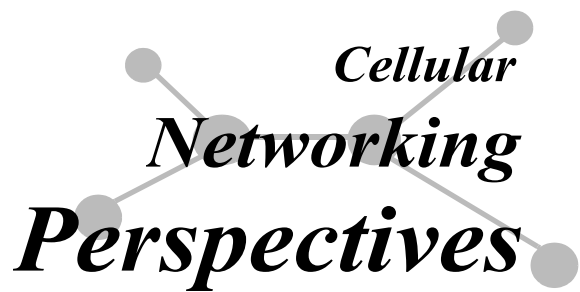


Wireless Security Perspectives



Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com

Vol. 4, No. 9. October, 2002

Cryptography in the News

NewScientist.com reported on October 2, 2002 that British researchers have made an important breakthrough towards a completely secure wireless communications system. Recent experiments transmitted encoded photons of light over more than 23 km (14 mi.) horizontally through the air. Transmissions of this type are fundamental to global key-distribution networks based upon quantum cryptography via satellite.

Quantum cryptography is not new. Experiments and commercial applications within fiber optics are well known. The method produces a guaranteed secure encryption key which is identical for both the sender and the receiver. This key is then used to encrypt and decrypt messages sent using conventional equipment (via radio waves, microwaves, wire-lines or whatever mode is suited for any given communications system).

Fiber optic quantum transmissions have reached distances of 60 km (37 mi.), but this new advance moves this form of cryptography out of the ground and into the air.

Through-the-air transmission offers a particular advantage. As with fiber optic transmission, both the sender and the receiver immediately detect any potential eavesdropper, but line-of-sight, open-air communication narrows the

search to an easy-to-access region – somewhere in plain sight between the sender and the receiver. On the down side, however, fog, smoke, a cloud or a bird could also disrupt transmissions.

Currently, these types of experiments occur at night to reduce interference from ambient light, but refining of the system with the introduction of light filtration may produce acceptable results during daylight hours.

Recent reports indicate transmissions of pulsed polarized single photons in a low light level communications system are not designed for transmission of messages. Their current application uses photons for building encryption keys intended for optical links to low-Earth orbit (LEO) satellites.

The key cannot be intercepted – not even a portion of it. Its basis is not the result of mathematicians using super-computers engineered with complex equations crunching pseudo-random numbers. Instead, the key is produced by the sheer randomness of physics. Some photons make it from sender to receiver – and some are lost. Only the photons completing the trip from source to target are used for creating the key.

Encoding data onto photons is accomplished using the spin given to each photon. A photon acts as a bit, representing either a “1” or a “0”, depending upon whether its spin is clockwise or counterclockwise. The spin is initiated and recorded by the sender.

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is \$300 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\$350 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.

We provide discounts to educational institutions and small businesses (less than 10 employees).

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

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

[www.cnp-wireless.com/
prices.html](http://www.cnp-wireless.com/prices.html)

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due...

November 15th, 2002.

Future Topics

802.11 Wireless LAN “Hotspot” Roaming Security • Wireless VPNs • Wireless Flash Memory Security • Radius for Wireless • Public Keys & Wireless • Security Issues in Ad hoc Wireless Networks • Latest in Watermarking

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone:** 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnp-sales@cnp-wireless.com **Web:** www.cnp-wireless.com/wsp.html **Subscriptions:** \$300 for delivery in the USA or Canada, US\$350 elsewhere. **Payment:** accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery:** Email or 1st class mail. **Back Issues:** Available individually for \$35 in the US and Canada and US\$40 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. Call for rates to allow more copies.

Technical Editor and Illustrator:
Les Owens.

Article Sourcing: Tim Kridel.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Each photon is paired with the time at which it was sent, and to build the key, the receiver utilizes only those photons having time and spin exactly matching one of the records sent (over a wireless connection, for instance) from the sender. Both sender and receiver hold records showing the time and spin for every encoded photon that was sent, but photons not verified as “received by the receiver” are deleted. The end result is a matching data sequence at both ends, and this data is used by each to produce identical keys.

Using the methods of these experiments, researchers are working toward a quantum cryptography system sending signals from earth-bound to air-borne or orbiting systems (e.g., LEOs). The available information indicates these were limited trials, and the practical application – beaming up to LEO systems – has yet to be tried, and a critical next step – secure transmissions to other LEOs ranging up to 1000 km (620 mi.) away – is not yet possible, although researchers are confident a

solution may develop within six months. If all goes well, through-the-air transmission may then enable two ground-based systems to reap the benefits of quantum cryptography, even when they are separated by very large distances.

Further information on this topic is available at:

www.cipherwar.com/news/01/dera_satellites.htm

www.quiprocone.org/pressrelease_JRarity.htm1/dera_satellites.htm

More NIST Documents

The National Institute of Standards and Technology (NIST) recently announced the release of draft **Special Publication, 800-38B, Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode**. The RMAC authentication mode allows for the generation and use of a message authentication code (MAC) on specified

input data. The MAC can provide assurance of the authenticity of the source of data and the integrity of the data.

NIST is accepting comments on 800-38B until December 2, 2002. Public comments may be sent to the following email address:

EncryptionModes@nist.gov

The 800-38B publication is another in the series of special publications on cryptographic modes. In the 800-38A publication, five confidentiality modes are specified for use with any FIPS-approved block cipher (e.g., AES). The modes in SP 800-38A are updated versions of the ECB (Electronic Code-book), CBC (Cipher Block Chaining), CFB (Cipher Feedback), and OFB (Output Feedback) modes that are specified in FIPS Publication 81 for the Data Encryption Standard (DES). Further information on the development of block cipher modes of operation is available at the [modes home page](#).

Upcoming Wireless Security and Fraud Conferences & Events

The following are some upcoming conferences and security events that may be of interest to the wireless and network security practitioners.

IASTED International Conference on Communications and Computer Networks

4th– 6th November 2002

Massachusetts Institute of Technology
Cambridge, MA

www.iasted.org/conferences/2002/cambridge/ccn.htm

SANS Minneapolis

4th – 9th November 2002

Hyatt Regency Minneapolis
Minneapolis, MN

www.sans.org/Minneapolis

29th Annual Computer Security Conference & Exhibition

11th – 13th November 2002

Hilton Chicago Towers
Chicago, Illinois

www.gocsi.com

SMS 2002

12th – 14th November 2002

Amsterdam Hilton
Amsterdam

www.iir-conferences.com

Homeland Security Critical Issues Forum

14th – 15th November 2002

Omni Sheraton Hotel
Washington, DC

www.wow-com.com

ACM 2002 Conference on Computer Supported Cooperative Work

16th – 20th November 2002

Hyatt Regency New Orleans
New Orleans, LA

www.acm.org/cscw2002

Comdex Fall 2002

16th – 22nd November 2002

Las Vegas Convention Center
Las Vegas, NV

www.comdex.com/fall

2002 Mobile Enterprise Strategies Seminar

20th November 2002

San Francisco, CA

www.brainstorm-group.com/bsgweb/index.asp?conf=6310733670

Cyber-Security in the Financial Services

20th – 22nd November 2002

Crowne Plaza
New York, NY

secure.imn.org/%7Econference/im/index2.cfm?sys_code=21120cybersecurity&header=on

802.11 Planet Conference & Exposition

27th – 28th November 2002

Santa Clara Convention Center
Santa Clara, CA

www.jupiterevents.com/80211/fall01/agenda2.html

NIST also announced the following documents in October:

DRAFT NIST Special Publication 800-36, *Guide to Selecting IT Security Products*

DRAFT NIST Special Publication 800-35, *Guide to IT Security Services*

DRAFT NIST Special Publication 800-4A, *Security Considerations in Federal Information Technology Procurements*

These may also be downloaded from the NIST web-site.

3GPP2 Security Algorithms

*Sarvar Patel and Marcus Wong
Lucent Technologies*

Various cryptographic functions are needed for establishing the security association between a user and the network and for protecting a session from eavesdropping and hijacking. A necessary element for the security of a system is that its cryptographic functions and algorithms be free from any weaknesses. Designing secure algorithms remains a challenging art. Although progress has been made, over the last two decades, in understanding the design of newer cryptographic functions and applications assuming the existence of a secure core cryptographic algorithm, the design of the core cryptographic algorithm itself remains part magic and part theory. A disquieting fact remains that a large fraction of the newly designed algorithms are eventually shown to have weaknesses.

Core Algorithms

Following the attacks on various Second Generation (2G) security algorithms, 3GPP2 (an international standards development organization for CDMA2000) decided to adopt a more systematic approach to algorithm design and selection for Third Generation wireless systems. In particular, it was decided that only well-scrutinized and time-tested algorithms were to be considered for adoption. Notably, this was a departure from the break-and-fix

approach that had been in vogue. This led to the adoption of algorithms that have been standardized by NIST (National Institute of Standards and Technology):

- The *NIST standard SHA-1*[7] is used as a core for all authentication, session key derivation, and message integrity functions. SHA-1 is a widely used standard hashing algorithm.
- The *NIST standard Rijndael algorithm*[6] is used as a core in a stream cipher mode for data encryption.

SHA-1 algorithm

The SHA-1 (SHA is Security Hash Algorithm) maps variable length inputs up to 2^{64} bits long into a 160-bit output. The hashing algorithm works by repeatedly invoking the SHA-1 compression function that maps two items – a block (512 bits) of input data and a 160-bit chaining variable – into a 160-bit output. The compression function is believed to be collision-resistant, which in turn can be shown to imply that the hashing function is collision-resistant also. Furthermore, the SHA-1 compression function is also widely believed to be a secure MAC (Message Authentication Code) when appropriately keyed – for example, loading the secret key in the chaining variable as in the HMAC standard [2]. The compression function is also assumed to have some pseudo-random properties. Reference implementation of SHA-1 compression and hashing functions are provided in the ECA (Enhanced Cryptographic Algorithm).

Rijndael algorithm

Rijndael, also known as AES, is the NIST standard block encryption algorithm, and it is a replacement for the aging DES algorithm. Although it can operate with various block sizes and key sizes, the most popular length is 128 bits for both block and key size. There are various modes in which the block cipher can be used to securely encrypt variable length data. Rijndael requires a key scheduling procedure, which expands the 128-bit ciphering key to a greater number of key bits used internally. A reference implementation of Rijndael is provided in the ECA [5].

Cryptographic Functions

Based on the core algorithms, the various cryptographic functions needed for different purposes are described below. The encryption function is used to hide the data, and it obviously uses the Rijndael algorithm. Some of the **AKA Functions** for creating a response to a challenge in the authentication protocol require the MAC property, as do the message integrity functions, HMAC and UMAC. A secure MAC makes it infeasible for an adversary to forge an output on a given input. The message integrity functions require a MAC capable of using inputs of variable length.

Some of the AKA functions require pseudo-random properties to perform random number generation and session key generation. To strengthen security, all AKA functions perform two additional steps:

1. At each application of the SHA-1 compression, only 64 bits are extracted from the 160 bits of compression output.
2. To make the 64 bits dependent on all 160 bits, a special mixing or whitening procedure is performed on the 160-bit compression output before the 64-bit extraction.

The compression function's chaining variable input and message data input are preset as specified by a specific AKA function. As shown in **Figure 3**, to ensure pseudo-randomness of the output, a special post-process whitening procedure [4] – with a modular multiplication and reduction function:

$$(AX+B) \bmod G$$

is applied to the results of compression. A and B are 160-bit values, randomly pre-selected and fixed, while G is the polynomial $T^{160} + T^5 + T^3 + T + 1$ (any irreducible polynomial of degree 160 can be used).

After the whitening is applied, the least significant 64 bits are used as an output of the function. These steps can be repeated as many times as needed to generate the expected number of bits. For example, the function is invoked

Figure 1: Core 3G-AKA (3GPP/3GPP2) Protocol

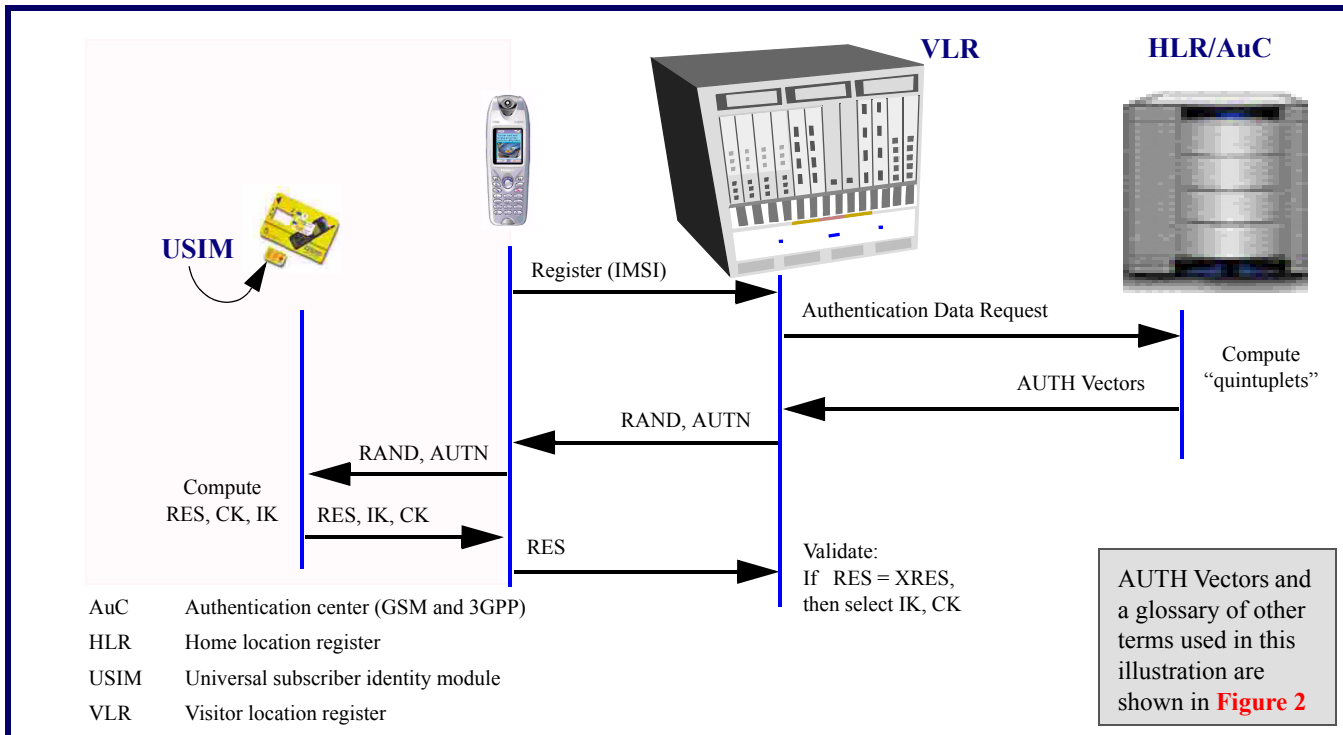
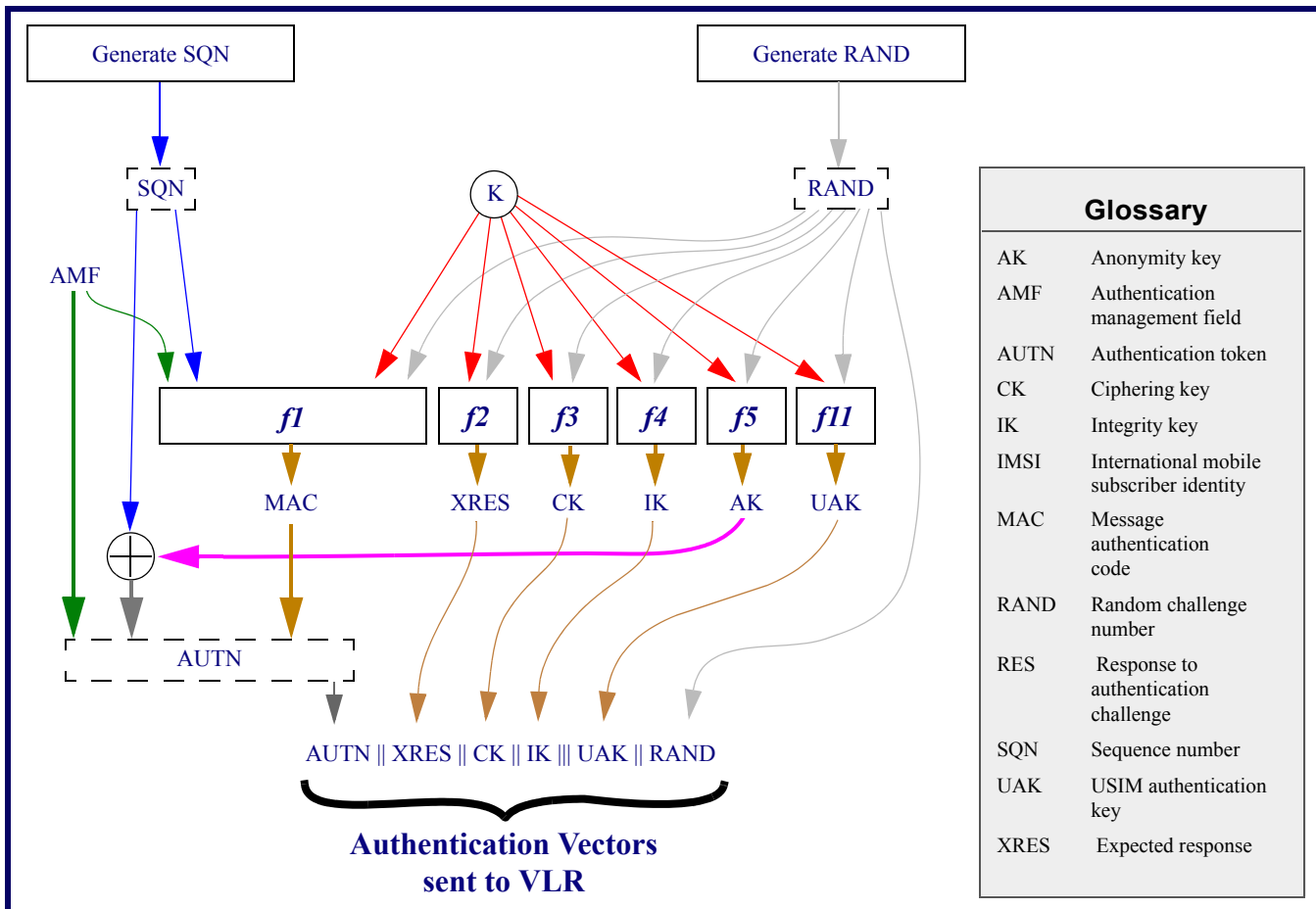


Figure 2: Authentication Vectors



twice to generate a 128-bit result, like CK or IK. The special TYPEID input differentiates one function from another, while the optional FAMILYKEY input may differentiate the same function for different system service providers.

Encryption

The 128-bit Rijndael encryption algorithm is used to create a variable length mask that is XORed (see **Figure 4**) with the signaling or user data bits to be ciphered or deciphered. For packets larger than 128 bits, a counter is used for each invocation of Rijndael encryption to produce different blocks of 128-bits.

The Rijndael is applied to individual layer 3 service bits, including signaling, teleservices, and voice data [1]. After these bits are encrypted, the cipher-text is presented to the lower layers for multiplexing and transmission. The same ciphering key (CK) is used for all instances of encryption, while each instance uses its own crypto-sync value applicable for specific service.

The EHMAL algorithm

Signaling messages carrying important sensitive information and critical commands (e.g., “turn off encryption”) need to be protected from malicious modifications and insertions by outsiders. A MAC based on a secret key (IK) provides such protection. Data that needs to be transmitted is first fed through the key-based MAC algorithm to create a short tag which is then sent to the receiver along with the data. Finally, the receiver also runs the MAC algorithm on the received data, and it checks to see if the calculated tag is equal to the received tag. If they match, the data is accepted; if they do not, it is rejected. Only the sender and the receiver who share the secret key can create the tag; thus, an outsider wanting to send his/her own data or modify the data in transmission would not be able to create the appropriate tag.

The IETF has standardized HMAC as the preferred algorithm for this purpose [2], but it is very inefficient for short signaling messages. For example, to MAC a message shorter than a block, HMAC requires at least two calls to the

basic SHA-1 function and, in general, it may require four calls rather than one. This inefficiency is particularly high for authenticating signaling messages with individual messages fitting within one or two blocks.

EHMAL, an enhanced and provable secure algorithm [3] – see **Figure 5** – was adopted by 3GPP2. Its security is shown to be directly tied to the security of the underlying SHA-1 algorithm. Note: In **Figure 5**, Y denotes a message digest and M denotes a message. This algorithm allows both short and long messages to be authenticated more efficiently than HMAC. In particular, for a message smaller than a block (i.e., 510 bits or fewer), EHMAL only requires one call to the basic SHA-1 function, as shown in **Figure 5** in the right-hand portion, while the processing shown in the left-hand portion is completely skipped. Note that the initial pre-processing to generate the intermediate keys, k1 and k2, is done just once at the beginning of the process call.

UAK and UMAC

The 3GPP2 security architecture mitigates the rogue shell threat (a phone ‘shell’ that captures information from a UIM and continues to use it after the UIM has been removed) by enhancing the core 3G-AK, shown in **Figure 3**. To protect against this rogue shell threat, the shell calculates a MAC first. This is then passed to the UIM. UIM uses UAK (UIM Authentication Key from **f11 – UIM Authentication Key Function**, which is only available at the UIM and is not shared with the shell, like CK and IK) to compute a UIM MAC (or UMAC) on the MAC received from the shell. This UMAC is then passed back to the shell and will become the MAC of a message for over-the-air transmission. This procedure, unique only to 3GPP2, is called the UMAC procedure. Both the shell and UIM use EHMAL to compute MAC of the UIM and MAC of the shell.

AKA Functions

The 3GPP2 Authentication and Key Agreement (AKA) is modeled after the 3GPP AKA procedures, shown in **Figure 1**. All functions, f_n (as shown in **Figure 2**), that support 3GPP2 AKA are

based on the SHA-1 compression function with Whitening post-process. The input Counter value specifies the necessary number of iterations to generate the required number of output bits. Functions differ by the Type Identifier. The value of Family Key can further differentiate these functions between different service providers.

f0 – Random Number Generation Function

f_0 random number generation is based on the SHA-1 compression function, run in a counter mode. Each iteration of the SHA-1 function produces a 160-bit output that is post-processed with the Whitening function, and the 64 Least Significant “hard” bits of it are used as the result. The necessary number of iterations is executed to produce required number of Pseudo-Random bits.

f1 – Message Authentication Code Function

f_1 computes the Message Authentication Code (MACA) that authenticates the received Authentication Vector to the UIM.

f_1^* computes the Message Authentication Code (MACS) of the Resynchronization Message to the Authentication Center. This function is only used when authentication vector’s Sequence Numbers (SQN) are out of synchronization.

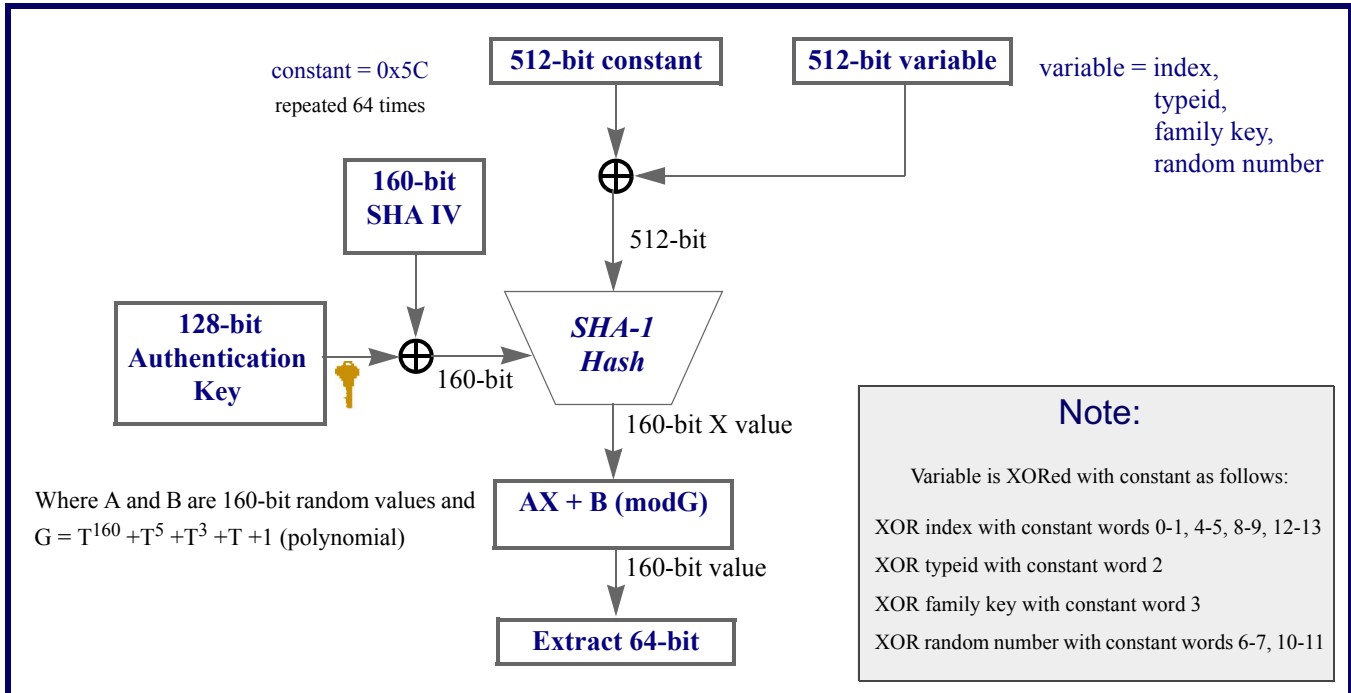
f2 – Challenge Response Function

f_2 is used in the UIM to compute the challenge response (RES) returned to the serving system when the Authentication Vector is processed. It is also used in the Authentication Center to compute the expected challenge response (XRES) included in the Authentication Vector for validation of the RES by the serving system.

f3 – Ciphering Key Function

f_3 is the pseudo-random function used to generate a session Ciphering Key (CK) for information ciphering. This function is also used for generating the Secure Mode Ciphering Key (SMCK) for *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems* (OTASP is described in TIA/EIA/IS-683B, which is the same as 3GPP2 TSG-C document C.S0016-A).

Figure 3: SHA-based 3GPP2 AKA Functions



In addition, f_3 is used for generating a GSM triplet from 2G ANSI-41 SSD-B for one-way roaming from 2G ANSI-41 to GSM MAP.

f_4 – Integrity Key Function

f_4 is the pseudo-random function used to generate a session Integrity Key (IK) for message authentication.

f_5 – Anonymity Key Function

f_5 is the pseudo-random function used to generate an Anonymity Key (AK) for concealing the AV sequence number SQN.

f_5^* is the pseudo-random function used to compute a Resynchronization Anonymity Key (AKS) for concealing the sequence number SQN in Resynchronization Message. It is only used in the re-synchronization procedure when Sequence Numbers are out of synchronization.

f_{11} – UIM Authentication Key Function

f_{11} is the pseudo-random function used to compute the UIM Authentication Key (UAK). This key is used to ensure that the UIM plays a critical part in computing the message authentication code (MAC), and thus it deters the “rogue shell” attack, which is only possible in terminals with a removable UIM.

Conclusion

We have described the main 3GPP2 cryptographic functions. 3GPP2 has taken a very conservative approach in specifying the functions. Only time-tested and well-scrutinized NIST standard algorithms – SHA-1 and Rijndael – are used as core algorithms, and the security of some of the functions can be shown to be directly related to the underlying core algorithm; for example, the security of the EHMACE message-integrity algorithm is related to the security of the SHA-1 compression function. Security is strengthened in the AKA procedures by performing a special whitening procedure on the output of the SHA-1 compression function and by extracting partial bits. These provide a secure foundation for 3G wireless systems.

References

[1]. 3rd Generation Partnership Project 2. *Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems*. 3GPP2 C.S0005-A-1. Oct., 2000. www.3gpp2.org/Public_html/specs/C.S0005-A-1.pdf

[2]. Internet Engineering Task Force. *HMAC: Keyed-Hashing for Message Authentication*. Feb., 1997. ftp.isi.edu/in-notes/rfc2104.txt

[3]. S. Patel. *An efficient MAC for Short Messages*, ePrint Archives, 2001. eprint.iacr.org/2001/097

[4]. S. Patel, Z. Ramzan, and G. Sundaram. *Security for Wireless Internet Access*. Bell Labs Tech. J., 6:2, 74–83.

[5]. TR45 Ad Hoc Authentication Group. *Enhanced Cryptographic Algorithms, Revision A*. Telecommun. Industry Assoc. Nov., 2001. ftp.tiaonline.org/tr-45/tr45ahag/public

[6]. Federal Information Processing Standards Publication 197. *Advanced Encryption Standard (AES)*. NIST. Nov., 2001. csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[7]. Federal Information Processing Standards Publication 180-1. *Secure Hash Standard*. NIST. May, 1993. www.itl.nist.gov/fipspubs/fip180-1.htm

Figure 4: Encryption Architecture in 3GPP2 IS-2000 Standard

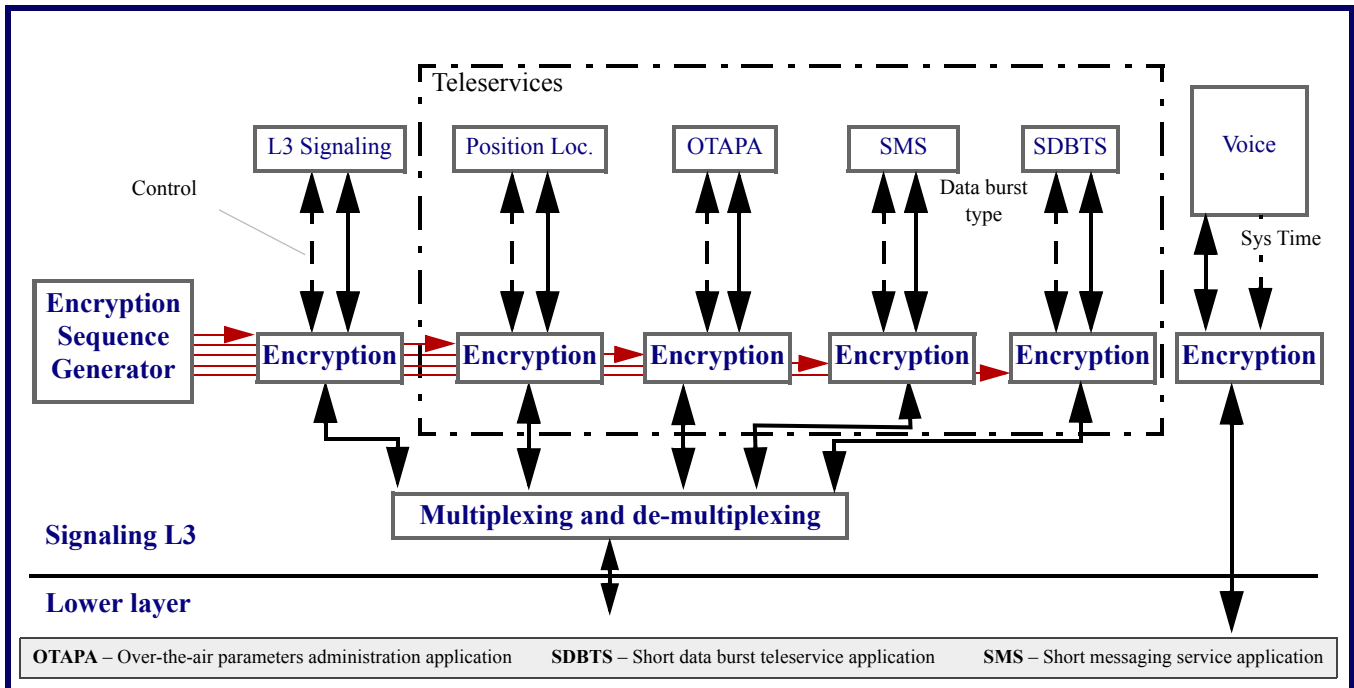
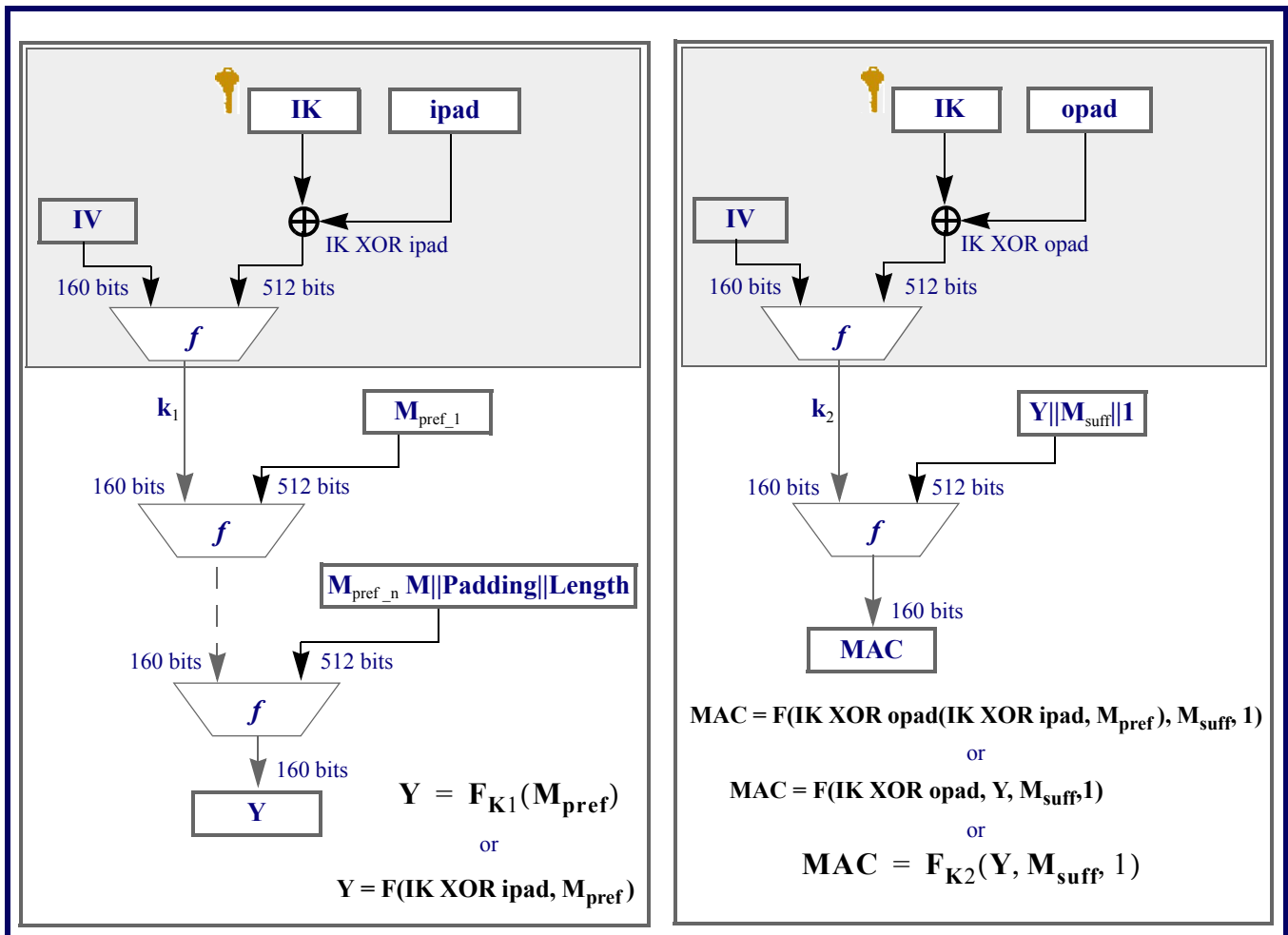


Figure 5: EHMAC Construction



Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents that may be of interest to wireless security practitioners. Each patent includes the patent number, the invention title – linked to the corresponding USPTO webpage – a brief description, the inventor(s), and the assignee (owner). All of these patents were granted in October of 2002.

With the listing below, one can see *who* is doing *what* in the world of inventions. Moreover, it is often instructive to read issued patents, since they include patent claims, specifications, illustrations, detailed descriptions and cited references. Patents often include other references, and these are sometimes useful to broaden one's perspective of wireless communications and security.

If the wording in these is difficult to understand, recognize that the patent abstracts are generally provided in their raw legal-jargon form, straight from an attorney's word-processor. Sometimes we edit the abstracts for readability when the legalese is too impenetrable.

US Patent: 6,463,535

System and method for verifying the integrity and authorization of software before execution in a local platform

A method to verify integrity of information and selectively determine whether the information is authorized to be executed by the platform. The information is downloaded to a platform operating in a pre-boot operational state.

Issued: October 8, 2002

Inventor: Paul Drews

Assignee: Intel Corporation
(Santa Clara, CA)

Interesting Reference:

Braziller, Clay. *Centralized boot systems tackle distributed network security needs.*

Computing Canada, Willowdale.
Sept. 1993. Abstract.

US Patent: 6,463,534

Secure wireless electronic-commerce system with wireless network domain

A method of conducting transactions in a wireless electronic commerce system, where the system comprises a wireless network operator certification authority having a root public key certificate and at least one attribute authority having a digital certificate that is dependent from the root public key certificate. The attribute authority is accessible by a wireless client device via a wireless network. The digital certificate is delivered from the attribute authority to the wireless device. The attribute authority is verified to the wireless client device using the digital certificate and the root public key certificate pre-loaded in the wireless client device under authority of the wireless network operator. An attribute (software, service, right/permission or other content item) is delivered to the wireless client device over the wireless network, and it is ultimately enabled at the wireless client device.

Issued: October 8, 2002

Inventor: Robert Geiger, *et al*

Assignee: Motorola, Inc.
(Schaumburg, IL)

US Patent: 6,463,473

Configuring a wireless computer network to allow automatic access by a guest client device

A network is configured so as to allow access by a client device for a limited period of time. During this period of time, the client device may have access to designated network resources. In some cases, the network may be so configured on-the-fly; that is, it may be configured to allow access by the client device in response to an installation request transmitted by the client device to a network master device. Such an installation request should include a unique identifier associated with the client device. This unique identifier may be broadcast by the client device without a prompt by the network master device. The use of a unique identifier allows for recognizing the guest client, and it further facilitates updating a client table wherein information regarding the available bandwidth for the guest client device may be stored. Upon expiration of the period of time, the guest client may be automatically uninstalling from the network.

Issued: October 8, 2002

Inventor: Rajugopal Gubbi

Assignee: Sharewave, Inc.
(El Dorado Hills, CA)

US Patent: 6,463,464

System and method for pushing information from a host system to a mobile data communication device

A system and method for pushing information from a host system to a mobile data communication device upon sensing a triggering event. A redirector program operating at the host system enables a user to continuously redirect certain user-selected data items from the host system to the user's mobile data communication device, upon detection of one or more user-defined triggering events. The redirector program operates in connection with event generating applications and repackaging systems at the host system to configure and detect a particular user-defined event, and then to repackage the user-selected data items in an electronic wrapper prior to pushing the data items to the mobile device.

Issued: October 8, 2002

Inventor: Mihal Lazaridis, *et al*

Assignee: Research in Motion
Limited (Waterloo, CA)

Interesting References:

1) Smith, *et al.* *Integration of wireless technology in the Defense Inform System Network (DISN).* Military Communications Conference, MILCO Conference Proceedings, IEEE. Vol. 2, pp. 389-393, Oct. 1996.

2) Woo, *et al.* *Pigeon: A Wireless Two-Way Messaging System.* IEEE Journal on Selected Areas in Communications. Vol. 15, No. 8, pp. 1391-1405, Oct. 1997.

US Patent: 6,463,300

Mobile communication terminal allowed to communicate within detachable IC card and method of allowing it to access the network

A mobile communication terminal includes a body and an IC (Integrated Circuit) card. The IC card is mounted on the body. The body includes an input portion, a detecting portion, a first controller, a second controller, and a third controller. The input portion is used to input a first code or a second code. The detecting portion detects whether or not the mounted

IC card is same as an IC card mounted when the mobile communication terminal has previously accessed a network as a previous IC card. The first controller allows the body to be operated in response to the first code from the input portion when the detecting portion detects that the mounted IC card differs from the previous IC card. The second controller allows the body to be operated when the detecting portion detects that the mounted IC card is the same as the previous IC card. The third controller allows the mobile communication terminal to access the network in response to the second code from the input portion after the first controller allows the body to be operated.

Issued: October 8, 2002

Inventor: Hiroyuki Oshima

Assignee: NEC Corporation
(Tokyo, JP)

US Patent: 6,463,286

Method, exchange, telecommunication system and mobile station for temporary selective national roaming at predetermined network operation conditions in a mobile radio communication system

The invention relates to a method, an exchange, a telecommunication system and a mobile station for providing a temporary selective national roaming at predetermined network operation conditions, e.g. at network overload in a mobile radio communication system. A first switching means (MSC/VLR) of a home network (HPLMN) performs a negotiation with a second switching means (MSC/VLR') of another network (VPLMN) which has free capacity to handle mobile stations (MS1-MS4) of the first network (HPLMN) which cannot be handled by said first network (HPLMN) during e.g. an overload condition occurring therein. When e.g. the overload condition occurs, a request message (RM) is first sent to the second switching means (MSC/VLR') in order to enquire whether the second network (VPLMN) has enough free capacity to take over mobile stations (MS1-MS4) from the first network (HPLMN). Thus, it can be ensured that mobile stations (MS1-MS4) of the first network (HPLMN) do not cause an overload condition in the second network (VPLMN) when they have been registered in the second

network (VPLMN) and receive a service therein.

Issued: October 8, 2002

Inventor: Reijo Salminen

Assignee: Telefonaktiebolaget L M Ericsson (publ) (Stockholm, SE)

Interesting References:

1) *Digital cellular telecommunications system (Phase2 +) Mobile-services Switching Center-Base Station System (MSC-BSS) interface*. Layer 3 specification in ETSI GSM 08.08. Nov., 1996.

2) Bremer, Rainer. *Inter-PLMN Handover – An Approach for a Functional Requirement Description*. 1995 Fourth IEEE International Conference on Universal Personal Communications Record, Gateway to the 21st Century. Nov. 6-10, 1995. pp. 442-446.

US Patent: 6,463,271

Portable radio telephone data terminal using CDPD

A portable radio telephone handset including the capability of operating as a data transfer terminal as well as an analog cellular telephone subscriber station. Two modes of operation are available in the handset: An analog cellular communication mode and a Cellular Digital Packet Data (CDPD) mode. A paging function for incoming analog cellular communication is carried out on a CDPD channel. The handset distinguishes between paging signals identifying CDPD mode communications and paging signals identifying analog cellular communications. The handset automatically preempts CDPD communications in favor of analog cellular communications, such as those carried out in an AMPS configuration. To maintain the security of the handset ID, AMPS communications can be set up and controlled using CDPD control channels.

Issued: October 8, 2002

Inventor: Martin Schroeder, *et al*

Assignee: Cirrus Logic, Inc.

Interesting Reference:

Ehrlich, *et al*. *Advanced Mobile Phone Service*. Bell System Technical Journal. Vol. 58, no. 1. 1979, N.Y.

US Patent: 6,463,154

Method for determining temporary mobile identifiers and managing use thereof

In the method for managing the use of temporary mobile identifiers (TIDs), the mobile and the network each store a list of TIDs for the mobile. Newly determined TIDs are added to the respective TID list such that the TIDs are stored in chronological order. To determine a new TID, the network sends a first challenge to the mobile and the mobile sends a second challenge to the network as part of a TID update protocol. The network and the mobile then determine the new TID based on the first and second challenges. As communication between the mobile and the network continues, the respective TID lists are updated. Namely, when either the network or the mobile confirms a TID, the TIDs older than the confirmed TID are deleted from the TID list. In communicating with one another, the mobile will use the oldest TID on its TID list, while the network will use the newest TID on its TID list.

Issued: October 8, 2002

Inventor: Sarvar Patel

Assignee: Lucent Technologies Inc.
(Murray Hill, NJ)

Interesting References:

1) Park, Chang-Seop. *On Certificate-Based Security Protocols for Wireless Mobile Communication Systems*. IEEE Network, IEEE Inc., New York, U.S. Vol. 11, NR. 5, pp. 50-55, XP000699941.

2) Campanini G. *et al*. *Privacy, Security and User Identification in New Generation Radiomobile Systems*. International Conference on Digital Land Mobile Radio Communications. pp. 152-164.

Further Patent Information

To obtain a complete copy of these patents, contact the US Patent and Trademark Office at the address or telephone numbers below:

General Information Services Division
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231

800-786-9199 or 703-308-4357