Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 2, No. 6 July, 2000

EPE - Enhanced Privacy and Encryption

This month's issue presents an article on EPE (Enhanced Privacy and Encryption) by one of its foremost architects. This voice privacy and signaling and data encryption standard has been adopted by TR-45.3 to better secure communications in TDMA (TIA/EIA-136 Revision B and later) systems, although it could be embedded in other systems as well. EPE does not cover authentication, and therefore does not affect the transition from CAVE-based authentication to the 3G AKA authentication system.

Inside EPE

by Bob Rance,
Secure Technologies Dept.,
Bell Labs, Lucent Technologies

Enhanced Privacy and Encryption (EPE) provides a highly increased level of security for Voice, signaling messages (DTC and DCCH), and Radio Link Protocol (RLP 1) User Data. It is intended to replace the existing Voice Privacy, Signaling Message Encryption (SME), and Data Privacy features for a new generation of TDMA mobiles. EPE is automatically applied if the mobile, and the Base Station, Mobile Switching Center, and Inter-Working Function (BMI) support the feature.

Why EPE?

In 1997, the CMEA algorithm (Cellular Messaging Encryption Algorithm) was found insufficient to secure expected amounts of Wireless (Cellular) messaging traffic [1]. CMEA had been planned for use in North American TDMA, CDMA, and Analog systems to encrypt a small but important subset of their messages. For TDMA systems, CMEA would have been used to encrypt certain messages on the DTC (traffic channel). In particular, one class of messages carried sensitive user information such as credit card numbers.

Glossary

For any terms you are unfamiliar with, please consult:

www.cnp-wireless.com/glossary.html

Other TDMA content needed to be better secured, namely voice, data, and DCCH messages. Existing privacy standards (included in TDMA standards IS-54, IS-136 and Revisions 0 and A of TIA/EIA-136) would have three major weaknesses if they were implemented:

1. Voice privacy using a fixed, 260-bit mask is considered to be insecure [2].
2. User data would be encrypted by an insufficiently strong algorithm called ORYX [3].
3. There is a need to protect some messages on the DCCH (digital control channel) as well, which earlier secu-

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security Perspectives* is $250 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$300 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

Current subscribers to *Cellular Networking Perspectives* receive a discounted price – only $200 for delivery within the US and Canada or $250 elsewhere.

Back issues are available individually, or in bulk at reduced prices.

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due...

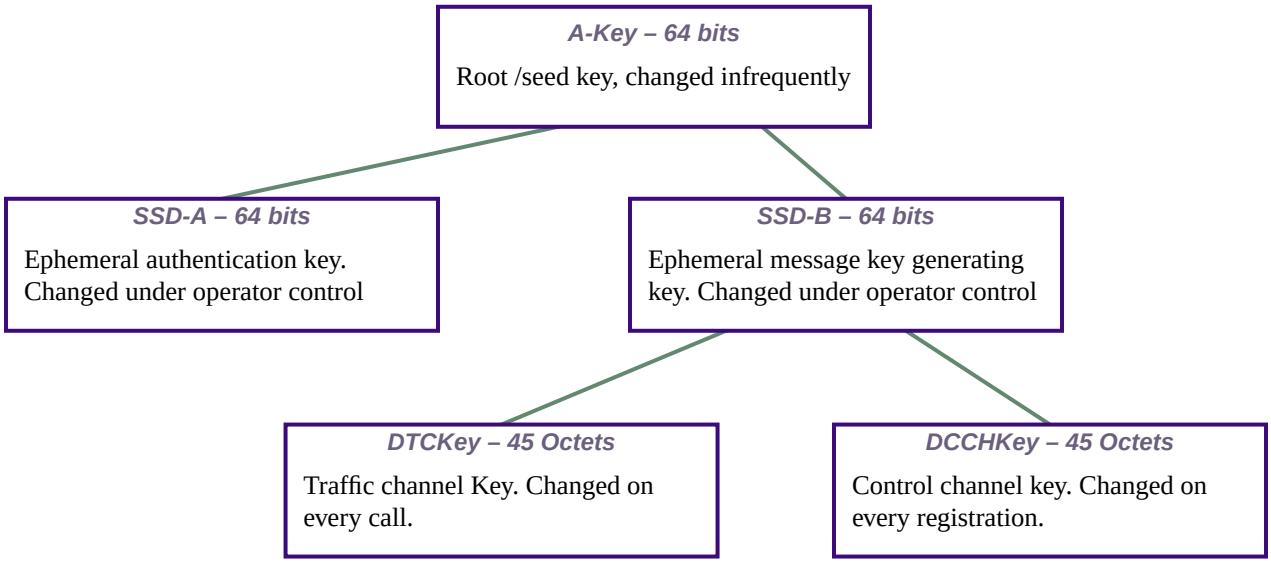
August 15th, 2000.

Future Topics

IP security • Public Keys & Wireless • Kerberos PKINIT• Public Key Infrastructure (PKI) • IKE • Wireless Data Security • Elliptic Curve Cryptography (ECC)• Abelian Varieties • IETF Security Standards

Wireless Security Perspectives is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada.
Contact Information: Phone: 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/wsp.html.
Subscriptions: $200 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$250 elsewhere. Non-subscribers pay $250/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery:** Email or 1st class mail. **Back Issues:** Available individually for $20 in the US and Canada and US$25 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

Figure 1: EPE key hierarchy for CAVE-based authentication



rity standards would send in the clear (unencrypted).

At the time of the development of the CMEA and ORYX algorithms, there were US export restrictions that limited the strength of commercial wireless systems. Since then, these restrictions have been eased significantly.

These issues motivated the development of a highly secure and more inclusive method of air interface protection called EPE (Enhanced Privacy and Encryption).

Two Original Approaches

The TDMA standards committee initially considered two approaches:

1. Lower Layer Encryption

   Encrypt all material at a lower layer with a cryptographic synchronization method (cryptosync).

2. Higher Layer Encryption

   Encrypt voice between the speech coder and convolutional coder, signaling messages at Layer 3 and user data at Layer 3 where it had been planned to be encrypted with ORYX.

The first approach had the benefit of simplicity. It also had the advantage of guaranteeing unique encryptions and not extending errors. If this approach had been followed, TDMA physical layer encryption would have had a predecessor to model after, namely GSM. However unlike GSM, which devotes part of its bandwidth to maintaining cryptosync, TDMA, being a mature system, had no available bandwidth for this purpose.

Thus, using the first approach of lower layer encryption with cryptosync, two related speech impairments would have occurred:

- In noisy channel handoffs, cryptosync might not have been identically replicated at both ends. This would have resulted in total inability to communicate speech and cause dropped calls.
- To mitigate against the first impairment, the system would have needed to introduce a significant delay in encrypting speech so that it could take the time needed to send the appropriate sequence of messages and their acknowledgments to ensure robust cryptosync.

The lower layer approach would also be more likely to require changes in silicon ASICs (Application Specific Integrated Circuits) which often process the content at the lower layers. In contrast, encryption at a higher layer would likely occur in processors where the changes would tend to be in software. Silicon changes would delay the fielding of an enhanced encryption system. Also moving the location of data encryption might have been problematic since on the system side, data encryption via ORYX would have occurred in a separate entity called the IWF (Inter-Working Function). Finally, the specification of new inter-layer messaging would have been needed to indicate which content was to be encrypted.

Due to the disadvantages of the lower layer encryption approach, the higher layer approach was selected for TDMA. This is EPE. The CAVE key hierarchy, as modified for EPE, is shown in Figure 1.

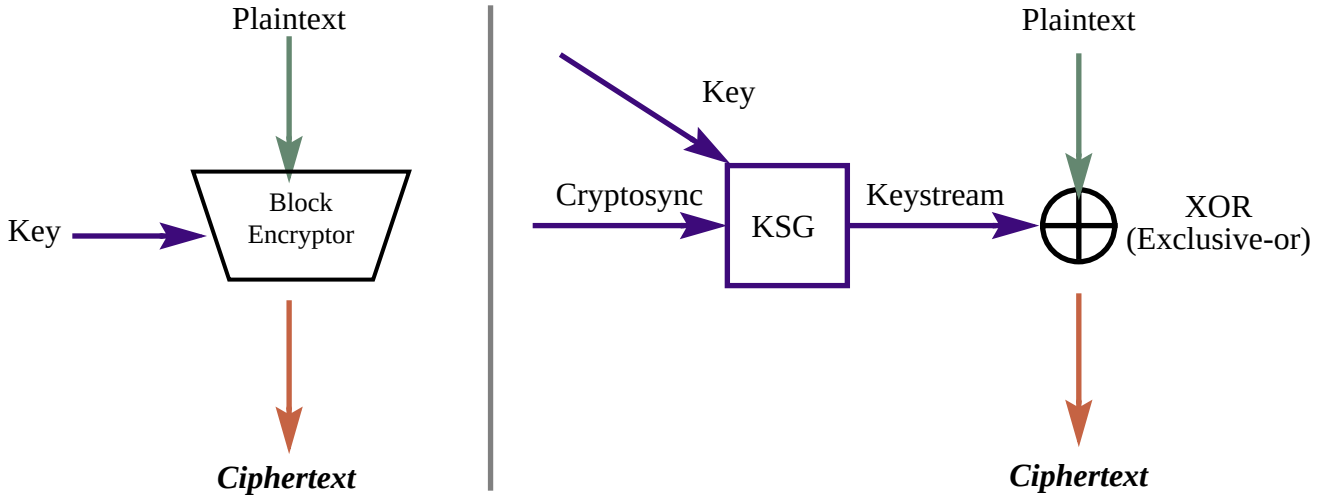
Types of Encryptors

Encryptors occur in two primary forms: block encryptors and keystream generators (or stream ciphers) – See Figure 2.

Block Encryptors

In many cases, block encryptors can provide high security without the need for external synchronizing information (cryptosync). They operate by taking a block of content called plaintext, and encrypt (secretly permute) it to yield a block of ciphertext so that the nature of the content is obscured. When encrypting over the air interface, a block decryptor will disadvantageously extend a single error over the entire block (known as *error extension*). Using a hypothetical example, if the 260-bit output of the convolutionally-encoded voice frame were

Figure 2: Block Encryptors and Keystream Generators (KSG's)



block encrypted and then block decrypted, any uncorrected channel errors would totally corrupt the block and significantly impair voice quality.

Keystream Generator (KSG)

A keystream generator (also called a running-key generator, rolling mask or stream cipher) encrypts by XORing a secret keystream with plaintext to yield ciphertext. Uniqueness of the keystream generator's output block is guaranteed by uniqueness of its input cryptosync, even when a plaintext block is identically repeated. Keystream generator encryption has the beneficial property that it does not extend errors. However, it requires the presence of totally reliable cryptosync (synchronizing information). Any differences of cryptosync between the two ends would result in total corruption of the block being encrypted.

EPE Voice, Message, and Data Architectures

Enhanced Privacy and Encryption for TDMA (EPE) uses the SCEMA algorithm for confidentiality of voice, DTC (digital traffic channel) messages, DCCH (Digital Control Channel) messages and RLP (user) data. The SCEMA algorithm may be operated in both a block cipher mode and a stream cipher mode (KSG).

Voice Privacy

The EPE voice architecture is novel in that it provides unique encryptions of speech frames without the use of an externally-provided cryptosync. This architecture would be useful in many systems which cannot allocate the additional communication bandwidth needed to generate robust cryptosync. As shown in Figure 3, the EPE voice architecture comprises a block encryptor and a keystream generator, which respectively encrypt the speech coder's Class 1A bits, and the remaining bits comprising Class 1B and Class 2 bits. The block encryptor employs, very effectively, the uniqueness of the Class 1A bits to provide unique encryptions of these bits. In turn, the block encryptor's output, namely ciphertext, substitutes for a formal, external cryptosync and ensures uniqueness of the keystream blocks.

Signaling Message Encryption

Signaling messages (e.g. for registration, call setup and maintenance purposes) are block encrypted and the general uniqueness of the messages results in a general uniqueness of the ciphertexts. The uniqueness is augmented by use of the parameter *Message Type*, and additionally in the DCCH, the parameter *RAND*. Figure 4 depicts encryption of messages greater than or equal to 48 bits in length. For messages less than 48 bits, a block encryptor alone is used with the *RAND* and *Message Type* input used in other ways to provide uniqueness.

Data

EPE encrypts data via a keystream generator driven by cryptosync that is developed in the RLP 1 protocol as shown in Figure 5. RLP content is encrypted via SCEMA in the keystream generator mode with the 32-bit *HOOK* as cryptosync. *HOOK* is input to SCEMA's cryptosync input and is repeated as necessary at SCEMA's plaintext input to create the appropriate amount of keystream. For example, if 33 bits of keystream are needed, *K* is set equal to 5 octets, and the first octet of *HOOK* is repeated to fill the plaintext field. The last 7 bits of the ciphertext output are discarded to yield 33 keystream bits.

Key Schedules

Key schedules are used to expand the session encryption keys. This deterministic bit-expansion of a cryptographic key allows a cryptoalgorithm to run faster at a given security level. EPE currently expands two 8-octet keys to yield two 45-octet key schedules:

- The DCCHKey schedule is exclusively used to protect DCCH messages. It is generated in the mobile and network (base station or MSC) when the mobile initiates Power Up, ACC to DCCH, Forced, or New System Regis-

Figure 3: ACELP Speech Coder Voice Encryption Placement

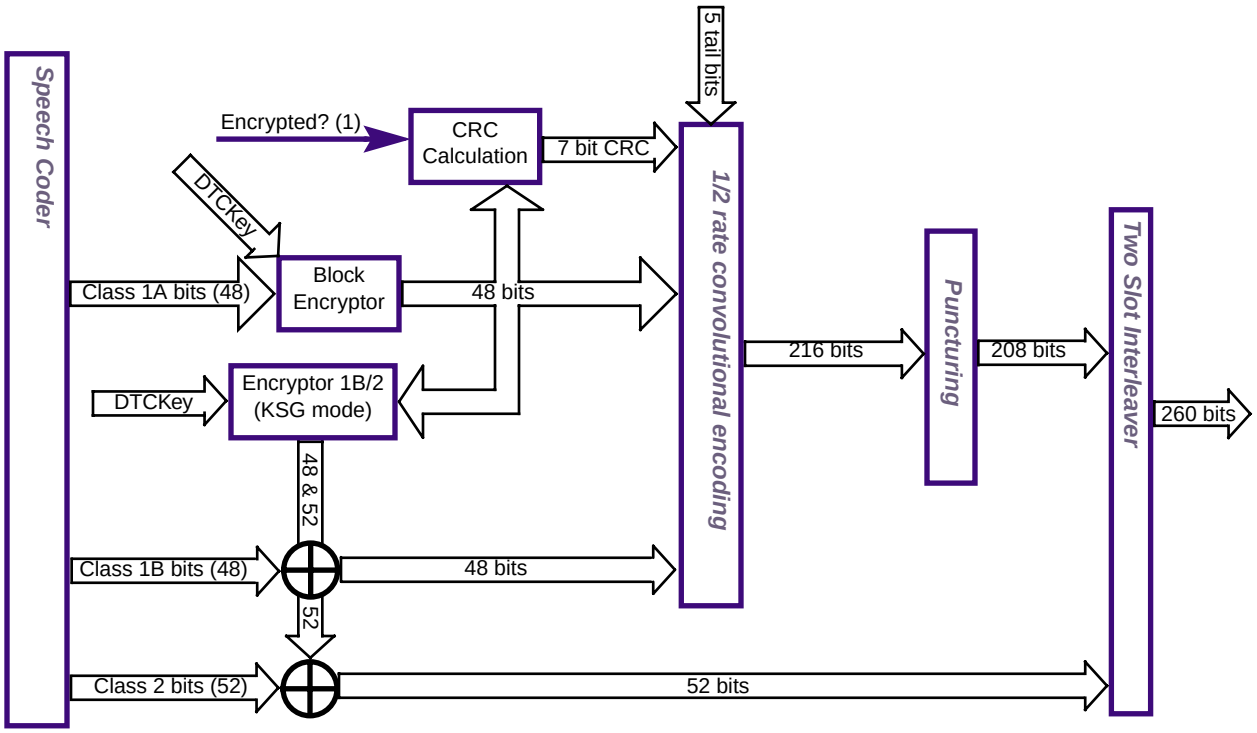


Figure 4: Encryption for Signaling Messages Over 48 bits

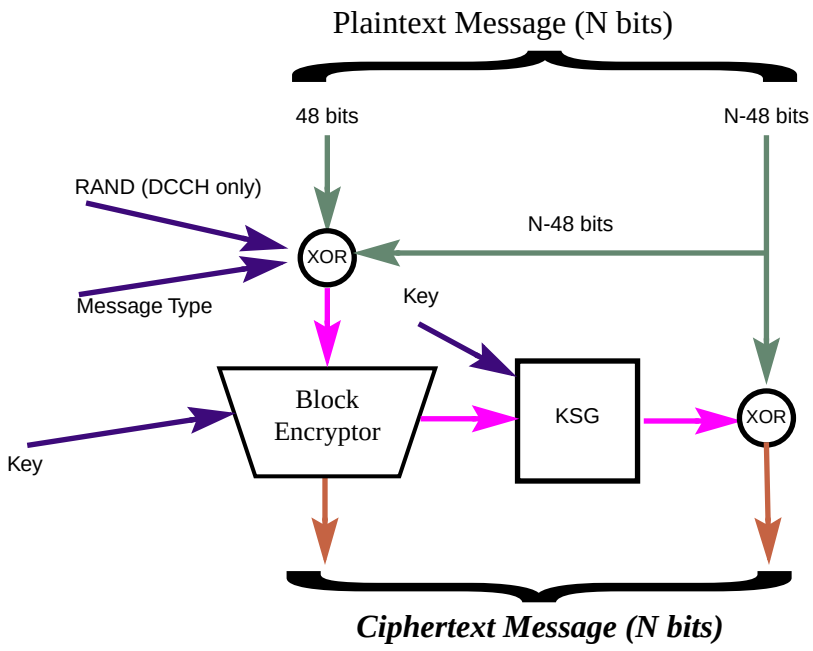
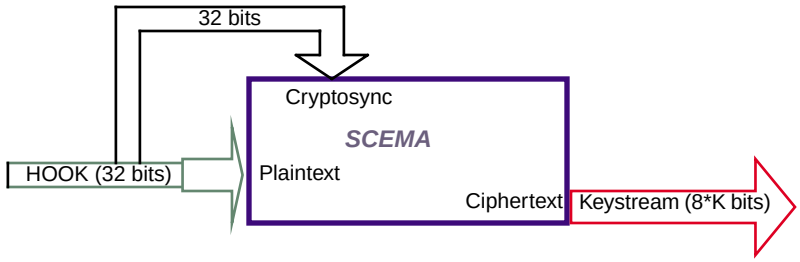


Figure 5: Enhanced Data (RLP) Encryption



tration. The DCCHKey remains valid while the MS is registered in a system.

- The DTCKey schedule is used to protect Voice, DTC Messages, and RLP Data. It is generated in the mobile and network at the beginning of a call and remains valid for the call's duration.

Both keys are necessary to handle Inter-MSC roaming. The DCCHKey must be regenerated when the mobile registers in the new system. The DTCKey must be maintained across MSCs during handoffs and will be transmitted as defined by TIA/EIA-41.

SCEMA

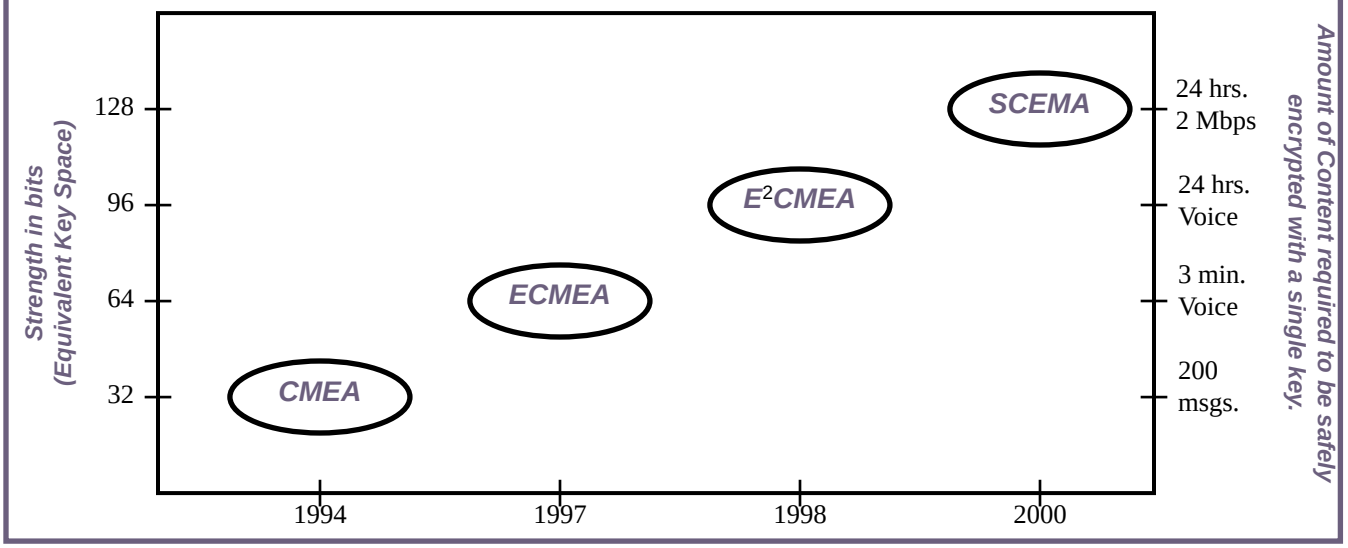
EPE uses a flexible encryption building block called SCEMA to implement the block encryptor and KSG [4]. SCEMA is a variable size block encryptor, so its utility lies in its ability to efficiently encrypt data of several types and sizes as are found in Wireless systems. SCEMA is far more secure than the CMEA algorithm (Cellular Messaging Encryption Algorithm). Over the past several years it has been extensively analyzed by industry experts and is believed to have strength of at least 96 bits, although no attacks have shown it to be weaker than 128 bits. This means that, because there are no known shortcut methods, an attacker would have to try at least 2^{96} or 2^{128} keys before finding the correct one [5,6]. Even on a supercomputer, such a search would still take longer than the age of the Universe, and even with Moore's law (processing power doubling every 1.5 years) this will still be true for many years. Figure 6 shows how CMEA evolved to SCEMA, with increasing strengths and amount of plaintext to be encrypted.

SCEMA should be secure for well beyond the next 20 years. (20 years corresponds to 80 bits of strength.)

Conclusions

This article has given an overview of EPE, which will be a significant enhancement in security over that in the current TDMA system. Further details may be obtained from the author (rrance@lucent.com).

Figure 6: Evolution of CMEA to SCEMA



Glossary

Cryptosync
: Externally-provided synchronizing information for cryptoalgorithms (ciphers) that allows an encryptor at one end to uniquely encrypt each block of content into ciphertext, and yet allows a decryptor at the other end to properly decrypt the ciphertext to yield the original plaintext. Cryptosync often takes the form of the output of a binary counter.

DCCHKey
: Digital Control Channel Key.

DTCKey
: Digital Traffic (Voice) Channel Key.

EPE
: Enhanced Privacy and Encryption: A North American TDMA architecture that secures voice, messages, and data.

KSG
: Keystream Generator.

SCEMA
: A variable length block cipher specifically designed for wireless systems.

References

[1] D. Wagner, B. Schneier, J. Kelsey, *Cryptanalysis of the Cellular Messaging Encryption Algorithm*, *Advances in Cryptology – Crypto '97, Proceedings*, pp. 526-537, Springer, 1997.

[2] J. P. Barlow, *Decrypting the Puzzle Palace*, Communications of the ACM, July 1992.

[3] D. Wagner, B. Schneier, J. Kelsey, *Cryptanalysis of ORYX*, unpublished manuscript, May 4, 1997.

[4] M. H. Etzel, D. N. Heer, R. J. Rance, *SCEMA - An efficient Encryption Algorithm for Multiple Types of Data*, NetWorld+Interop 2000 Las Vegas, May 7-12, 2000.

[5] R. J. Rance, *Linear Cryptanalysis of ECMEA*, TIA TR45.AHAG, July 20, 1998.

[6] R. J. Rance, *ISSI Report on SCEMA*, TIA TR45.AHAG, October 27, 1998.

About the Author

Robert J. Rance is a Consulting Member of Technical Staff at Bell Laboratories – Lucent Technologies.

Mr. Rance joined Bell Labs in 1976 and has worked throughout on the design and analysis of security/privacy related products and studies. Some of these products and studies comprise novel high-speed, high-accuracy A/D and D/A converters, robust RNGs (Random Number Generators), RNG analyses, key management and encryption architectures for HFC and Wireless systems, and security system threat analyses. Mr. Rance shares three patents relating to the above areas.

His education includes a BSEE (1971), an MSEE (1974), and a Degree of Electrical Engineer (1974), all from M.I.T.