Keynote Speech at JWIS 2006

Mobile Radio Communications and Wireless Security

Man Young Rhee

Endowed Chair Professor, Kyung Hee University
myrhee@tsp.snu.ac.kr

1. Introduction

This speech presents the evolution and migration from first-generation (1G) to third-generation (3G) mobile radio technologies, with an emphasis on wireless security. 1G, or circuit-switched analog systems, consist of voice-only communication; 2G and beyond systems, comprised of both voice and data communications, largely rely on packet-switched wireless mobile technologies.

The topic of this speech will cover technological development of wireless mobile communications in compliance with each iterative generation over the past decade. Currently, mobile data services have been rapidly transforming to facilitate and to ultimately profit from the increased demand for non-voice services. Through aggressive 3G deployment plans, the world's major operators boast attractive and homogeneous portal offerings in all of their markets, notably in music and video multimedia services. Despite the improbability of any major changes in the next 4-5 years, rapid technological advances have already bolstered talks for 3.5G and even 4G systems. New All-IP wireless systems will come into a position to compete with current cellular networks; Wi-Fi technology, along with WiMax and TDD mode may make it possible for new entrants to compete with incumbent mobile operators.

The speech is separated into six parts and will progress in a systematic manner on wireless mobile communications.

2. 2G Mobile Technologies

There are two major 2G mobile telecommunications standards that have been dominating the global wireless market: GSM, developed at the beginning of the 1990s by the ETSI in Western Europe, and TDMA-136/CDMA IS-95, developed by TIA in North America. Since the GSM standard was originally designed for voice, GSM was ill-suited to data transmission. Although GSM is the most widely used

circuit-switched cellular system for voice communications, GSM networks were not optimised for high-speed data, image, and other multimedia applications and services. The ETSI hence upgraded the GSM standard, albeit still in circuit-switched mode. The HSCSD technology was first deployed to enable higher data rates. GPRS soon followed, introducing packet-switched mode. Lastly, EDGE was introduced to further increase the data speeds provided by GPRS. Currently, most GSM-based networks are expected to evolve 3G UMTS.

Qualcomm developed a mobile communication technology based on the CDMA spectrum-sharing technique. This network technology, which is modulated by codes, is called cdmaOne IS-95A/B and was standardized by TIA. Under the influence of Qualcomm, the IS-95 technology continues to evolve steadily to provide higher data rates, such as 3G CDMA2000 1x networks that were standardized by 3GPP2.

The IS-54, based on the TDMA access mode, was the first North American digital telephony standard. This standard was also adapted for use in wideband PCS networks under the name TDMA-136. The IS-54 was primarily used by the US operators, but limitation in data transfers from the utilization of a relatively narrowband forced its demise in December 2001.

In addition, two other proprietary technologies classified as 2G systems include, NTT DoCoMo's i-mode in Japan and WAP protocol, the de facto standard created by the WAP Forum, which was founded in 1997 through the initiative of Nokia, Motorola, Ericsson, Phone.com, etc. NTT DoCoMo's i-mode is the mobile Internet access system, which provides service over the packet-switched network. The i-mode gives users a new range of capabilities, offering voice and data cellular service in one convenient package The WAP Forum's initial aim was to establish a universal and open standard to provide wireless users access to the Internet. WAP was designed to deliver Internet content by adapting to the features and constrains of mobile phones. WAP technology cannot be exactly defined as 2G system; it was designed work with all wireless network technologies, beginning with a majority of 2G system (GSM, GPRS, PCD IS-95, TDMA-136) and 3G systems. However, with the commercial failure of the launch of WAP at the beginning of 2000, the European industry missed the mobile data service explosion. Only SMS service appeared to offer access to WAP portal via GSM networks. The MMS technology will make it possible to overcome the technological constrains of SMS and to further enhance existing services with SMS. The i-mode service started in February of 1999; WAP 2.0 was released from WAP Forum in August 2001; and M-service Phase 2 has started in GSM-A.

3. 2.5G Mobile Radio Technologies

Second-generation (2G) mobile radio technologies enable voice traffic and limited data traffic, such as SMS, to transmit over wireless. Improvements must be made in order to facilitate high data rate services

that ultimately allow the transmittal and receiving of high quality data and video to and from the Internet. However, the data handling capabilities of 2G mobile systems are limited.

For 2.5G systems, HSCSD in circuit-switched mode was the first step for GSM's evolution in increased data transmission rates, reaching maximum speeds of about 43 Kbps (3 simultaneous GSM circuits running at 14.4 Kbps). The drawback of HSCSD, when compared to GPRS, is the several time slots used in *circuit mode*, whereas GPRS uses several time slots in *packet mode*. HSCSD is considered an interim technology to GPRS, which offers instant connectivity at higher speeds.

GPRS is the evolution of GSM for higher data rates within the GSM carrier spacing. GPRS introduces packet transmission for data services, replacing GSM's circuit-switched mode. EDGE (an upgraded version of GPRS) was designed for a network to evolve its current 2G GSM system to support faster throughput and to give operators the opportunity to understand the new technology prior to the complete 3G rollout. EDGE is a higher-bandwidth version of GPRS, with transmission rates up to 384 Kbps. Such high speeds can aptly support wireless multimedia applications.

ITU defined IMT 2000 program for the 3GPP as well as 3GPP2 as a main part of the 3G technical framework. The primary objective of the standardization activities for IMT2000 is to develop a globally unified standard for worldwide roaming and mobile multimedia services. In order to achieve these goals, the ITU has been striven its maximum efforts in creating harmonized recommendations by backed up such technical forums as the 3GPP and 3GPP2. The ITU-R and ITU-T are the main bodies that produce recommendations for IMT2000. The 3GPP, created in late 1998, is the group responsible for standardizing UMTS with WCDMA technology.

The 3GPP has so far released: Release 99, Release 4, Release 5, and Release 6. Release 99 includes the basic capabilities and functionalities of UMTS. Release 4 was contributed by CWTS and incorporated as WCDMA/TDD, but it was frozen in 2003. Since Release 5 was successfully completed in March 2002, 3GPP is moving toward the next release, Release 6, to further improve performance and enhance capabilities.

The 3GPP2 specifies an air interface based on cdmaOne technology and the cdma2000 interface to increase capability and to enable faster data communication. The technical area of 3GPP2 is similar to that of the 3GPP.

cdmaOne IS-95B is enhanced through the migration from cdmaOne IS-95A. In the non-GSM regions (notably the USA and South Korea), network operators are preparing next-generation wireless systems based on cdmaOne IS-95A/B. The first phase with IS-95A was fully covered in TIA/EIA/IS-95A + TSB74. In late 1997, the second phase with IS-95B brought about improvements in terms of capacity, allowing data transmission at 64 Kbps. The 2.5G equivalent for CDMA operators is a technology called CDMA2000 1x. The IS-95 technology continues to improve to provide higher data rates towards the natural evolution of CDMA2000 1x networks for 3G, i.e., CDMA2000 1xEV-DO and 1xEV-DV, both standardized by 3G PP2, that will be covered in Section 4.

4. 3G Mobile Radio Technologies (Situation and Status of 3G)

3G mobile technologies referred to cellular radio systems for mobile technology. ITU defined the 3G technical framework as a part of the IMT 2000 program. The 3GPP, created in late 1998, is the group responsible for standardizing UMTS at a global level. It was composed of several international standardization bodies involved with defining 3G technologies. TDMA-136 and GSM/GPRS operators plan to use UMTS (3G), which is an advanced version of EDGE(2.5G). GSM/GPRS operators plan to deploy UMTS with WCDMA technology. Unlike CDMA2000, WCDMA will be deployed in the frequency bandwidths identified for 3G, leading some American operators to adopt EDGE. TDMA networks are steadily being replaced with GSM-evolved technology, i.e., from GPRS, to EDGE, and finally to the 3G WCDMA (UMTS) standard.

The 3GPP2 is the international organization in charge of the standardization of CDMA2000, which in turn is the 3G evolution of the IS-95A/B standards. CDMA2000 represents a family of ITU-approved IMT-2000 (3G) standards including, CDMA2000 1x networks, CDMA2000 1xEV-DO, and 1xEV-DV technologies. The first CDMA2000 1x networks were launched in Korea in October 2000 by SK Telecom and LG Telecom. CDMA2000 1xEV-DO was recognized as an IMT-2000 technology in data rates of 2.4Mbps on 1.25 MHz CDMA carrier. Since 1xEV-DO makes use of the existing suite of Internet Protocol (IP), operating systems, and software applications, 1xEV-DO builds on the architecture of CDMA2000 1x network, while preserving seamless backward compatibility with IS-95A/B and CDMA2000 1x. CDMA2000 1xEV-DV provides integrated voice with simultaneous high-speed packet data services at speed of up to 3.09 Mbps. But 1xEV-DV is still in the development stage. The CDMA2000 family of air interfaces operates with an IS-4 network, an IP network, or a GSM-WAP network. This allows operators tremendous flexibility with the network and assures backward compatibility with deployed terminal base.

In June 2000, the Ministry of Postal and Transportation of Japan awarded 3G licences to three mobile operators NTT DoCoMo, KDDI and Vodafone KK (J-Phone) via a comparative bidding process. NTT DoCoMo's i-mode (2G) is the first mobile Internet service in the world with 42 million subscribers at the end of March 2004. NTT DoCoMo commercially launched a WCDMA network based on the UMTS standard in the Tokyo area under the name of FOMA. Since its first launch of the 3G FOMA service in October 2001, new and exclusive services accessible to FOMA subscribers include: video telephony and i-motion's video clip distribution service, as well as i-motion's mail messaging service.

KDDI, unlike its two competitors (NTT DoCoMo and Vodafone KK), opted for 3G CDMA2000 technology. In April 2002, KDDI opened its CDMA2000 1x network by using 3G bandwidths. KDDI began deployment of the 3G version of 1x. KDDI launched its commercial CDMA2000 1xEV-DO services nationwide in the first quarter of 2004. KDDI has offered WIN services based on CDMA 1xEV-DO technology from November 2003. Since March 2004, KDDI has offered a BREW (a new application platform) terminal with Bluetooth technology.

The three major South Korean mobile operators (SK Telecom, KTF, and LG Telecom) provide 2G and 2.5G mobile services, using the Qualcomm developed CDMA IS-95 system and its successor CDMA2000 1x. These three mobile operators have been very quick to set up services based on CDMA2000 1x, thus enabling a maximum bandwidth capacity of 144 Kbps. In fact, SK Telecom was the first operator in the world to launch a CDMA2000 1x service in October 2000. As for 3G technologies, the Ministry of Information and Communication of Korean government decided to grant licences according to the type of technology, either WCDMA or CDMA2000. The Korean government decided to grant WCDMA licences to SK telecom and KTF, and a CDMA2000 licence to LG Telecom. Thus, SK Telecom and KTF, holders of 3G WCDMA licences, are deploying networks based on the CDMA2000 1xEV-DO standard in their existing frequency bandwidths. This resulting system is capable of providing 3G services with a maximum bandwidth of 2 Mbps.

SK telecom was the first in the world to launch a CDMA2000 1xEV-DO network in January 2002, followed by KTF in May 2002. This was one of the very first operators in the world, including KDDI (2003), to launch 3G service. SK Telecom launched the WCDMA service at the end of 2003.

KTF is the mobile subsidiary of KT Corporation. KTF launched services based on CDMA2000 1x technology in June 2001 and on CDMA2000 1xEV-DO technology in May 2002. Deployment uses Qualcomm's BREW platform, but the Java WIPI platform was used by all operators towards the end of 2003. Launch of the WCDMA service started at the end of 2003.

LG telecom is the subsidiary of LG Corporation. Launch of services using CDMA2000 1x technology was in August 2001. LG Telecom is the holder of a 3G licence based on the CDMA2000 standard.

Seven operators control the market for mobile telephony in the USA. Instead of facing open competition between three or even four major mobile operators, the North American market is now structured around two main operators, i.e., AT&T Wireless + Cingular Wireless and Verizon Wireless. This follows the merger between AT&T Wireless and Cingular wireless announced in February 2004 and the less important merger between Verizon Wireless and Qwest Wireless. In response to this situation, other operators may have to join forces in terms of operations and capital.

Verizon wireless is a leader in the USA in terms of number of subscribers; it covers 40 of the 50 key markets in the USA. Launched in January 2002, Verizon Wireless was the first major U.S. operator to commercially provide a CDMA2000 1x network. Verizon Wireless launched its CDMA2000 1xEV-DO broadband access in Washington DC and San Diego in 2003, and plans to continue deploying its market on a national level.

Cingular Wireless is the subsidiary of the regional operators SBC and BellSouth. It originally was the operator of a TDMA-136 network, but Cingular Wireless decided to migrate to GPRS, first launched in March 2001. Cingular Wireless is also the first U.S. operator to launch EDGE in June 2003.

AT&T Wireless is the North America operator which was acquired by the Cingular Wireless in February 2004. AT&T Wireless launched GPRS service in mid 2001 and coverage of all markets was done by the end of 2002. AT&T Wireless launched an i-mode type services called "mMode" on the

GPRS network in April 2002. The EDGE deployment plan was established as of mid 2002 and nationally launched in November 2003. AT&T Wireless announced its UMTS deployment plan at the beginning of 2003, and on 26 December 2003 the company announced the 4 markets (San Francisco, San Diego, Seattle and Dallas) in which the first WCDMA networks were to be deployed by the end of 2004. In partnership with NTT DoCoMo the first UMTS call between New York and Tokyo was carried out on November 12, 2002.

The wireless industry world wide will put their continuous efforts to derive the technology evolution to support even greater data throughput and better network capacity than those offered by 3G. In a 4G environment, aggressive and iterative generation of all wireless mobile communications (a combination of 2G/2.5G/3G) along with Bluetooth and IEEE 802.11 could all coexist for attaining faster data throughput and greater network capacity.

Since IMT 2000 has just been commercialised, new standardization work should be commenced for the system beyond IMT 2000. Those new systems will be expected to provide more sophisticated services to meet the further demands of the wireless community. Overall objectives of the future development of IMT 2000 and of systems beyond IMT 2000 will include new radio access capabilities and a new IP-based core network to be realized for resulting in another phase of harmonization.

Since 3GPP Release-5 of UMTS was almost completed in March 2002, 3GPP is moving toward Release-6 which aims to further improve performance and to enhance capabilities. The interworking between WLAN and UMTS has been proved to be one of keys for providing flexibility when accessing multiple radio resources and also providing mobility between WLAN and the 3G system in various mobile environments.

As one of major applications, MBMS (Multimedia Broadcast Multicast Service) may pioneer a new service which allows broadcast of multimedia messaging and video/music streaming capabilities. HSDPA (High Speed Data Packet Access) will represent a change in WCDMA systems and could be compatible with existing networks. HSDPA may enable packet transmission to make speeds of 8 to 10 Mbps for the downlink in UMTS channels of 5 MHz. With the MIMO function, speeds of 20 Mbps could even be reached for providing the throughput. HSDPA systems will be in a position to compete with Wi-Fi services at certain mobile markets : NTT DoCoMo in Japan, several Western European operators, and Cingular Wireless and Verizon Wireless in the USA.

OFDM (Orthogonal Frequency Division Multiple Access) is being studied as a radio access technology which may drastically increase data rates by using a large number of orthogonal frequencies. It is also foreseen that OFDM could be a promising candidate for what is called the 4G mobile system.

The 3GPP2 has been working on an evolution of CDMA technology to enhance new features. CDMA2000, backed by the USA (primarily by Qualcomm), is the direct successor to cdmaOne IS-95 A/B networks. There are two phases to deploy CDMA2000, that is, CDMA2000 1x and CDMA2000 1xEV. CDMA2000 1xEV is the final stage in the evolution from cdmaOne network to 3G. The transition from 1x to 1xEV is taken place in two states: CDMA2000 1xEV-DO and 1xEV-DV.

CDMA2000 1xEV-DO is the first phase, utilizing a separate carrier for traffic and data. The 1xEV-DO may function on a bi-mode operation (1x for voice and EV-DO for data only). In the end of 2000, a specification for High Rate Packet Data (HRPD) was issued to enhance downlink data transmission. HRPD sometimes called the 1xEV-DO (1x Evolution Data Only), allows mobile terminals to easily access on IP network through a high-speed data communication link. Since the 1xEV-DO was primarily devised for data communication only, another radio channel should be required for speech communication, which led to the development of the 1xEV-DV. CDMA2000 1xEV-DV (1x Evolution Data and Voice) builds on the architecture of CDMA2000 1x while preserving seamless backward compatibility with cdmaOne IS-95 A/B and CDMA2000 1x. CDMA2000 1xEV-DV (was approved by the 3GPP2 in June 2002 and was submitted to ITU for approval in July 2002) provides integrated voice with simultaneous high-speed packet data services such as video, video-conferencing and other multimedia services at speeds of up to 3.09 Mbps. In order to support multimedia services, it is necessary to provide simultaneous speech and data communication using the same carrier frequency.

The systems beyond IMT-2000 may include new radio access capabilities and a new IP-based core network to be realized in the future around 2010. Due to tireless efforts by ITU and 3GPPs, a global consensus has been recognized to further develop a world wide harmonized standard that makes it easier to improve mobile services and to stimulate the mobile market.

5. Cryptographic Protocols Applicable to Wireless Security

In November 1976, the Data Encryption Standard (DES) was adopted as a federal standard and authorized for use on all unclassified US government communications. The official description of DES was published in FIPS PUB 46 on 15 January 1977. The DES algorithm, developed by IBM, was the best proposed standard, even though there was much criticisms on key size and the design criteria on the internal structure of S-box. Nevertheless, DES came to fame as popular security algorithm for the organizations worldwide. In fact, DES has been survived remarkably well over 23 years in spite of intensive cryptanalysis, and it has been a worldwide standard of more then 20 years. After much debate, DES was reaffirmed as a US government standard until 1992 because there was still no alternative instead of DES. The NIST again solicited a review to assess the continued adequacy of DES to protect data. In 1993, NIST formally solicited comments on the recertifications of DES. After reviewing many comments and technical inputs, NIST recommended that useful lifetime of DES would be ended in the late 1990s.

In 2001, the Advanced Encryption Standard (AES), known as the Rijndael algorithm, became as FIPS-proved advanced block cipher algorithm which was developed by Deamen and Rijmen in 1999. AES will become a strong advanced algorithm in lieu of DES. It is likely expected that AES will provide the data security for the communications network and access control systems. AES will provide the algorithm specifications such as the key expansion routine, encryption by cipher and decryption by inverse cipher.

The concept of the Elliptic Curve Cryptosystem (ECC) was introduced by Victor Miller (1985) and Neal Koblitz (1987). The elliptic curve discrete algorithm problem appears to be substantially more difficult and somewhat harder than the existing discrete logarithm problem. Implementations can exploit this difference when providing both faster speed and smaller key size for a given level of security. Providing an equivalent level of security, ECC uses smaller parameters than the conventional discrete logarithm systems. Elliptic Curves (ECs) have been well studied by the mathematicians for many years, and in the latter half of the 20th century it has yielded some very significant results.

All practical public-key systems, like Diffie-Hellman, RSA, ElGamal, Schnorr, DSS, and many other public-key algorithms, exploit the arithmetic properties using large finite groups. For those systems, the security depends directly on the relative difficulty of performing to group operations such as exponentiation vs. discrete logarithm. Computation of exponentiation is much easier than that of its inverse operation, i.e., discrete logarithm. In the commonly used groups, discrete log is hard to compute when the modulus is very large. This makes large exponentiation expensive.

All commercial public-key cryptosystems rely on the difficulty of a discrete log problem. When discrete log gets easier, long bit-lengths are required to keep the algorithms safe. Discrete logs in ordinary prime number fields Z_p are much easier to solve than in elliptic curve fields. Thus, the discrete log problem for ordinary fields has been getting steadily easier due to successive refinement in the Number Field Sieve (NFS) techniques. In contrast, Elliptic Curve discrete log techniques have not seen significant improvement in the past 20 years. This difference accounts for today's reduced key-size requirement for elliptic curves. Cracking RSA has never been proven to be as hard as prime factoring, while factoring has never been proven to be as hard as discrete log. The only way for future breakthroughs is to rely on the best mathematicians to whom we could resort for help. The study of elliptic curves has been yielded some significant results that provide for elliptic curve cryptography. When mathematicians study the points where the elliptic curve exactly crosses the integer coordinates (x,y), it was found that the elliptic curve could provide a version of public-key cryptosystems. We first review the concept of an elliptic curve and then discuss its application to existing public-key algorithms over the finite fields. Elliptic Curves over the finite prime field Z_p or the finite binary field $GF(2^m)$ are particularly interesting because they have the potential to provide faster public-key cryptosystems with smaller key sizes. The elliptic Curve Digital Signature Algorithm (ECDSA) was first proposed by Scott Vanstone in 1992 and was accepted in 1999 as an ANSI standard and in 2000 as IEEE and NIST standards. ECDSA is the elliptic curve signature protocol analogue of DSA specified in DSS. Elliptic Curve Cryptosystems (ECCs) are viewed as elliptic curve analogues to the conventional discrete logarithm cryptosystems in which the subgroup of Z_p^* is replaced by the group of points on an elliptic curve over a finite field. The security of elliptic curve cryptosystems is based on the computational intractability of the elliptic curve discrete logarithm problem.

The second half of Section 5 deals with one-way hash function, HMAC, master secret computation, data expansion function, and pseudo-ransom function. The WTLS Record Protocol requires specification of a suite of algorithms, a master secret, and two peers' random values for secure connection. The

encryption and MAC algorithms are determined by the cipher suite selected by the server and revealed in the server hello message. The key exchange and authentication algorithms are determined by the key-exchange suite and are also revealed in the server hello message. The creation of a shared master by means of the key exchange and the generation of cryptographic parameters from the master secret are of interest to study. For all key exchange methods, the same algorithm is used to convert the premaster secret into the master secret. In order to create the master secret, a premaster secret is first exchanged between two parties and then the master secret is calculated from it. The master secret is hashed into a sequence of secure bytes, which are assigned to the MAC secret, keys, and non-export IVs required by the CipherSpec. The master secret is always exactly 20 bytes in length. The length of the premaster secret will vary depending on key exchange method. The master secret is used to generate shared keys and secrets for encryption and MAC computations. In 1996, Netscape Communications Corporation introduced its own procedure for generating the master secret and the key block.

When RSA is used for server authentication and key exchange, a 20-byte secret value is generated by the client, encrypted under the server's public key, and sent to the server. The server uses its private key to decrypt the secret value. The pre_master_secret is the secret value appended with the server's public key. Both parties then convert the pre_master_secret into the master_secret. There is RSA key exchange with RSA based certificates. The server sends a certificate that contains its RSA public key. The server certificate is signed with RSA by a third party (i.e., CA) trusted by the client. The client extracts server's public key from received certificate, generates a secret value, encrypts it with the server's public key and sends it to the server. The pre_master_secret is the secret value appended with the server's public key. If the client is to be authenticated, it then signs some data with its RSA private key and sends its certificate and the signed data. The key size (bits) is unlimited. Keys smaller than 1024 bits should not be used for RSA and DSA signature operations. The general goal of the key exchange process is to create a pre_master_secret which is known to the communicating parties, but not to the attackers. The pre_master_secret will be used to generate the master_secret. The master_secret is required to generate the certificate verify and finished messages, encryption keys, and MAC secrets.

Completely anonymous sessions can be established using RSA or Diffie-Hellman, or EC Diffie-Hellman for key exchange. With anonymous RSA, the client encrypts a pre_master_secret with the server's uncertified public key extracted from the server key exchange message. The result is sent in a client key exchange message. Since eavesdroppers do not know the server's private key, it will be infeasible for them to decode the pre_master_secret. For the conventional Diffie-Hellman key exchange, both the client and server generate a Diffie-Hellman common secret key which is used as the pre_master_secret, and is then converted into the master_secret. For the EC Diffie-Hellman key exchange, the negotiated secret key is used as the pre_master_secret, and is converted into the master_secret. For the case of ECDH-ECDSA key exchange, the server sends a certificate that contains its ECDH public key. The server certificate is signed with ECDSA by a third party trusted by the client. Depending whether the client is to be authenticated or not, it sends its certificate containing its ECDH public key signed with

ECDSA by a third party trusted by the server, or just its (temporary) ECDH public key. Each party calculates the pre_master_secret based on one's own private key and counterpart's public key received (contained in a certificate).

A WTLS connection state is the operating environment of the Record Protocol. An algorithm is required to generate the connection state (encryption keys, IVs, and MAC secrets) from the secure session parameters provided by the handshake protocol. In WTLS, many connection state parameters can be recalculated during a secure connection. This key refresh is performed in order to minimize the need for new handshakes. In the key refresh, the values of MAC secret, encryption key, and IV will change due to the sequence number. The frequency of these updates depends on the key refresh parameter.

A number of operations in the WTLS record and handshake layer require a keyed-Hashing Message Authentication Code (HMAC) which is a secure digest of some data protected by a secret. An HMAC mechanism based on a cryptographic hash function is called HMAC. HMAC can be used with a variety of different hash algorithms, namely MD5 and SHA-1, denoting these as HMAC-MD5 (secret, date) and HMAC-SHA-1 (secret, date). Forgery of the HMAC is infeasible without knowledge of the MAC secret.

An HMAC mechanism can be used with any iterative hash functions where data is hashed by iterating a basic compression function on blocks of data. HMAC uses a secret key for computation and verification of the message authentication values. The HMAC is a cryptographic checksum with the highest degree of security against attacks. HMACs are used to exchange information between parties (where both have knowledge of the secret key K), while a digital signature does not require any secret key to be verified for authentication. The security of the HMAC mechanism depends on cryptographic properties of the hash function, the choice of random keys, a secure key exchange mechanism, periodic key refreshment, and good secrecy protection of keys. Since the HMAC construction and its secure use for message authentication are independent from the particular hash function in use, the hash function can be replaced by any other secure iterative hash function. The strongest attack against HMAC is based on the frequency of collisions for the hash function. As an example, consider a hash function like MD5 whose hash code length equals 16 bytes (128 bits). The attacker will need to acquire the correct message authentication tags computed on about 2^{64} = 18,446,744,073,709,551,616 plaintexts. This is impossible task in any realistic scenario for a block length of 64 bytes, because it will take 250,000 years in a continuous 1Gbps link and without changing the secret key K during all this time. This attack could become realistic only if serious flaws in the *collision* behaviour of the hash function are discovered.

The data expansion function, P_hash (secret, data), uses a single hash function to expand a secret and seed into an arbitrary quantity of output. P_hash (secret, seed) is iterated as many times as necessary to produce the required quantity of data. Thus, the data expansion function makes use of the HMAC algorithm with either SHA-1 or MD5 as the underlying hash function.

In the TLS standard, two hash algorithms (for example, MD5 and SHA-1) were used in order to make the Pseudo-Random Function (PRF) as secure as possible. TLS's PRF computation is created by splitting the secret into two halves (S1 and S2) and using one half to generate data with P_MD5 and the other half

to generate data with P_SHA-1. These two expansion results created from mixing the two pseudo-random streams are then XORed to produce the PRF output. S1 and S2 are the two halves of the secret and each has the same length. In order to save resources, WTLS can be implemented using only one hash algorithm. That is,

PRF (secret, label, seed) = P_hash (secret, label || seed)

which should be agreed during the handshake as a part of the cipher spec.

6. Cryptographic Protocols Applicable to Wireless Security

I would like to present the topic relating to the elliptic curve cryptosystems that are frequently referred in the crypto-literature. Figure 1 below illustrates the elliptic curves for two cases.

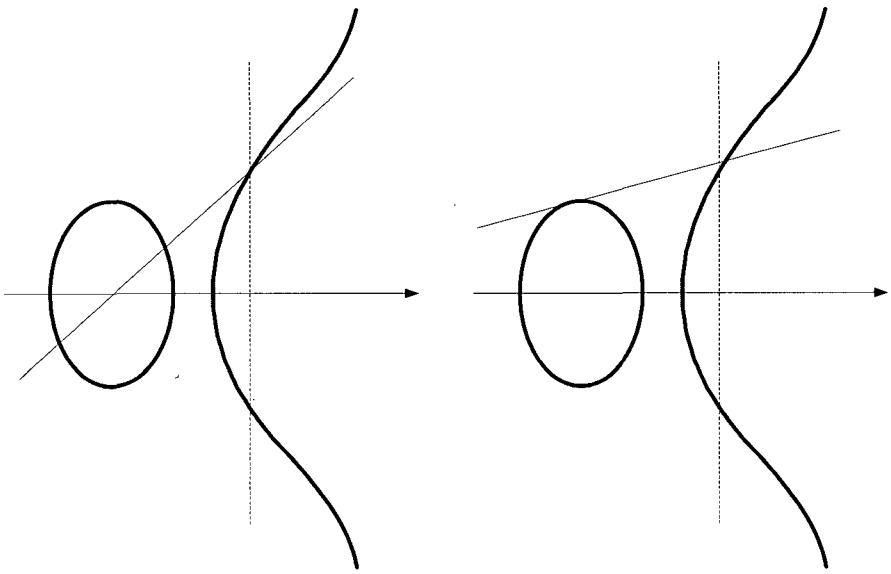

Figure. 1. Elliptic Curve

Computation for the addition or doubling of two points on EC is shown below.

Elliptic curve over the finite prime field Z_p $y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0 \pmod p$	
$P \neq Q$	$P = Q$
$\alpha = \frac{y_2 - y_1}{x_2 - x_1}$	$\beta = \frac{3x_1^2 + a}{2y_1}$
$x_3 = \alpha^2 - x_1 - x_2$	$x_3 = \beta^2 - 2x_1$
$y_3 = \alpha(x_1 - x_3) - y_1$	$y_3 = \beta(x_1 - x_3) - y_1$

Elliptic Curve over the finite binary field $GF(2^m)$ $y^2 + xy = x^3 + ax^2 + b$, $a,b \in GF(2^m)$ and $b \neq 0$
Addition of two points on EC over $GF(2^m)$ $P \neq Q$: $P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$ $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$, $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$ $y_3 = \lambda(x_1 + x_3) + x_3 + y_1$ Doubling of two points on EC ($GF(2^m)$) $P = Q$: $2P(x_1, y_1) = R(x_3, y_3)$ $x_3 = x_1^2 + \frac{b}{x_1^2}$, $y_3 = x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3$

Choosing $a = \alpha^4$ and $b = 1$, the EC equation over the finite binary field $GF(2^4)$ becomes $y^2 + xy = x^3 + \alpha^4 x^2 + 1$.

The points on the elliptic curve are 0 (point at infinity) and the following 15 points:

$(0, 1)$	$(1, \alpha^6)$	$(1, \alpha^{13})$	(α^3, α^8)	(α^3, α^{13})
(α^5, α^3)	(α^5, α^{11})	(α^6, α^8)	(α^6, α^{14})	(α^9, α^{10})
(α^9, α^{13})	(α^{10}, α)	(α^{10}, α^8)	$(\alpha^{12}, 0)$	$(\alpha^{12}, \alpha^{12})$

The order of the EC curve is 16 = #EC ($GF(2^4)$).

D-H Key Exchange Algorithm

x,y : Two large integers chosen by User A and B

g: a primitive element of the prime integer p

User A		User B
$X \equiv g^x \pmod p$	⟶	
	⟵	$Y \equiv g^y \pmod p$

Let Z be the negotiated secret key.

$Z \equiv Y^x \pmod p$	$Z \equiv X^y \pmod p$
$\equiv g^{yx} \pmod p$	$\equiv g^{xy} \pmod p$

Example 1 Choose $g = 2$ of $p = 11$.

User A	User B
	$y = 7$
$X \equiv g^x \pmod p$	$Y \equiv g^y \pmod p$
$\equiv 2^5 \pmod{11} \equiv 10$	$\equiv 2^7 \pmod{11} \equiv 7$
$Z \equiv Y^x \pmod p$	$Z \equiv X^y \pmod p$
$\equiv 7^5 \pmod{11} \equiv 10$	$\equiv 10^7 \pmod{11} \equiv 10$

Thus, the negotiated common key is Z = 10.

EC Diffie-Hellman Key Exchange over Z_p

Choose G as a generator of EC

User A		User B
Choose x		Choose y
$X = xG$	⟶	
	⟵	$Y = yG$
$Z = xY$		$Z = yX$
$= x(yG)$		$= y(xG)$

Example 2 Choose a generator G = (2, 7) for EC $y^2 \equiv x^3 + x + 6 \pmod{11}$. Scalar multiplication of a point on EC is simply repeated addition of a point with itself. When letting $x = 2$ and $y = 3$, X = 2G and Y = 3G are computed as follows:

$$X = 2G = G + G = (2, 7) + (2, 7)$$

Since P = Q,

$$\beta \equiv \frac{3x_1^2 + a}{2y_1} (\text{mod } p) \equiv \frac{3 \times 2^2 + 1}{2 \times 7} (\text{mod} 11) \equiv \frac{2}{3} (\text{mod} 11) \equiv 8$$

$x_3 \equiv \beta^2 - 2x_1 \pmod{p} \equiv 64 - 4 \pmod{11} \equiv 5$

$y_3 \equiv \beta(x_1 - x_3) - y_1 \pmod{p} \equiv 8(2 - 5) - 7 \pmod{11} \equiv -31 \pmod{11} \equiv 2$

Thus, 2G = (5, 2)

Y = 3G = 2G + G = (5, 2) + (2, 7)

For P≠Q, $\alpha \equiv \frac{y_2 - y_1}{x_2 - x_1} (\text{mod } p) \equiv \frac{7-2}{2-5} (\text{mod} 11) \equiv -5 \times 4 (\text{mod} 11) \equiv 2$

$x_3 \equiv \alpha^2 - x_1 - x_2 \pmod{p} \equiv (4 - 5 - 2) \pmod{11} \equiv 8$

$y_3 \equiv \alpha(x_1 - x_3) - y_1 \pmod{p} \equiv (2(5 - 8) - 2) \pmod{11} \equiv -8 \pmod{11} \equiv 3$

Hence, 3G = (8, 3).

Continuing in this way, the remaining multiples are evaluated as shown below:

G = (2, 7), 2G = (5, 2), 3G = (8, 3), 4G = (10, 2), 5G = (3, 6), 6G = (7, 9),
7G = (7, 2), 8G = (3, 5), 9G = (10, 9), 10G = (8, 8), 11G = (5, 9), 12G = (2, 4).

User A's computation:

Z = x(yG) = 2(3G) = 2(8, 3) = (8, 3) + (8, 3)

since P=Q,

$$\beta \equiv \frac{3x_1^2 + a}{2y_1} (\text{mod } p) \equiv \frac{3 \times 64 + 1}{2 \times 3} (\text{mod} 11) \equiv \frac{193}{6} (\text{mod} 11) \equiv 1$$

$x_3 \equiv \beta^2 - 2x_1 \pmod{p} \equiv -15 \pmod{11} \equiv 7$

$y_3 \equiv \beta(x_1 - x_3) - y_1 \pmod{p} \equiv (8 - 7) - 3 \pmod{11} \equiv -2 \pmod{11} \equiv 9$

Thus, Z = (x_3, y_3) = (7, 9)

User B's computation:

Z = y(2G) = 3(2G) = (2G + 2G) + 2G = P + Q

For P = (2G + 2G),

$$\beta \equiv \frac{3x_1^2 + a}{2y_1} (\text{mod } p) \equiv \frac{76}{4} (\text{mod } 11) \equiv 19 (\text{mod } 11) \equiv 8$$

$$x_3 \equiv \beta^2 - 2x_1 (\text{mod } p) \equiv (64 - 10) (\text{mod } 11) \equiv 10$$

$$y_3 \equiv \beta(x_1 - x_3) - y_1 (\text{mod } p) \equiv (8(5 - 10) - 2) (\text{mod } 11) \equiv 2$$

Thus, $Z = (10, 2) + (5, 2)$

Since $P \neq Q$, $\alpha \equiv \frac{y_2 - y_1}{x_2 - x_1} (\text{mod } p) \equiv \frac{2-2}{5-10} (\text{mod } 11) \equiv 0$

$$x_3 \equiv \alpha^2 - x_1 - x_2 (\text{mod } p) \equiv -15 (\text{mod } 11) \equiv 7$$

$$y_3 \equiv \alpha(x_1 - x_3) - y_1 (\text{mod } p) \equiv -2 (\text{mod } 11) \equiv 9$$

$$Z = (x_3, y_3) = (7, 9)$$

Thus, it had shown that the negotiated common key is $Z = (7, 9)$.

EC Diffie-Hellman Key Exchange over GF(2^m)	
Select the base point (generator) G	
User A	**User B**
Choose x_A from $1 \leq x_A \leq n$	Choose x_B from $1 \leq x_B \leq n$
Compute $X = x_A G$	Compute $Y = x_B G$
A sends X to B	B Sends Y to A
Compute the Common Keys	
$K = x_A Y = x_A(x_B G)$	$K = x_B X = x_B(x_A G)$

Example 3 Consider an EC equation $y^2 + xy = x^3 + \alpha^4 x^2 + 1$ for $a = \alpha^4$ and $b = 1$

Let the base point (generator) be G= (α^6, α^8)

User A:

Choose $x_A = 2$ from $1 \leq x_A \leq 15$.

Compute $X = x_A G = 2G = (\alpha^6, \alpha^8) + (\alpha^6, \alpha^8)$

$$x_3 = (\alpha^6)^2 + \frac{1}{(\alpha^6)^2} = \alpha^{12} + \alpha^3 = \alpha^{10}$$

$$y3 = (\alpha^6)^2 + \left(\alpha^6 + \frac{\alpha^8}{\alpha^6}\right)\alpha^{10} + \alpha^{10} = \alpha^8$$

$$X = (\alpha^{10}, \alpha^8)$$

A sends $X = (\alpha^{10}, \alpha^8)$ to B

User B:

Choose $x_B = 3$ from $1 \le x_B \le 15$.

Compute $Y = x_B G = 3(\alpha^6, \alpha^8)$

$= 2(\alpha^6, \alpha^8) + (\alpha^6, \alpha^8)$

$= X + (\alpha^6, \alpha^8) = (\alpha^{10}, \alpha^8) + (\alpha^6, \alpha^8)$

$$\lambda = \frac{\alpha^8 + \alpha^8}{\alpha^{10} + \alpha^6} = 0$$

$$x_3 = \alpha^{10} + \alpha^6 + \alpha^4 = \alpha^3$$

$$y_3 = \alpha^2 + \alpha^8 = \alpha^{13}$$

Thus, we have

$$Y = (\alpha^3, \alpha^{13})$$

B sends $Y = (\alpha^3, \alpha^{13})$ to A.

Now, the common key K is computed as follows:

User A computes $K = x_A Y$

$K = 2(\alpha^3, \alpha^{13}) = (\alpha^3, \alpha^{13}) + (\alpha^3, \alpha^{13})$

$$x_3 = (\alpha^3)^2 + \frac{1}{(\alpha^3)^2} = \alpha^6 + \alpha^9 = \alpha^5$$

$$y_3 = (\alpha^3)^2 + (\alpha^3 + \frac{\alpha^{13}}{\alpha^3})\alpha^5 + \alpha^5$$

$$= \alpha^6 + \alpha^8 + \alpha^{15} + \alpha^5 = \alpha^{11}$$

$K = (\alpha^5, \alpha^{11})$

User B computes the common key $K = x_B X$.

$K = 3(\alpha^{10}, \alpha^8) = (\alpha^{10}, \alpha^8) + (\alpha^{10}, \alpha^8) + (\alpha^{10}, \alpha^8)$

$$x_3 = (\alpha^{10})^2 + \frac{1}{(\alpha^{10})^2} = \alpha^5 + \alpha^{10} = 1$$

$$y_3 = (\alpha^{10})^2 + (\alpha^{10} + \frac{\alpha^8}{\alpha^{10}}) + 1 = \alpha^5 + \alpha^{10} + \alpha^{13} + 1 = \alpha^{13}$$

$K = (1, \alpha^{13}) + (\alpha^{10}, \alpha^8)$

$$\lambda = \frac{\alpha^{13} + \alpha^8}{1 + \alpha^{10}} = \alpha^{13}$$

$$x_3 = \alpha^{26} + \alpha^{13} + 1 + \alpha^{10} + \alpha^4 = \alpha^5$$

$$y_3 = \alpha^{13}(1 + \alpha^5) + \alpha^5 + \alpha^{13} = \alpha^3 + \alpha^5 = \alpha^{11}$$

$K = (\alpha^5, \alpha^{11})$ as expected.

Thus, the secret common key (i.e., session key) has been exchanged between A and B.

RSA Signature Algorithm

p and q: Two large primes (secret)

$n = p \times q$: A composite integer (public)

$\phi(n)$: lcm $(p-1, q-1)$ (a positive number)

Key-pair generation:

e: User B's public key, relatively prime to $\phi(n)$

d: User B's private key, coprime to $\phi(n)$

$d \equiv e^{-1} \pmod{\phi(n)}$ from $ed \equiv 1 \pmod{\phi(n)}$

Encryption: (encrypt the message m with B's public key)

$c \equiv m^e \pmod{n}$ (signature, i.e., encrypted ciphertext)

Decryption: (decrypt the ciphertext c with B's private key)

$m \equiv c^d \pmod{n}$

Example 4 Given $p = 11$ and $q = 17$

$n = p \times q = 11 \times 17 = 187$

$\phi(n) = \text{lcm}(p-1, q-1) = \text{lcm}(10, 16) = 80$

Key Generation:

Take User B's public key $e = 27$. User B can then compute his private key as follows:

$27d \equiv 1 \pmod{80}$

$d \equiv 81 / 27 = 3$ (User B's private key)

Encryption:

Suppose user A chooses the message as $m = 55$.

Encrypt m with B's public key e:

$c \equiv m^e \pmod{n}$

$\equiv 55^{27} \pmod{187} = 132$

This is the signature to be sent to User B.

Decryption:

Upon received the ciphertext c, User B decrypts c with his private key d as follows:

$m \equiv c^d \pmod{n}$

$\equiv 132^3 \pmod{187} = 55$

Thus, the message m is decrypted.

EC RSA Signature Algorithm

EC curve: $y^2 \equiv x^3 + b$ for $a = 0$.

p and q : Two large primes satisfying $p \equiv q \equiv 2 \pmod 3$

n: $p \times q$

N_n: lcm (#E(0, b, p), #E(0, b, q)) ≡ lcm (p+1, q+1)

Key Generation:

e: Public key such that gcd(e, N_n) = 1 (coprime)

d: Private key calculated from $ed \equiv 1 \pmod{N_n}$

Encryption: (User A)

M(m_x, m_y): This message should be a point on the elliptic curve E(0, b, n) and m_x, $m_y \in Z_p$. b can be calculated from $b = y^2 - x^3$.

$C \equiv eM$ over E(0, b, n) and send it to User B

Decryption: (User B)

User B decrypts $C(c_x, c_y)$ with

$M \equiv dC$ over E(0, b, n)

Example 5 Consider the elliptic curve $y^2 \equiv x^3 + 1 \pmod{11}$ for $a = 0$ and $b = 1$.

Choose $p = 11$ and $q = 5$ to be satisfied by $11 \equiv 5 \equiv 2 \pmod 3$.

$n = p \times q = 11 \times 5 = 55$

$N_n = N_{55}$ = lcm (p+1, q+1) = lcm (12, 6) = 12

Choose $e = 5$ (encryption key) such that gcd (5, 12) = 1.

d (private key) can be calculated from $d \equiv 5^{-1} \pmod{12} = 5$.

Choose an message $M(2, 3)$ in E(0, b, p) = E(0, 1, 11) : $y^2 \equiv x^3 + 1 \pmod{11}$

Encryption:

$C \equiv eM \equiv 5(2, 3) = (2, 3) + (2, 3) + (2, 3) + (2, 3) + (2, 3)$

For $C_1 = (2, 3) + (2, 3)$, we compute $\beta = 2$, $x_3 = 0$, and $y_3 = 1$, so $C_1 = (0, 1)$

For $C_2 = C_1 + (2, 3) = (0, 1) + (2, 3)$, we evaluate $\alpha = 1$, $x_3 = 54$, and $y_3 = 0$,

hence $C_2 = (54, 0)$

For $C_3 = C_2 + (2, 3) = (54, 0) + (2, 3)$, $\alpha = 1$, $x_3 = 0$, and $y_3 = 54$,

hence $C_3 = (0, 54)$

For $C_4 = C_3 + (2, 3) = (54, 0) + (2, 3) = C$,

$\alpha = 2$, $x_3 = 2$, and $y_3 = 52$, finally $C = (2, 52)$

Decryption:

$M \equiv dC \equiv 5(2, 52) = (2, 52) + (2, 52) + (2, 52) + (2, 52) + (2, 52)$

Let $M_1 = (2, 52) + (2, 52)$, $\beta = 53$, $x_3 = 0$, and $y_3 = 54$, $M_1 = (0, 54)$

$M_2 = M_1 + (2, 52) = (0, 54) + (2, 52)$, $\alpha = 54$, $x_3 = 54$, and $y_3 = 0$,

$M_2 = (54, 0)$

$M_3 = M_2 + (2, 52) = (54, 0) + (2, 52)$, $\alpha = 53$, $x_3 = 2$, and $y_3 = 3$,

We compute $M = (2, 3)$

Thus, the message M is recovered by decryption of the signature C and authentication is proved.

ElGamal Public-key Encryption

Choose p (a prime), $g < p$, and $x < p$ (a private key).

Public key: (p, g, y) where

$$y \equiv g^x \pmod{p}$$

Encryption:

$r \equiv g^k \pmod{p}$

$s \equiv (y^k \bmod p)\,(m \pmod{p-1}) \equiv my^k \pmod{p}$

where k is a random number, relatively prime to $p - 1$, and m is the message.

Decryption:

$$m = s/r^x \pmod{p},\ 0 < m \leq p - 1.$$

Example 6 Choose $p = 11$, $g = 6$, $x = 3$ and $m = 7$.

Compute:

$y \equiv g^x \pmod{p} \equiv 6^3 \pmod{11} \equiv 7$

Public key: $(y, g, p) = (7, 6, 11)$

Private key: $x = 3 < p$

To encrypt the message $m = 7$, first choose $k = 7$ and then compute:

$r \equiv g^k \pmod p \equiv 6^7 \pmod{11} \equiv 8$

$s \equiv (y^k \bmod p)\,(m \pmod p - 1)),\ m < p - 1$

$\equiv 7^7 \times 7 \pmod{11} \equiv 9$

To decrypt the message m, first compute:

$r^x \pmod p \equiv 8^3 \pmod{11} \equiv 6$ and take the ratio:

$$m \equiv \frac{s}{r^x} \pmod p \equiv \frac{9}{6} \pmod{11} \equiv 3 \times 2^{-1} \pmod{11} \equiv 18 \pmod{11} \equiv 7$$

Thus, the message $m = 7$ is completely recovered.

EC ElGamal Encryption over Z_p

Public Key: (Y, G, p)

$Y = xG$

Private Key: $x < p$

k: a random number, relatively prime to $p - 1$

Encryption:

$R = kG$

$S = kY + M$

Decryption:

$M = S - xR$

Example 7 Choose a generator G = (2, 7) that is a base point on EC $y^2 = x^3 + x + 6$ over Z_{11} and picks User B's private key $x = 7$.

Compute first kG, $1 \le k \le 12$.

$2G = (2, 7) + (2, 7)$ for P = Q

$\beta = 8$, $x_3 = 5$ and $y_3 = 2$

Then, 2G = (5, 2)

3G = 2G + G = (5, 2) + (2, 7) for P≠Q

$\alpha = 2$, $x_3 = 8$ and $y_3 = 3$

Then, 3G = (8, 3)

Repeating same processes yields in the following results:

G = (2, 7), 2G = (5, 2), 3G = (8, 3), 4G = (10, 2), 5G = (3, 6), 6G = (7, 9),

7G = (7, 2), 8G = (3, 5), 9G = (10, 9), 10G = (8, 8), 11G = (5, 9), 12G = (2, 4)

Using the above listing, the public key Y can be calculated as follows:

$Y = xG = 7G = 7(2, 7) = (7, 2)$

Public key: $(G, Y = 7G, p)$

User A chooses a random number $k = 3$ and wants to send the plaintext M = (10, 9) to User B by Encryption.

Encryption:

$R = kG = 3(2, 7) = (8, 3)$,

and $S = kY + M = 3(7, 2) + (10, 9) = (3, 5) + (10, 9) = (10, 2)$

User A then sends R = (8, 3) and S = (10, 2) to User B.

Decryption:

User B decrypts the ciphertext to recover the message using the following formular.

$M = S - xR$

$= (10, 2) - 7(8, 3) = (10, 2) - (3, 5)$

$= (10, 2) + (3, 6) = (10, 9)$

Thus, the message (10, 9) is successfully recovered.

Elliptic Curve ElGamal Encryption Over GF(2^m)

Choose the base point G on a Elliptic Curve $y^2 + xy = x^3 + ax^2 + b$ over GF(2^m).

Let M∈EC(GF(2^m)) be the plaintext.

User A		User B
Choose a random number k		Generate a private key x_B
such that $1 \le k \le n$		Compute $Y_B = x_B G$
Encryption:	←	B sends Y_B to A.
Compute $R = kG$, $S = kY_B + M$		
A sends the ciphertext pair (R,S) to B	→	
		Decryption: $M' = S - x_B R$

Example 8 Consider $EC(GF(2^4)) = y^2 + xy = x^3 + a^4x + 1$ for $a = \alpha^4$ and $b = 1$.

Select a generator $G = (\alpha^3, \alpha^8)$ and choose $x_B = 2$.

Compute $Y_B = x_B G = 2(\alpha^3, \alpha^8) = (\alpha^3, \alpha^8) + (\alpha^3, \alpha^8)$

$$x_3 = (\alpha^3)^2 + \frac{1}{(\alpha^3)^2} = \alpha^6 + \alpha^{-6} = \alpha + \alpha^2 = \alpha^5$$

$$y_3 = \alpha^6 + (\alpha^3 + \alpha^5)\alpha^5 + a^5 = \alpha^3$$

$$Y_B = (a^5, a^3)$$

Encryption :

Choose $k = 3$ and the message $M = (\alpha^6, \alpha^8)$.

Compute R = kG = 3(^{3}, ^{8}) = (^{5}, ^{3})+(^{3}, ^{8})

$$\lambda = \frac{\alpha^3 + \alpha^8}{\alpha^5 + \alpha^3} = \frac{\alpha^{13}}{\alpha^{11}} = \alpha^2$$

$$x_3 = \alpha^4 + \alpha^2 + \alpha^5 + \alpha^3 + \alpha^4 = \alpha^2 + \alpha^5 + \alpha^3 = \alpha + \alpha^3 = \alpha^4$$

$$y_3 = \alpha^2(\alpha^5 + \alpha^4) + \alpha^9 + \alpha^3 = 1 + \alpha + \alpha^2 = \alpha^{10}$$

$$R = (\alpha^9, \alpha^{10})$$

Compute S = kY$_B$+M

$$= 3(a^5, a^3) + (a^6, a^8)$$

$$= (\alpha^{10}, \alpha) + (\alpha^6, \alpha^8)$$

$$\lambda = \frac{\alpha + \alpha^8}{\alpha^{10} + \alpha^6} = \frac{\alpha^{10}}{\alpha^7} = a^3$$

$$x_3 = \alpha^6 + \alpha^3 + \alpha^{10} + \alpha^6 + \alpha^4 = \alpha^6$$

$$y_3 = \alpha^3(\alpha^{10} + \alpha^6) + \alpha^6 + \alpha^4 = 1 + \alpha^3 = \alpha^{14}$$

$$S = (\alpha^6, \alpha^{14})$$

A sends the ciphertext (R;S) to B.

Decryption :

$M' = S - x_B R$

$$= (\alpha^6, \alpha^{14}) - 2(\alpha^9, \alpha^{10})$$

$$= (\alpha^6, \alpha^{14}) - (\alpha^{10}, \alpha)$$

Since - $P(x, y)$ = $P(x, x + y)$, we have

$$M' = (\alpha^6, \alpha^{14}) + (\alpha^{10}, \alpha^{10} + \alpha)$$
$$= (\alpha^6, \alpha^{14}) + (\alpha^{10}, \alpha^8)$$

$$\lambda = \frac{\alpha^{14} - \alpha^8}{\alpha^6 + \alpha^{10}} = \frac{\alpha^6}{\alpha^7} = \alpha^{-1} = \alpha^{14}$$
$$x_3 = \alpha^{28} + \alpha^{14} + \alpha^6 + \alpha^{10} + \alpha^4 = \alpha^2 + \alpha^3 = \alpha^6$$
$$y_3 = \alpha^{14}(\alpha^6 + \alpha^6) + \alpha^6 + \alpha^{14} = 1 + \alpha^2 = \alpha^8$$

$$M' = (\alpha^6, \alpha^8)$$

Thus, since M=M′ $= (\alpha^6, \alpha^8)$, the EC ElGamal encryption scheme works well.

DSA signature scheme

Key pair generation:

p: a prime number between 512 to 1024 bits long

q: a prime factor of $p - 1$, 160 bits long

$g \equiv \lambda^{(p-1)/q} \pmod{p} > 1$, and $\lambda < p - 1$

(p, q and g): public parameters

$x < q$: the private key, 160 bits long

$y \equiv g^x \pmod{p}$: the public key, 160 bits long

Signing process (sender):

$k < q$: a random number

$r \equiv (g^k \bmod p) \pmod{q}$

$s \equiv k^{-1} (h + xr) \pmod{q}$

where $h = H(m)$ is a one-way hash function of the message m.

(r, s): signature

Verifying signature (receiver):

$w \equiv s^{-1} \pmod{q}$

$u_1 \equiv h \times w \pmod{q}$

$u_2 \equiv r \times w \pmod{q}$

$v \equiv (g^{u_1} y^{u_2} \pmod{p}) \pmod{q}$

If $v = r$, then the signature is verified.

Example 9

Choose $p = 23$ and $q = 11$ (q is a prime factor of $p - 1$).

Choose $\lambda = 16 < p - 1$ such that $g \equiv 16^2 \pmod{23} \equiv 3$.

Choose the private key $x = 7 < q$:

The public key $y \equiv g^x \pmod{p} \equiv 3^7 \pmod{23} \equiv 2$.

Sender (signing)

Choose $k = 5$.

$r \equiv (g^k \bmod p) \pmod q$

$\equiv (3^5 \bmod 23) \pmod{11} \equiv 13 \pmod{11} \equiv 2$

Assume $h = H(m) = 10$.

$s \equiv k^{-1} (h + xr) \pmod q$

$\equiv 5^{-1} (10 + 7 \times 2) \pmod{11} \equiv (9 \times 24) \pmod{11} \equiv 7$

$(5k^{-1} \equiv 1 \pmod{11}, k^{-1} = 9)$

Receiver (verifying)

$w \equiv s^{-1} \pmod q$

$\equiv 7^{-1} \pmod{11} \equiv 8$

$u_1 \equiv h \times w \pmod q$

$\equiv (10 \times 8) \pmod{11} \equiv 3$

$u_2 \equiv r \times w \pmod q$

$\equiv (2 \times 8) \pmod{11} \equiv 5$

$v \equiv (g^{u_1} y^{u_2} \pmod p) \pmod q$

$\equiv ((3^3 \times 2^5) \bmod 23) \pmod{11}$

$\equiv ((864 \pmod{23})) \pmod{11} \equiv 2$

Since $v = r = 2$, the signature is verified.

Elliptic Curve DSA Signature Scheme over Z_p

User A	User B
Key pair (d, Q)	Verification of (r, s) from User A
d: Private key	Compute:
$Q = dG$: Public key	$w \equiv s^{-1} \pmod n$
Select k (a random integer)	$u_1 \equiv hw \pmod n$
Compute:	$u_2 \equiv rw \pmod n$
$R = kG = (x_1, y_1)$	$X = u_1G + u_2Q = (x_2, y_2)$
Set $r = x_1$	Set $v = x_2$
$s \equiv k^{-1} (h + dr) \pmod n$	Accept the signature if $r = v$.
where $h = \text{SHA-1}(m)$	
Send (r, s) to User B	

Example 10 Consider the elliptic curve $y^2 = x^3 + x + 6$ over Z_{11}. n =13 is the order of the curve. Choose the key pair (d, Q) in which d = 2 (A's private key) and Q = dG = (7, 9) (A's public key). Pick k = 5 (a random integer) and G = (8, 3) (a generator).

User A

R = kG = (5, 2), then r = 5

Assume h = SHA-1(m) = 8

$k^{-1} = 8$, $s \equiv k^{-1}(h + dr) \pmod{13} \equiv 8(8 + 2 \times 5) \pmod{13} \equiv 1$

(s, r) = (1, 5) → User B

User B

$w \equiv s^{-1} \pmod{n} \equiv 1^{-1} \pmod{13} \equiv 1$

$u_1 \equiv hw \pmod{n} \equiv 8 \times 1 \pmod{13} \equiv 8$

$u_2 \equiv rw \pmod{n} \equiv 5 \times 1 \pmod{13} \equiv 5$

$X = (x_2, y_2) = u_1\mathrm{G} + u_2\mathrm{Q}$

$= 8(8, 3) + 5(7, 9)$

$= (5, 9) + (10, 2) = (5, 2)$

$v = x_2 = 5$, $r = 5$

Since $v = r = 5$, the signature verification is accepted.

Elliptic Curve DSA signature scheme over GF(2^m)

Example 11 Select the base point $G = (\alpha^{12}, 0)$. Let $X \in EC(GF(2^4))$ be the plaintext. Choose a prime $n = 17 > 15$.

Signature Generation at User A :

Key pair (d,Q) where $d=2$ is the private key and Q is the public key, $Q = (\alpha^9, \alpha^{10})$.

A chooses a random integer $k=3$ between $1 \le k \le 15$.

A computes $kQ = (x_1, y_1) = 3(\alpha^9, \alpha^{10}) = (\alpha^{10}, \alpha)$

User A converts $x_1 =$ ^{10} into an integer by means of the following integer conversion mapping:

r	x_1
1	$\longleftrightarrow \alpha^0$
2	$\longleftrightarrow \alpha^1$
.	
.	
.	
15	$\longleftrightarrow \alpha^{14}$

For example, when ^{10} is converted into an integer, it would be 11, i.e., $r = 11$.

Suppose the message digest is $h = 8$.

A calculates $s = k^{-1}(h+dr) \pmod n$

$$= 6(8 + 2 \times 11) \pmod{17} = 10$$

A's signature for the message is $(r,s) = (11,10)$.

A sends the signature $(r,s) = (11,10)$ to B.

Signature Verification at User B.

B computes:

$w = s^{-1} \pmod n = 10^{-1} \pmod{17} = 12$

$u_1 = hw \pmod n = 8 \times 12 \pmod{17} = 11$

$u_1 = rw \pmod n = 11 \times 12 \pmod{17} = 13$

Finally, User B computes $X = u_1 G + u_2 Q$

$$= 11(\alpha^{12}, 0) + 13(\alpha^9, \alpha^{10})$$

$$= (\alpha^{10}, \alpha^8)$$

We can again convert ^{10} into an integer . = 11. Since = $r = 11$, the DSA signature is accepted.

I hope this presentation will shed some positive light to all of you in this field. Thank you very much.

<著 者 紹 介>

*** Speaker's Name**
Man Young Rhee (이만영)

*** Affiliations of speaker**
Endowed Chair Professor, Kyung Hee University, Korea

*** Professional Career**

- Endowed Chair Professor, Kyung Hee University (2003-Present)
- Invited Professor, Seoul National Univeristy (1997-2003)
- Professor Emeritus, Hanyang University (1990-Present)
- Professor, Virginia Tech and State University(1964-1971)

*** Publications**

- M. Y. Rhee, *Error Correcting Coding Theory*, McGraw-Hill, New York, NY, 1989.
- M. Y. Rhee, *Cryptography and Secure Communications*, McGraw-Hill, New York, NY, 1994.
- M. Y. Rhee, *CDMA Cellular Mobile Communications and Network Security*, Prentice Hall, Upper Saddle River, NJ, 1998.
- M. Y. Rhee, *Internet Security*, John Wiley & Sons, West Sussex, UK, 2003.
- M. Y. Rhee, *CDMA Cellular Mobile Communications and Network Security*, House of Electronics Industry, Beijing, China, 2001. (English Reproduction)
- M. Y. Rhee, *CDMA Cellular Mobile Communications and Network Security*, Chinese Edition, House of Electronics Industry, Beijing, China, 2002.
- M. Y. Rhee, *CDMA Cellular Mobile Communications and Network Security,* Japanese Edition, Science and Technology Publishing Co., Tokyo, Japan, 2002.

2006년도 한국정보보호학회 학회지 특집호 발간 계획

◈ 한국정보보호학회의 2006년도 특집호는 다음과 같은 주제로 편집, 발간할 예정입니다.
◈ 해당 특집 분야에 관한 의견이 있으시면 주관편집위원에게 연락주시기 바랍니다.
◈ 해당 호의 원고 마감 일은 발간 월의 전월 마지막일까지입니다. 투고를 원하시는 분은 마감 일을 고려하시어 미리 주관편집위원과 상의하여 주시기 바랍니다.
◈ 투고요령에 관한 사항은 본 학회 홈페이지(http://www.kiisc.or.kr/)를 방문하여주시기 바랍니다.

호수	특집호 주제	책임 편집
제16권 1호 (2006. 2)	사이버 공격기술	서동일 팀장(ETRI)
제16권 2호 (2006. 4)	보안상황 인지기술	김상욱 교수(경북대)
제16권 3호 (2006. 6)	보안 칩셋 & SoC 기술	전성익 팀장(ETRI)
제16권 4호 (2006. 8)	연구회 특집 (암호분석)	암호연구회
제16권 5호 (2006. 10)	연구회 특집 (소프트웨어보안)	소프트웨어보안연구회
제16권 6호 (2006. 12)	연구회 특집 (홈네트워크보안)	홈네트워크보안연구회