이산대수에 기반한 표준 키 분배 프로토콜의 응용분야에 관한 연구

김경진*, 오수현*, 김현주*, 원동호*
*성균관대학교 전기전자 및 컴퓨터공학부
e-mail : {kjkim, shoh, hjkim, dhwon}@dosan.skku.ac.kr

Practical use of Standard Key agreement protocols based on Discrete Logarithm

Kyung-Jin Kim*, Soo-Hyun*, Hyun-Joo Kim*, OhDong-Ho Won*
*School of Electrical & Computer Engineering, SungKyunKwan University

요 약

최근 인터넷의 발달로 대량의 디지털 정보를 활용할 수 있는 기반이 성숙됨에 따라 이를 이용한 다양한 서비스가 증가하고 있으며, 이와 더불어 인터넷 상에서 전송되는 메시지에 대한 기밀성을 제공하기 위한 다양한 암호시스템의 사용 또한 증가하고 있다. 그러나, 암호 시스템 내에서 사용되고 있는 키 분배 프로토콜들에 대한 적절한 선택 기준이 미흡한 실정이다. 따라서, 본 논문에서는 표준으로 제정된 이산대수 기반의 키 분배 프로토콜들의 특징을 분석하고 이것을 바탕으로 가장 적합한 응용분야를 제시한다.

1. 서론

최근 컴퓨터와 같은 정보기술의 발달과 더불어 다양한 지식과 정보들이 디지털화되고 있고, WWW(World Wide Web)의 등장으로 인터넷은 대중에게 보다 친숙한 환경을 제공함으로써 이러한 개방형 네트워크 상에서의 디지털 정보 전송을 활성화시키는 계기가 되었다.

그러나, 개방형 네트워크 상에서 전송되는 디지털 정보들은 일반 문서들에 비하여, 무단 절취, 위·변조, 정보의 파기 등의 위험이 훨씬 크기 때문에, 개인의 정보와 컨텐츠의 정보 보호, 인증 등 정보의 암호화에 대한 중요성이 더욱 강조되고 있으며, 최근에는 이러한 문제를 해결하기 위한 다양한 암호 시스템의 사용이 증가하고 있다.

암호 시스템[1]이란 송신자가 보내고자 하는 원래의 메시지(M)를 키(K_e)라는 상대적으로 작은 비밀 정보를 이용하여 암호화($C=K_e(M)$)하여 전송하면 수신자는 수신한 암호문(C)을 대응하는 키(K_d)로 복호화($M=K_d(C)$)하여 원래의 메시지(M)를 얻는 것으로, 키 관리는 암호 시스템의 가장 중요한 분야 중의 하나이며, 그 중에서도 키 분배(Key distribution)는 키 관리의 가장 근본적인 문제이다. 이러한 키 분배 프로토콜의 목적은 두 사용자가 네트워크와 같은 공개 채널을 통해 비밀 정보를 공유하는 것이며, 공유된 비밀 정보는 대칭키 암호 방식의 키로 사용되거나 사용자 인증 시스템 등에 사용할 수 있다.

본 논문에서는 표준으로 제정된 이산대수 기반의 키 분배 프로토콜의 특징을 자세히 분석하고, 각 키 분배 프로토콜들의 특징을 고려하여 가장 적합한 응용분야를 제시한다[2,3,4].

2. 이산대수에 기반한 표준 키 분배 프로토콜

2.1 ANSI X9.42 프로토콜의 키 분배 과정

ANSI X9.42는 이산대수 기반 키 분배 프로토콜에 대한 미국 표준안으로써 6개의 Diffie-Hellman형 키 분배 프로토콜과 2개의 MQV형 키 분배 프로토콜을 정의하고 있다[4].

X9.42의 프로토콜들은 고정 도메인 파라미터와 고정된 키 쌍만을 사용하여 세션키를 설정하는 dhStatic 프로토콜을 기본 방식으로 하며, 이것을 일회용 도메인 파라미터와 일회용 키 쌍을 사용하는 방식으로 변경한 것이 dhEphem 프로토콜이다. dhOneFlow 프로토콜은 사용자 모두 고정 도메인 파라미터를 사용하지만 사용

<표 1> ANSI X9.42 키 분배 프로토콜

프로토콜	사용자	전송정보		세션키 설정과정	세션키
		고정(y)	일회용(t)		
dhStatic	U	$g_s^{x_U}$		$y_V^{x_U}$	$g_s^{x_U x_V} \bmod p_s$
	V	$g_s^{x_V}$		$y_U^{x_V}$	
dhEphem	U		$g_e^{r_U}$	$t_V^{r_U}$	$g_e^{r_U r_V} \bmod p_e$
	V		$g_e^{r_V}$	$t_U^{r_V}$	
dhOneFlow	U		$g_s^{r_U}$	$y_V^{r_U}$	$g_s^{r_U x_V} \bmod p_s$
	V			$t_U^{x_V}$	
dhHybrid1	U	$g_s^{x_U}$	$g_s^{r_U}$	$y_V^{x_U} \| t_V^{r_U}$	$g_s^{x_U x_V} \bmod p_s \| g_s^{r_U r_V} \bmod p_s$
	V	$g_s^{x_V}$	$g_s^{r_V}$	$y_U^{x_V} \| t_U^{r_V}$	
dhHybrid2	U	$g_s^{x_U}$	$g_e^{r_U}$	$y_V^{x_U} \| t_V^{r_U}$	$g_s^{x_U x_V} \bmod p_s \| g_e^{r_U r_V} \bmod p_e$
	V	$g_s^{x_V}$	$g_e^{r_V}$	$y_U^{x_V} \| t_U^{r_V}$	
dhHybridOneFlow	U	$g_s^{x_U}$	$g_s^{r_U}$	$y_V^{x_U} \| y_V^{r_U}$	$g_s^{x_U x_V} \bmod p_s \| g_s^{r_U x_V} \bmod p_s$
	V			$y_U^{x_V} \| t_U^{x_V}$	
MQV2	U	$g_s^{x_U}$	$g_s^{r_U}$	$(t_V(y_V^{t_V'}))^{S_U}$	$g_s^{S_U S_V} \bmod p_s$
	V	$g_s^{x_V}$	$g_s^{r_V}$	$(t_U(y_U^{t_U'}))^{S_V}$	
MQV1	U	$g_s^{x_U}$	$g_s^{r_U}$	$y_V^{S_U}$	$g^{x_V S_U} \bmod p_s$
	V			$(t_U(y_U^{t_U'}))^{x_V}$	

자 U는 일회용 키 쌍을, 사용자 V는 고정된 키 쌍을 이용하여 세션키를 설정하는 1-pass 프로토콜이다. 또한, dhHybrid1 프로토콜은 dhStatic와 dhEphem 프로토콜을 연접한 방식이고, 이것의 도메인 파라미터 설정을 약간 변형한 것이 dhHybrid1 프로토콜이다. 그리고 dhHybridOneFlow 프로토콜은 dhStatic 프로토콜과 dhOneFlow 프로토콜을 접목시킨 방식으로 dhOneFlow 프로토콜과 마찬가지로 1-pass 프로토콜이며, MQV 알고리즘을 사용한 키 분배 방식이 MQV2와 MQV1 프로토콜이다.

지금까지 설명한 각 키 분배 프로토콜에서 사용되는 기호는 다음과 같고, 각 프로토콜들의 세션키 설정에 필요한 고정 데이터, 일회용 데이터, 사용자들의 세션키 설정 과정 및 설정된 세션키는 <표 1>과 같다[4]

[ANSI X9.42 기호 정의]

- p : 유한체 GF(p)를 정의하는 큰 소수
- q : $q \mid p-1$인 소수
- j : p-1의 cofactor, $p-1 = jq$
- g : GF(p)상에서 원시원소
- U : 키 분배 프로토콜의 시행자(initiator)
- V : 키 분배 프로토콜의 응답자(recipient)
- $x_U, x_V / r_U, r_V$: 사용자 U/V의 고정/일회용 비밀키
- $y_U, y_V / t_U, t_V$: 사용자 U/V의 고정/일회용 공개키
- MQV algorithm : $w \equiv \lceil |q|/2 \rceil$

$$t' \equiv (t \bmod 2^w) + 2^w$$

$$S \equiv (r + t'x) \bmod q_s$$

2.2 키 분배 프로토콜의 특징 분석

본 논문에서는 위에서 살펴본 ANSI X9.42의 각 프로토콜들에 대하여, 사용자 U와 V가 공통의 세션키를 설정하기 위하여 필요한 통신 회수, 개체 인증, 키 확인, 묵시적 키 인증과 key freshness를 중심으로 프로토콜의 특징을 분석하였다[5]. 각각의 정의는 다음과 같고, ANSI X9.42 키 분배 프로토콜의 특징을 분석한 결과는 <표 2>와 같다.

- **통신 회수** : 한 사용자의 입장에서 상대방과 세션키를 설정하기 위하여 필요한 통신 회수
- **개체 인증(Entity authentication)** : 키 분배 프로토콜에 참여하고 있는 상대방의 신원을 확인
- **키 확인(Key confirmation)** : 키 분배 프로토콜에 참여한 합법적인 사용자가 자신이 의도한 상대방과 실제로 공통의 비밀 세션키를 공유하였음을 확인
- **묵시적 키 인증(Implicit key authentication)** : 키의 소유 여부는 알려져 있지 않다고 하더라도 키 분배 프로토콜에 참여한 합법적인 상대방만이 공통의 비밀 세션키를 계산할 수 있음을 보장

<표 2> ANSI X9.42 키 분배 프로토콜의 특징

프로토콜	통신 회수	개체 인증	키 확인	묵시적 키 인증	Key freshness
dhStatic	2	-	-	양방향	-
dhEphem	2	-	-	-	양방향
dhOneFlow	1	-	-	일방향	일방향
dhHybrid1	2	-	-	양방향	양방향
dhHybrid2	2	-	-	양방향	양방향
dhHybridOneFlow	1	-	-	양방향	일방향
MQV2	2	-	-	양방향	양방향
MQV1	1	-	-	양방향	일방향

• **Key freshness** : 매 세션마다 설정된 키가 변경됨

3. 응용 분야

키 분배 프로토콜의 목적은 두 사용자가 네트워크와 같은 공개 채널을 통해 비밀 정보를 공유하는 것이며, 공유된 비밀 정보는 대칭키 암호 방식의 키로 사용되거나 사용자 인증 시스템 등에 사용할 수 있다.

따라서, 키 분배 프로토콜의 주요한 응용 분야로는 최근 들어 널리 이용되고 있는 인터넷을 이용한 전자 우편, 전자 상거래와 전자 금융 거래 등이 있다.

각 응용 분야는 기반 환경과 사용 목적에 따라 각기 다른 요구 사항을 만족해야 하므로, 사용되는 키 분배 프로토콜 또한 각 응용 분야의 특징을 고려하여 선택해야 한다. 각각의 응용 환경의 특징 및 만족해야 할 요구 사항은 다음과 같다.

3.1 전자 우편 보안(e-mail 보안)

전자 우편 시스템은 현재 가장 많이 이용되고 있는 인터넷 서비스 중에 하나이다. 전자 우편 시스템에서는 사용자들이 전자 메일 주소와 같은 공개된 정보만으로 자신이 메시지를 보내고자 하는 사용자에게 암호화된 메시지를 전송할 수 있도록 해야하며, 메시지를 보낸 사람만이 동일한 세션키를 계산할 수 있어야 한다.

따라서 전자 우편을 송·수신하고자 하는 사용자들 간에 별도의 사전 키 분배 과정 없이 세션키를 설정할 수 있어야 하고 묵시적 키 인증을 제공하여야 한다.

dhStatic 프로토콜은 이러한 요구 사항을 모두 만족하지만, 고정된 키 쌍만을 이용하여 세션키를 설정하기 때문에, 항상 동일한 세션키가 이용된다는 단점이 있다. 이러한 문제를 해결하기 위해서는 dhOneFlow 프로토콜을 이용하여 송신자 측에서 key freshness에 대한 제어가 가능하도록 할 수도 있다. 그러나 1-pass 프로토콜을 사용하는 경우에는 수신자 측에서 송신자에 대한 묵시적 키 인증을 보장받을 수 없다는 단점이 있으므로, 통신회수의 증가 없이 양방향 묵시적 키 인증을 제공할 수 있는 키 분배 프로토콜을 사용하는 것이 적합하다. dhHybridOneFlow 프로토콜의 경우는 통신회수는 1번이지만, 양방향 묵시적 키 인증과 일방향의 key freshness를 제공하므로, 송신자 측에서 key freshness에 대한 제어가 가능하도록 한다면, 위의 요구 사항을 만족하는 가장 적합한 방식이라고 할 수 있다.

3.2 전자 상거래

전자 상거래(Electronic Commerce)란, 인터넷이나 통신망을 통한 상거래를 의미하며, 종래에는 상거래에 수반하는 서류의 작성과 교환 등을 포괄적으로 전자화하는 전자 자료 교환(EDI)과 같은 의미로 취급되는 일이 많았으나, 최근에는 주로 인터넷을 통한 상거래를 가리키며, 최근 네트워크의 발달로 기업 간 거래에 추가하여 기업이 인터넷을 통해서 일반 고객에게 물품을 판매하거나 서비스를 제공하는 사이버 쇼핑이 폭발적으로 증가하고 있다.

인터넷에서 전자 상거래를 실현하기 위해서는 인터넷이라는 개방형 네트워크의 특성상 사용자들이 전송하는 정보가 의도되지 않은 사람들에게 공개될 수 있는 단점을 극복하기 위한 비밀 보호나 대금 결제 기능이 반드시 필요하며, 이러한 문제를 해결하기 위해 사용자들이 물건을 구입하거나 예약하기 위하여 인터넷 상점에 전송하는 정보를 암호화하여 전송하는 방식을 이용하여야 한다.

이러한 경우, 서버와 사용자 사이에 공유된 비밀키를 이용하여 대칭키 암호 방식으로 암호화하여 전송하거나 서버의 공개키를 이용하여 공개키 암호 방식으로 암호화하여 전송하는 방식을 이용할 수 있는데, 대칭키 암호 방식은 공개키 암호 방식에 비해 암호화와 복호화가 효율적이라는 장점으로 인해 현재 널리 사용되고 있으나, 사전에 서버와 사용자 사이에 공유된 비밀 정보를 설정해야 하므로 키 분배 프로토콜이 반드시 필요하다.

이러한 전자 상거래의 기본적인 요구 사항을 만족하는 키 분배 프로토콜로는 해당 사용자만이 세션키를 계산할 수 있음을 보장할 수 있는 묵시적 키 인증을 제공하고, 일회용 키 쌍을 이용하여 세션키가 매 세션마다 다르게 설정되도록 하는 dhOneFlow, dhHybrid1, dhHybrid2, MQV2 프로토콜이 있다.

또한, 전자 상거래는 기존의 상거래 방식과 달리 사용자들의 익명성이 보장되는 인터넷이라는 매체를 사용하므로 이러한 비 대면 상거래의 특성상 정보를 전송하는 사용자의 신분에 대한 인증을 제공하는 방식이 적합하다. 또한 사용자들이 구매하거나 예약한 상품에 대해 후에 부인할 수 없도록 하는 부인 불가 기능을 제공하고 사용자의 신분에 대한 정확한 개체 인증을 수행하기 위해서는 디지털 서명을 이용하는 키 분배 방식을 이용할 수도 있다. 그러나 디지털 서명을 이용하는 키 분배 방식은 세션키 설정에 많은 계산이 요구된다는 단점이 있다.

3.3 전자 금융 거래

전자 금융 거래란, 인터넷이나 PC 통신으로 가정에서 금융 서비스를 제공받는 것을 의미하며, 최근 전자 상거래와 함께 인터넷 뱅킹(Internet Banking)과 같이 네트워크를 통한 금융 거래가 널리 이용되고 있다. 전자 금융 거래는 전자 상거래와 비슷한 특징을 가지지만 인터넷 상으로 사용자의 계좌 번호나 금액 등과 관련된 정보가 전송되기 때문에 전자 상거래에 비해 보다 강력한 사용자 인증 기능을 제공해야 한다. 따라서, 묵시적 키 인증이나 개체 인증을 제공할 수 있는 키 분배 프로토콜이 적합하며 각 세션마다 세션키가 다르게 설정될 수 있도록 key freshness를 제공하는 방식이 적합하다. 이러한 요구 사항을 만족하는 키 분배 방식으로는 dhOneFlow, dhHybird1, dhHybrid2, MQV2 등이 있다.

또한, 보다 강력한 보안 기능을 제공하기 위해서는 위에서 제시한 요구 사항 이외에도, 사용자의 신분에 대한 확실한 인증을 제공하거나, 메시지를 전송하기 전에 서비스를 이용하는 사용자와 금융 기관 간에 동일한 세션키가 설정되었음을 확인할 수 있어야 한다. 이를 위해서는 개체 인증을 제공하기 위한 디지털 서명 시스템을 이용하는 키 분배 방식이나, 암호화된 메시지를 전송하기 전에 서버와 사용자 사이에 동일한 키가 설정되었는지를 확인하는 키 확인 기능을 제공하는 키 분배 프로토콜을 사용하는 것이 바람직할 것이다.

4. 결론

본 논문에서는 표준으로 제정된 이산대수 기반의 키 분배 프로토콜의 동작 과정 및 특징을 통신 회수, 개체 인증, 키 확인, 묵시적 키 인증, Key freshness를 중심으로 자세히 분석하고, 이것을 바탕으로 각각의 키 분배 프로토콜들의 가장 적합한 응용분야를 제시하였다.

본 논문에서 분석한 ANSI X9.42 프로토콜들은 사용하는 도메인 파라미터나, 키 쌍에 따라서 묵시적 키 인증과 key freshness는 제공하지만, 개체 인증이나 키 확인은 제공하지 않기 때문에, 이러한 기능을 중요 기능으로 요구하는 응용 분야에 대해서는 적합하지 않다.

향후, 좀더 다양한 키 분배 프로토콜들에 대하여 분석함으로써, 응용 분야에 대한 보다 다양한 선택 기준을 제시하고자 한다.

참고문헌

[1] W.Diffie, M.E. Hellman, "New directions in cryptography", IEEE Trans. Inform. Theory, IT-22, 6, pp 644-654, 1976.

[2] IEEE P1363/D13, "Standard Specifications for Public Key Cryptography," 1999.

[3] RSA Laboratories Technical Note v1.4, "PKCS #3 : Diffie-Hellman Key Agreement Standard" , 1993.

[4] ANSI X9.42, "Agreement of symmetric Key on Using Diffie- Hellman Cryptography", 2001.

[5] R.A Rueppel and P.C vanOorschot, "Modern Key Agreement Techniques" Computer communications volume 17 number 7, pp. 458-465, 1994.

[6] W.Diffie, P.C. Oorschot, M.J. Wiener, "Authentication and Authenticated Key Exchange", Designs, Codes and Cryptography, 2, pp 107-125, 1992.

[7] A.Menezes, P. van Oorschot, and S.Vanstone, Handbook of Applied Cryptography, CRC Press, 1997