通信情報保護學會誌
第3卷 第1號, 1993. 3

DSS(DIGITAL SIGNATURE STANDARD)의 소개

한 상 근*

이 글에서는 DSS(Digital Signature Standard)를 소개하고자 한다. DSS는 NIST(National Institute of Standards and Technology)의 Computer Systems Laboratory에서 새로이 제안한 공개 열쇠 Digital Signature이다. 사용 기법은 1985년에 발표된 Taher ElGamal의 Discrete Logarithm 방법이다. 그 제안서 원문은 Federal Register 1991년 8월 30일자에 "A Proposed Digital Signature Standard (DSS)"라는 제목으로 실려 있다. 원래의 주된 목적은, DES(Data Encryption Standard)가 더 이상 안전하지 않게 될 것을 가정하고, 새로운 암호를 미국 연방정부의 주도로 만들자는 것으로 알려져 있다. 어쨌든 DSS 역시 DES가 그랬던 것처럼 공식 승인이 될 때 까지는 꽤 시간이 걸릴 것이다.

이제 먼저 그간의 논의를 소개하고, 그 뒤에 DSS 알고리듬 자체를 소개하기로 하자. 논의의 대부분은,

① RSA와 Discrete Logarithm 중에서 어느 것이 더 우수한가. 안전성과 속도를 말한다. ② DSS를 사용할 때에 쓰이는 커다란 소수를 누가 만들것인가, 즉 정부가 만들어 주는지 아니면 개개인이 만드는지, ③ NIST와 NSA 중에서 어느쪽이 더 힘이 있는가, 즉 DSS를 실제로 어느 기관에에서 만들었는가, ④ NIST와 NSA 중에서 어느쪽이 더 우수한 능력이 있는가, 즉 만일 DSS를 NIST의 주도하에 만들었다면 이 DSS가 안전한가, ⑤ 후진국에 약한 암호만을 판매해서 얻는 이익(후진국의 암호를 미국이 쉽게 해독)과, 다른 선진국이 강한 암호를 판매함으로 인하여 잃게 되는 미국의 해외 수출시장 중에서, 어느것이 더 큰 국가 이익인가, ⑥ 위 ④와 비슷한 것으로, 일반인이 안전한 암호를 사용해서 얻는 개인 비밀의 보호와, 범죄자가 안전한 암호를 사용하기 때문에 일어나는 범인 검거 및 처벌의 어려움 중에서 어느것이 더 큰 국가 이익인가 하는 것 등이다.

1992년 9월의 IEEE Spectrum에 Special Report/Data Security라는 제목으로 나온 기사에 따르면 DSS는 NSA(National Security Agency)가 만들었고, NSA는 암호를 만드는 동시에 암호를 해독하기도 하기 때문에 산업계의 의구심을 불러 일으키고 있다. NIST는 1990년 12월까지는 RSA 공개 암호를 DSS에 사용하려고 했으나 NSA와 협의를 거친 뒤 갑작스레 1991년 8월 30일 DSS에 ElGamal의 Discrete Logarithm을 사용하겠다고 제안했다. 그리고 RSA를 Discrete Logarithm으로 바꾼 이유에 대해서는 IEEE Spectrum이 Background Comment조차도 얻을 수 없었고, 한 사람만이 익명으로

"…that legitimate national security factors had come into play"

* 한국과학기술원 수학과 부교수

라고 말했다고 한다. 정부내의 소식통에 따르면 NIST가 RSA를 사용하지 않기로 결정한 것은 1989년 12월이라고 한다. 그리고 1991년 봄에 NSA가 NIST에 DSS를 제안했다고 한다. 여기서 참고로 말하면 1987년에 제정된 Computer Security Act는 Unclassified Information에 관한 업무 관장권을 Commerce Department의 NIST에 주었다. 따라서 DES에 관한 업무는 NIST의 소관이다. 그러나 Unclassified Information에 관한 NIST의 의지나 실제 영향력이 NSA를 능가하는지는 알려지지 않았다.

1992년 5월 7일 NIST의 Director인 John Lyons가 하원에서 증언한 내용은, DSS를 선택한 가장 큰 이유는 안전성과 특허 사용료 문제라고 한다. 실제로 미국 정부는 DSS를 특허로 신청해 놓고 있다. 그리고 RSA에는 RSA Data Security Inc.의 특허가 걸려 있다.

이런 논의중에 DSS의 Trapdoor가 발견되었다. p를 홀수인 소수라고 하자. p-1이 Smooth하면 소인수 분해를 할 때에 Pollard의 p-1 방법에 의해 p를 찾아내기가 쉽다. 소인수 분해와 마찬가지로, 이때에도 역시 Discrete Logarithm을 계산하기가 쉽다. 그런데 Number Field Sieve를 사용하면 어떤 특정한 형태의 소수들에 대해서는 Discrete Logarithm을 계산하기가 쉽다. 그리고 여기서 문제가 되는 것은 정부 기관에 의해서 주어진 소수가 이런 특정한 형태인지 아닌지를 판별해 내기가 쉽지 않다는 것이다. 어떤 소수에 대해서는 Number Field Sieve를 적용하기가 상당히 쉽다는 지적은 University of Georgia의 Dan Gordon이 NIST에 보낸 의견서에 잘 나타나있다. 이에 대한 대응 방안으로 NIST는 Revised DSS Proposal을 다시 제안한다고 하였으나 필자는 아직 Revised DSS Proposal을 구하지 못했다.

RSA를 왜 채택하지 않았는지 우리가 알지 못하는 중대한 이유가 있을지도 모른다. NIST의 Branstad는

"For patent and export reasons, DSS was preferred over RSA. DSS as specified can't be used for encryption"

라고 했다. Encryption Software는 International Traffic in Arms Regulations의 Munitions Control List에 올라가 있기 때문에 Encryption Software를 수출하려면 State Department의 까다로운 승인절차를 통과해야 한다. NIST의 실제 의도가 무엇이든 Microsoft, IBM, Sun Microsystems 세 회사는 DSS Proposal이 공표된 후에도 RSA를 채택했다. 그리고 Lotus, Digital Equipment, Motorola, Northern Telecom, Exxon, Citicorp, Boeing Computer Services, Dupont, Apple, Novell, General Electric Information Systems 등은 이미 DSS Proposal이 발표되기 이전에 RSA를 채택했었다. 또한 International Standards Organization의 X.500는 Electronic Directories에, 프랑스의 Etebac-5는 French Banking에, 호주의 AS2805.6.5.3는 Digital Signature Standard에, RFC1114는 Internet Privacy Enhanced Mail에 RSA를 포함하는 표준안이다. IBM의 관계자는 하원에서 DSS가 Unproven Methodology에 근거한 것이라고 증언했다. IBM은 DES를 개발한 회사이기 때문에 그 증언은 신중히 고려해 볼 가치가 있다고 생각한다. 이 관계자는 계속해서 DSS를 표준으로 채택하면 많은 회사들이 RSA를 사용하는 기자재를 병행해서 구입해야만 할 것이라고 했다.

이 기사에는 R. Rivest등 RSA를 선호하는 전문가의 반박 의견이 역시 실려있다. R. Rivest는 Massachusetts Institute of Technology의 전산학과 교수이며 또한 International Association for Cryptologic Research의 Director의 한 사람이다. D. Bidzos는 RSA Data Secyrity Inc.의 회장이다. Rivest가 요약한 상황은

"…it seems that NSA is responding positively to othe legitimate concerns that have been raised about the lack of security in the proposed DSS, including the possibility of trapdoors. Their 'patches' to the original proposal may overcome the observed defects. However, some time will be required for the cryptographic community to study and evaluate these proposed changes,".

이다.

한편 미국정부의 Government Computer News

1991년 12월 23일자에는, DSS를 FIPS(Federal Information Processing Standard)로 채택하는데 The Computer Security and Privacy Advisory Board가 반대한다는 Memo가 실려 있다. 이 Memo가 Board의 공식 결정은 아니지만 Board 자체는 미국 정부의 공식 기구이다. 또한 CPSR(Computer Professionals for Social Responsibility)가 1992년 8월 11일자로 하원 법사 위원회 위원장 J. Brooks에게 보낸 장문의 편지 역시 DSS를 충분한 검증없이 FIPS로 채택하는데 반대하고 있다.

DSS를 설명하려면 Secure Hash Standard(SHS)가 필요한데, SHS에 관한 설명은 지면관계상 생략하겠다. 이 소개서에서 우리가 필요로 하는 것은 SHS는 길이가 $<2^{64}$비트인 메세지가 주어졌을 때에 160비트의 Message Digest를 주는 어떤 함수 H라는 것이다. 즉 H는

$$H : \{\text{길이}<2^{64}\text{비트}\} \rightarrow \{160\text{비트}\}$$

인 Secure Hash 함수이다.

이제 DSS로 돌아가자. 우선

p=소수이고 $2^{511} < p < 2^{512}$
(십진법으로 154~155자리)
q=수 p-1의 소인수이고 $2^{159} < q < 2^{160}$
(십진법으로 48~49자리)
h=0 < h < p이고 $h^{(p-1)/1} \bmod p$가 1이 아닌 임의의 수
$g=h^{(q-1)/q} \bmod p$
x=0 < x < q인 수
$y=g^x \bmod p$
m=Sign해야 할 Message
k=0 < k < q인 Random한 수
H=SHS의 one-way hash function

이라고 놓자. 여기서 p, q, g는 공개할 수 있다. 사용자의 비밀 열쇠는 x이고 공개열쇠는 y이다. x와 k는 비밀이다. 여기서 k는 Message를 Sign할 때마다 바꾸어야 한다.

Signature Generation

Message m을 Sign하려면 사용자는 Random한 k를 만들어서

$$r=(g^k \bmod p) \bmod q$$
$$s=(k^{-1}(H(m)+xr)) \bmod q$$

를 계산한다. 여기서 k^{-1}은 mod q로 k의 역원이다. 그러면 r과 s가 Message m의 Signature가 된다. 따라서 사용자는 (m, r, s)를 송신한다.

Signature Verfication

(m', r', s')를 수신하였다고 하자. 수신인은 먼저 $0 < r' < q$이고 $0 < s' < q$인지를 확인해 본다.

만일 위의 확인 과정을 통과하면, 그 다음에는

$$w = (s')^{-1} \bmod q$$
$$u_1 = (H(m')w) \bmod q$$
$$u_2 = r' w \bmod q$$
$$v = (g^{u1} y^{u2} \bmod p) \bmod q$$

를 계산한다. 만일 $v=r'$이면 Signature가 맞다고 확인할 할 수 있다. 그 이유는 다음과 같다. $m=m'$, $r=r'$, $s=s'$라 하자. 그러면

$$v = (g^{u1} y^{u2} \bmod p) \bmod q$$

에서 $y=g^x \bmod p$이므로

$$\begin{aligned} g^{u1} y^{u2} \bmod p &= g^{u1}(g^x)^{u2} \\ &= g^{u1+xu2} \\ &= g^{H(m)w+xrw} \\ &= g^{((m)+xr)w} \end{aligned}$$

이다. 그런데

$$w=s^{-1} \bmod q$$와
$$s=k^{-1}\ (H(m)+xr) \bmod q$$

에서

$$w=k(H(m)+xr)^{-1} \bmod q$$

이다. 따라서

$$\begin{aligned} v &= g^{(H(m)+xr)w} \bmod q \\ &= g^k \\ &= r \end{aligned}$$

이다.

References

1. *NIST, A Proposed Digital Signature Standard(DSS)*, August, 30(1990).

2. *Office of Technology Assessment, Congress of the United States, Defending Secrets, Sharing Data*, 1988.

3. J. Seberry and J. Pieprzyk, Cryptography, *An Introduction to computer Security*, Prentice Hall, 1989.

4. *National Security agency, A Letter to the Questions Raised by Daivd Banisar*, Dated June 10, 1992.

□ 著者紹介

한 상 근 (종신회원)

서울대학교 수학과 졸업(학사)
미국 오하이오 주립대학교 수학과 졸업(박사)
현 재 : 한국과학기술원 수학과 부교수