Robustness-Agile Encryptor for ATM Networks

HERBERT LEITOLD, WOLFGANG MAYERWIESER, UDO PAYER, KARL CHRISTIAN POSCH, REINHARD POSCH, JOHANNES WOLKERSTORFER

Institute for Applied Information Processing and Communications,
Graz University of Technology, Austria[1]

Key words: ATM encryption, agile encryption, ATM, DES, Triple DES

Abstract: This paper describes a robustness-agile ATM encryption unit which exploits parallel control processes. A VLSI chip implementing these concepts is presented. This single-chip encryptor performs CBC-mode Triple-DES encryption up to 155 Mbps with delays well below one ATM cell period. The microchip advances the field of confidentiality services in ATM networks in several dimensions: First, the delay introduced due to encryption has been minimized and is negligible in terms of Quality of Services requirements of delay sensitive applications. Second, outer-CBC Triple-DES is supported at 155 Mbps, so far not used by ATM encryptors. Third, the unit is scalable in the number of virtual connections, i.e. the number of agile session keys. Finally, the single-chip approach allows to integrate encryption into the end-user ATM access device, such as a desktop PC.

1. INTRODUCTION

Catch-phrases like "broadband to the curb" or "broadband to the home" characterize a trend towards ubiquitous high-speed telecommunication [1][2]. Asynchronous transfer mode (ATM) is a technology of choice and

[1] The work described origins from the European Commission funded project Secure Communications in ATM Networks (SCAN) established under contract AC0330 in the Advanced Communications Technologies and Services (ACTS) Program.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

has matured from first pilot installations and research test beds in the early 1990s [3] to continuously increasing popularity as demonstrated in its use in the Trans European Network [4]. The benefits promised by ATM can be summarized by sketching two major characteristics: First, ATM is a technology that can deliver different types of traffic with Quality of Service (QoS) over a single digital transport mechanism. Second, ATM is defined independently from the transmission media. The former enables ATM to carry the diversity of communication profiles, such as voice, video, digital data, or computer based local area network traffic [5]. The latter characteristic resulted in numerous media ATM has been applied to, such as 2 Mbps/1.5 Mbps E1/T1 plesiochronous digital hierarchy [6], cable television networks [7], asymmetric digital subscriber line [8], and synchronous optical network at 155 Mbps optical carrier 3 (OC3) [9].

However, whenever publicly accessible communication infrastructure is involved, security aspects are a major concern. The ATM Forum started to standardize security services in 1996 [10]. These efforts resulted in the approval of the ATM Forum Security Specification, version 1.0 in 1999 [11]. The specification covers data origin authentication, data confidentiality, data integrity, access control, and security parameter negotiation services.

In this paper, we focus on data confidentiality. In particular, we discuss specific requirements and user expectations to be met when migrating ATM networks to an infrastructure that provides secrecy on demand. These are mainly end-to-end confidentiality services that retain the key benefits of ATM: the bandwidth offered, the service independence, the QoS guarantees, and its applicability to different physical media. Based on the constraints defined by these characteristics, we describe a model enabling robustness-agile encryption in ATM networks and demonstrate a single-chip VLSI system which is currently available as a prototype.

This paper is structured as follows: Section 2 sketches the basics of ATM and discusses general constraints faced when applying cryptography to ATM. In section 3, we deepen the view to confidentiality in ATM networks by surveying features that form the user expectations from an ATM encryption system. The architecture of a solution for an ATM encryptor based on these requirements and the resulting single-chip are discussed in section 4. Finally, the current state and further directions of the underlying project are discussed.

2. ATM CONFIDENTIALITY BASICS

In principle, ATM is a switching technique that operates on fixed size data units called cells. ATM cells consist of five-octet headers carrying the information used to guide cells through the network and 48-octet payloads that carry the user information. The fixed cell size and virtual channel (VC) techniques enable efficient hardware processing for switching cells.

In order to convert information generated in an ATM-enabled end system into the ATM cell format understood by the ATM network, a variety of ATM adaptation layers (AALs) has been defined. These AALs consist of segmentation and re-assembly (SAR) functions and convergence sub-layer functions. In order to achieve independence from the transmission media, the transmission convergence (TC) mechanisms convert ATM cells to the transmission frame, and the physical media dependent functions operate on the bit streams transmitted by the media.

The ATM protocol reference model [12] collects these characteristic functions. The protocol model is a layered architecture where the AAL resides on top and offers interfaces to the application sitting above. The ATM layer operates on ATM cells and combines the AAL and the physical layer, which interfaces to the transmission media. In its vertical representation, the ATM protocol model is divided into several planes: There is the control plane which defines the signalling functions required to establish, to maintain, and to close communication channels. Next comes the user plane which is responsible for transmitting the user data over VCs. Finally, the management plane defines the functions to keep the ATM network operational as a whole.

For adding means of security in this reference model, the following arguments become important: An obvious requirement is that the security system should neither confine the service independence, represented by several AALs, nor should the applicability to different media be restricted, which is represented by different implementations of the physical layer (PHY). This leads to integrating the data confidentiality services to the only layer that is independent of both AAL and PHY: the ATM layer. For these reasons, the ATM Forum Security Specification [11] defines the ATM layer for embedding user plane confidentiality as well.

Confidentiality is achieved by encrypting the ATM cell payload and leaving the ATM cell header unchanged. In this way, the header can be interpreted by the intermediate network elements, the ATM switches. The ATM cell payload can be accessed by either intercepting the ATM cell stream at the interface between the SAR sub-layer and the ATM layer, by integrating cryptographic procedures into the ATM layer, or by intercepting the ATM cell stream at the interface between the ATM layer and the TC sub-layer. In fact, the latter approach, using the ATM-TC interface, has been followed in our project. The reasoning is that this interface is usually implemented as the industrial de facto standard interface for ATM end systems, called UTOPIA [13].

Based on the approach of encrypting the ATM cell payload, a hurdle to take is the bandwidth to be dealt with. Obviously, symmetric encryption mechanisms are the choice. The block size of widespread symmetric block ciphers neatly fits the 48-octet ATM-cell payload: the data encryption standard (DES) [14] or its triple encryption derivative Triple DES [15] both operate on 64-bit data blocks. This results in six DES or Triple DES blocks per ATM cell payload.

In the context of this paper we limit our scope to the 155 Mbps OC3c SONET signal. The reasoning is that the work described in this paper origins from a project that brings ATM security services to the desktop PC by developing a secure ATM network interface card. Nowadays OC3c rates represent the state-of-the-art of ATM PC internetworking. Obviously, the ATM cell payload encryption causes the major processing load in an encryption system. The ATM payload rate amounts to 135.63 Mbps. During a period of 2.83 μs six blocks must be encrypted.

One might conclude that the figures above are not the most critical constraint, as six DES processors could act in parallel. Whereas this is an obvious speed-up opportunity in electronic codebook (ECB) operational mode, this approach is not feasible with feedback modes such as cipher block chaining (CBC) [16]; in CBC mode subsequent blocks depend on each other and thus cannot be encrypted in parallel.

ATM cells are statistically multiplexed between different VCs identified by a 24-bit value, usually referred to as the virtual path identifier (VPI) virtual channel identifier (VCI) pair, at the user network interface (UNI) [9]. This spans a huge VPI/VCI space of 2^{24} possible VCs, where potentially dozens or hundreds out of the VPI/VCI range of values are active simultaneously at a certain end system. Each connection is assigned a unique encryption context in terms of session keys, encryption method, operational mode, or even encryption algorithm. This requires that the encryption system switches the encryption context, such as session keys or initialization vectors (IVs), between two adjacent ATM cells that are assigned different VCs. This means that within the ATM cell period of 2.83 μs we need to include an encryption context switch. Such an ATM encryption approach is termed "per-VC encryptor" or "agile ATM encryptor". This problem is further discussed in section 3.

Agile encryption leads to a further constraint: ATM guarantees QoS. For instance, the maximum cell transfer delay (CTD) and cell delay variation

(CDV) limits are negotiated for real time services during the VC establishment phase. The encryption process shall not affect these parameters, i.e., the latency introduced by encryption has to be minimized. Two factors determine latency. These are the encryption process itself, and the period required to identify the encryption context. This decision is based on the values of VPI/VCI and payload type identifier (PTI) which are found in the ATM cell header.

Typical delays of ATM encryptors currently available on the market are in the order of 3 to 5 ATM cell periods. Postponing further discussion of this aspect to section 4, we conclude that identifying and loading the encryption context does not further increase the delay introduced by the encryption process itself, as long as it is in the order of one encryption process, i.e. about 472 ns with an OC3c UNI.

3. AGILE ENCRYPTION IN ATM NETWORKS

As defined in [17], *key-agile ATM encryption* employs a single algorithm together with a single mode of operation. Thus, the agile encryption context is limited to session keys, IVs, or state vectors in the case of counter operational modes. The development of a key-agile ATM encryption system for the North Carolina Information Highway is described in detail in [18]. Single-algorithm ATM encryption draws the question to agility in the cryptographic robustness. Different applications might require different cryptographic strength in terms of key-length, or different cryptographic robustness in terms of operational modes.

Robustness-agile encryption refers to an approach where the encryption context consists of a number of encryption algorithms or variants of the same algorithm, and various operational modes. Our encryption unit can rapidly switch between reasonable combinations of these algorithms and operational modes depending on ATM cell header parameters.

An *algorithm-agile encryptor* [19] switches rapidly between different algorithms, such as IDEA, FEAL, DES, and even variants of the algorithms and different operational modes.

In our approach, all parameters of the encryption context are stored together. This includes the session key, the IV, as well as the encryption algorithm and the mode of operation. In section 4 we describe the modular architecture of a single-chip ATM encryptor featuring DES, Triple DES, ECB, and CBC up to 155 Mbps. Several on-chip control processors, each optimized for its specific task to be fulfilled, operate in parallel. This robustness-agile system keeps the delay introduced by the encryption fairly below one ATM cell period, in fact just slightly above 1000 ns under OC3c.

This means that the maximum delay is one ATM cell period when embedding encrypted ATM cells into synchronous transmission frames.

4. HADES, A SINGLE-CHIP ROBUSTNESS-AGILE ATM ENCRYPTOR

A block diagram of the ATM encryptor chip is shown in figure 1. Basically, the ATM encryption unit is inserted at the UTOPIA interface between the ATM layer and the physical layer. UTOPIA is a clocked octet-wide interface with two line hand-shaking at a clock rate of 25 MHz. In addition, there is an extra "start-of-cell"-bit for synchronization on cell level.

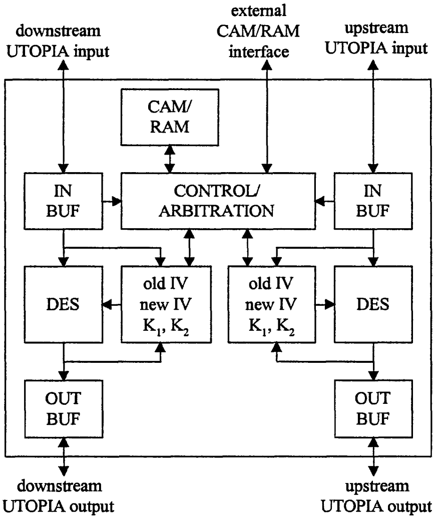

Figure 1. Block diagram of the ATM encryption module

The chip recognizes special ATM cells carrying information for configuring the ATM encryption unit. Basically, these cells are used for loading new keys into the memory (CAM/RAM), or for invalidating already loaded keys in memory. Once a key is stored in the memory, it can be referred to by using its associated VPI/VCI. The ATM encryption unit recognizes ATM header blocks with their VPI/VCI and tries to locate the keys in the content addressable memory (CAM). It subsequently unloads and stores the current encrypted block in the RAM for potential later usage as initialization vector (IV), and loads the new keys and the IV into the encryption core.

In order to achieve the given speed requirements, we use a mix of techniques. First, the two communication directions are treated almost independently. Only the access to memory is sequenced by an arbitration unit. Second, the DES encryption cores are running at a clock frequency of 250 MHz. With this frequency the specified throughput of 155 Mbps is achieved. The third major ingredient is a pair of hierarchically ordered set of control machines in charge of sequencing the activities on the chip. For each of the two directions we use five independent control machines. In addition, an arbitration unit manages access to CAM and its associated RAM.

The *DES-core controller* sequences the 16 DES rounds. This machine lies at the bottom of the hierarchy and gets its commands from the DES-mode controller. The *DES-mode controller* manages the two plus one modes ECB, CBC, and “no encryption”. The *DES-load controller* shuffles 8-octet blocks between a set of 5 locations. In its simplest form it sequences loading and unloading of the DES core. It can handle blocks of 5 octets and 8 octets. Depending on the situation, input blocks are loaded into the DES core and/or into the IV input buffer, and output blocks are potentially fed back to the DES-core input for exclusive-ORing with the input data.

The *block-level controller* recognizes 8-octet data blocks and 5-octet header blocks. It also distinguishes between the first data block after a header block and all other data blocks. For the first data block usually a different IV is needed, whereas for all other data blocks the previously encrypted block serves as IV. The block level controller also recognizes situations when for a given period of time no new input data block arrived in the input queue. After this timeout it issues an unload-command to the DES-load controller.

The *cell-level controller* monitors the input data. Depending on these data, it issues commands to its lower level controllers, and requests access to the memory bus from the arbitration unit. After being granted access to the memory (CAM and associated RAM), it sequences the compare operations in the CAM, and the write and read operations to and from the RAM. Basically, there are three types of cells which generate rather different activities. Configuration cells are used after hardware reset for setting up registers, CAM, and RAM with appropriate contents. Key-download cells are used for specifying encryption mode, keys, and IVs for a corresponding VPI/VCI. A series of write operations to CAM and RAM is issued by the controller transferring data from the input buffer and the source IV buffer to RAM and CAM. The third basic type of cell is the user cell. Depending on its VPI/VCI and its payload type identifier all necessary actions are controlled by the cell-level controller. Typically, after a CAM-compare cycle and a read cycle from the RAM such a cell is recognized. Then, the keys are read from the RAM and transferred to the DES core. The cell-level controller must wait for an appropriate time slot in order to not interfere with the ongoing activities in the DES core. In addition to loading new keys, the IV has to be managed: the old IV needs to be saved in RAM for future use, and the new IV is copied from the current RAM locations to the DES core.

The *arbitration unit* gets requests from both cell-level controllers for being granted access to CAM and RAM. In response to these requests it issues grant signals. The two directions are treated in a different manner. A request coming from the upstream is granted at the earliest convenience. Once being granted to access memory, the upstream does not release the memory bus until it has finished all actions related to the current ATM cell, i.e. loading encryption mode and keys, and managing the IV. In contrast, the arbiter may remove the down-stream's grant signal at any time.

For each VPI/VCI to be managed by the chip, corresponding *CAM and RAM* locations need to be present. The CAM has to supply 24 bits plus one bit per VPI/VCI. The additional bit specifies the validity of the CAM entry. In the RAM we need 3 times 64 bits (for two keys and the IV) plus 4 bits (for specifying the mode) per VPI/VCI. The encryption chip has on-chip CAM/RAM and an interface for adding extra off-chip CAM/RAM. The interface to the off-chip memory is 32 bits wide. Typical speed requirements are 32 ns access time for the RAM, and approximately 80 ns compare time for the CAM. The write time for the CAM is not critical. The chip has status registers for setting CAM and RAM speed upon setup. Finally, an *on-chip oscillator* runs at a nominal frequency of 250 MHz.

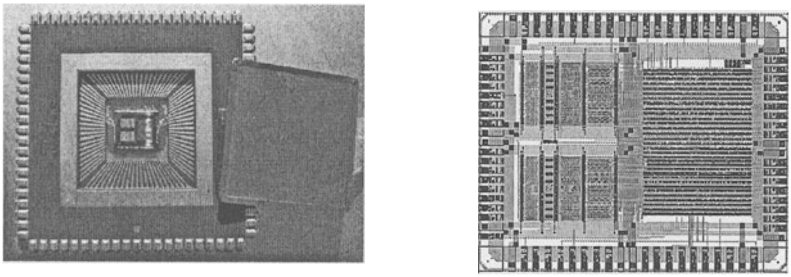

Figure 2. The prototype chip and its layout

The high-speed ATM DES/TripleDES (HADES) unit has been designed as a VLSI circuit in 0.6 micron CMOS technology. The architecture consists of two parts: The data path with input/output buffers and the DES/Triple DES core, and the data sequencing and key queuing path. The throughput limiting block in the data path is the DES-TripleDES core. It is designed in full custom design style using a true single phase clocked (TSPC) logic style. Running at a nominal frequency of 250 MHz, the net DES throughput is about 440 Mbps, or 145 Mbps in TripleDES outer-CBC mode, respectively. The two DES cores together with the input/output buffers consist of about 33.000 transistors. The area of one DES core is approximately 1.8 mm^2.

The controller and key queuing block are designed in semi-custom style using standard cells. The standard-cell block operates at a quarter of the nominal frequency. Figure 2 illustrates the HADES layout which consists of the two DES cores on the left, and the controller and key queuing block to the right. The chip as a whole consists of about 120.000 transistors, and its silicon area is 27.2 mm^2. The power consumption is 230 mA at the nominal supply voltage of 5 V.

HADES can be transparently integrated into ATM end systems supporting UTOPIA, which constitute the vast majority of ATM end systems. In this context "transparent integration" means that the chip offers a PHY layer component interface to the ATM layer and vice versa substitutes an ATM layer component to the PHY layer. We support 155 Mbps OC3c adaptors, mainly used in ATM LAN environments, as well as 2 Mbps common in public ATM access networks. Applicability to ADSL modems is under investigation, as these usually also support the UTOPIA interface.

5. CONCLUSIONS

It is commonly recognized that ATM-based multimedia and communication applications increasingly have to transfer sensitive information on a large scale. This paper is based on a project addressing this area of confidential end-to-end communication over ATM. We have compared different methods of ATM encryption, and have chosen a VC-based approach where the ATM cell payload is encrypted. We have implemented encryption at the ATM layer, and use the de facto standard UTOPIA interface to intercept the ATM cell stream.

We have designed a single-chip encryptor which basically consists of a pair of DES/TripleDES encryption cores steered by a set of control machines and augmented by on-chip CAM and RAM. To increase the number of confidential connections, the size of CAM/RAM is extendable over a wide range, either on-chip or off-chip by using a 32 bit data interface. The ATM encryption chip has been tested up to 290 MHz clock frequency, which is far above its nominal frequency of 250 MHz required to provide TripleDES in outer-CBC mode at 155 Mbps.

In future work we will integrate the single-chip encryption unit into an ATM network interface card. This single slot peripheral component interconnect (PCI) adapter fits a conventional desktop PC.

6. REFERENCES

[1] B. Khasnabish, "Broadband to the Home (BTTH): Architectures, Access Methods, and the Appetite for it", *IEEE Network*, vol. 11, no. 1, Jan./Feb. 1997, pp. 58-69.

[2] L. A. Ims, D. Myhre, B. T. Olsen, "Economics of Residential Broadband Access Network Technologies and Strategies", *IEEE Network*, vol. 11, no. 1, Jan./Feb. 1997, pp. 51-57.

[3] B. J. Ewy, J. B. Evans, V. S. Frost, G. J. Minden, "TCP/ATM Experiences in the MAGIC Testbed", *Proceedings of the Fourth IEEE International Symposium on High Performance Distributed Computing*, 1995, pp. 87-93.

[4] M. H. Behringer, "The Implementation of TEN-34", *Proceedings of 8th Joint European Networking Conference JENC'97*, 1997, pp. 331/1-7.

[5] I.F. Akyildiz, K.L. Bernhardt, "ATM Local Area Networks, A Survey of Requirements, Architectures, and Standards", *IEEE Communications Magazine*, vol. 35, no. 7, July 1997, pp. 72-80.

[6] ATM Forum, "E1 Physical Interface Specification", *The ATM Forum, Technical Committee*, 1996.

[7] E.J. Hernandez-Valencia, "Architectures for Broadband Residential IP Services Over CATV Networks", *IEEE Network*, vol. 11, no. 1, Jan./Feb. 1997, pp. 36-43.

[8] K. Maxwell, "Asymmetric Digital Subscriber Line: Interim Technology for the Next Forty Years", *IEEE Communications Magazine*, vol. 34, no. 10, October 1996, pp. 100-106.

[9] G. Dobrowsky, (Ed.) "ATM User-Network Interface Version 3.1 Specification", *The ATM Forum, Technical Committee*, 1994.

[10] M. Peyravian, T. Tarman, "Asynchronous Transfer Mode Security", *IEEE Network*, vol. 11, no. 3, May/June 1997, pp. 34-40.

[11] ATM Forum, "ATM Security Specification Version 1.0", *The ATM Forum, Technical Committee*, atm-sec-01.0100, 1999.

[12] ITU-T, "B-ISDN Protocol Reference Model and its Application", *International Telecommunication Union, Telecommunication Standardisation Sector*, Recommendation I.321, 1991.

[13] ATM Forum, "Utopia Level 2, Version 1", *The ATM Forum, Technical Committee*, af-phy-039.000, 1995.

[14] ANSI, "American National Standard for Data Encryption Algorithm (DEA)", *American National Standards Institute,* ANSI 3.92, 1981.

[15] W. Tuchman, "Hellman Presents no Shortcut Solutions to DES", *IEEE Spectrum*, vol. 17, no.7, 1979.

[16] ANSI, "American National Standard for Information Systems-Data Encryption Algorithm-Modes of Operation", *American National Standards Institute*, ANSI 3.106, 1983.

[17] L.G. Pierson, E. L. Witzke, M. O. Bean, G. J. Trombley, "Context Agile Encryption for High-Speed Communiction Networks", *ACM SIGCOMM, Computer Communications Review*, vol. 29, no. 1, January 1999, pp. 35-49.

[18] D. Stevenson, N. Hillery, G. Byrd, "Secure Communications in ATM Networks", *Communications of the ACM*, vol. 38, no. 2, February 1995, pp. 45-52.

[19] Encryption in ATM Networks", IEEE Computer, vol. 31, no. 9, September 1998, pp. 57-63.