2 represents the next layer of architecture developed for this purpose. Different modes provide the ability to respond to various channel conditions.

The mode configuration layer provides registration and multiplexing around the block cipher. This structure can be controlled to operate the algorithm in some common cryptographic modes. Z1 and Z2 represent the same variables as in Figure 1 where Z1 controls the field customization and Z2 is the key variable. The feedback depicted in this representation can operate with 64 bits, 1 bit or no feedback.

Supporting multiple cryptographic modes provides the flexibility to account for different channel conditions and communication applications. In block Cipher Feedback (CFB) mode, a toggled bit channel error will result in corruption of one bit in the current decrypted block and corruption of all of the next block. This standard mode is intended primarily for error free channels or in applications requiring “spoof protection”. Counter mode does not use feedback. A toggled
bit channel error will result in corruption of only one bit during decryption. In other words, this mode has only one bit of error extension. This mode is intended for toggled error prone channels. The architecture in Figure 2 can also be configured in Self-Syncing CFB mode. This mode has the same error extension as standard CFB mode in the presence of toggled bit errors. However, this mode allows the architecture to recover from added or dropped bit channel errors. Here, a specific pattern in the ciphertext will cause the encrypter and the decrypter to resynchronize their block boundaries and re-establish communication. This mode is intended for the synchronization of error prone channels (fades, etc.) or for applications requiring a “late entry” capability.

In addition, this architecture can be configured in Codebook mode. This mode encrypts a 128 bit input under a given key and produces a 128 bit output. This serves as a separate mode for traffic key encryption and black key management applications. This mode accounts for the two 64 bit multiplexers following the Block Cipher in Figure 2.

Figures 1 and 2 illustrate the architecture’s compliance with the remaining requirements. The architecture provides logical separation between plaintext, ciphertext and key spaces. It can be configured for encryption or decryption and, with appropriate I/O buffering, can support serial and parallel traffic processing. The architecture can use keys of various lengths by setting unused bits in R128 to default initial values. Finally, the architecture can support low complexity applications. By setting the parameters and functions described in Sections 2.1.1.1 and 2.1.1.2 to default values, the interface and the operation of the architecture is simplified.

3. EMBEDMENTS
3.1 Hardware

The CITADEL™ Cryptographic device is an application of the Harris Customizable Cryptographic Architecture, implemented in a digital ASIC. This device provides a cryptographic data processing function for many different types of telecommunications systems. The interface structure, command set and operating modes provide efficient command and data processing while promoting a flexible and secure integration effort. In addition to parallel bus control of the chip, a Stand Alone mode is available for applications requiring low power and minimum chip count (e.g., handheld communications devices). The device is capable of 5Mbps data rate. This implementation incorporates all the features of the architecture. It provides high quality security, it allows unique architecture variants to be provided and it allows further structural modification in the field.

CITADEL™ has a parallel interface that can be used for traffic, commands and command data. The interface includes a command set appropriate for black key management, red key management, key generation, cryptographic synchronization and channel multiplexing. Black traffic, red traffic and keys can be handled using the parallel interface or by separate serial interfaces. The device can process serial or parallel traffic and maintain red/black separation within traffic and key spaces. This enables seamless integration with host equipment designed for Type 1 cryptography.

The command set was designed to implement black or red key management. Keys can be generated, updated, zeroized and wrapped off-chip using a loaded, generated or module unique key for storage. This supports the design of basic to complex key management plans. Commands for the manipulation of cryptographic synchronization are available to implement full duplex transmissions, multiple channels or context switching. Independent synchronization can also be achieved through commands that support Time of Day (TOD) or Over the Air Rekey (OTAR). In addition, command sequences can be used to calculate cryptographic functions such as Message Authentication Codes (MAC) and hashing of files.

The architecture supports the four cryptographic modes described in Section 2.1.3. Cipher Feedback (CFB), Counter and Self Synchronization modes allow the architecture to accommodate channel conditions present in a variety of telecommunication systems. The system designer can switch between modes to minimize error extension or to provide self synchronization under poor channel conditions. Late entry can also be provided using the Self Synchronizing CFB mode. A separate Codebook mode is used for all key encryption and decryption operations.

4. CONCLUSION

This paper describes the Harris Customizable Cryptographic Architecture. This architecture meets the INFOSEC requirements for domestic, international and government applications. The architecture provides the user with Security Autonomy, Cryptographic strength and a variety of functions traditionally available in Type 1 applications. The architecture is used in the CITADEL™ Cryptographic device. CITADEL™ is Harris' prime export encryption solution for all of its new products requiring security, such as the FALCON II HF, VHF, and Multi-band radio platforms.

5. References