情報保護學會論文誌
第19卷 第6號, 2009. 12

Diffie-Hellman 가정에 기초한 새로운 대화식 DH 문제와 이를 이용한 Identification 기법*

양 대 헌,[1†] 이 경 희[2‡]
[1]인하대학교, [2]수원대학교

An Interactive Diffie-Hellman Problem and Its Application to Identification Scheme*

DaeHun Nyang,[1†] KyungHee Lee[2‡]
[1]INHA University, [2]University of Suwon

요 약

이 논문에서는 CDH가정에 안전성을 기초로 하는 공격자가 참여하는 새로운 문제를 정의하고 이의 안전성을 증명한다. 이 새로운 문제는 암호 프로토콜의 설계에서 프리미티브로 이용될 수 있다. 이 논문에서는 이 문제의 응용 예로 새로운 identification 기법을 보인다. 또한, 이 문제의 판별 버전(decisional version)에 대해서도 살펴본다.

ABSTRACT

This paper defines a new variation of CDH problem where an adversary interacts with a challenger and proves its security is equivalent to the CDH problem. This new problem is useful in designing a cryptographic protocol. To show the versatility of this problem, we present a new identification scheme. Finally, we show a decisional version of this protocol.

Keywords: Diffie-Hellman Assumption, Interactive CDH, Identification

I. 서론 및 배경

Diffie-Hellman이 공개키 암호시스템의 개념을 발명한 후에 Diffie-Hellman 키 교환의 안전성과 이산대수문제와의 관계를 찾으려는 노력을 오랫동안 해왔지만 답을 찾지 못했다. 결국 Diffie-Hellman Assumption이라는 이름을 붙여서 안전성을 가정하고 이를 여러 암호 알고리즘과 암호 프로토콜에 이용해 왔다[1,2]. DH 가정은 CDH(Computational DH)과 DDH(Decisional DH)으로 나뉘는데, 당연히 CDH를 풀 수 있다면 DDH문제가 풀리지만, 거꾸로는 알려진 바가 없다. 따라서, 각각 CDH 가정 그리고 DDH가정으로 불리운다.

많은 암호 프로토콜의 안전성이 주로 DL (Discrete Logarithm), CDH, DDH 가정에 기반을 두고 있다. 특히 DL, CDH 가정만으로는 안전성 증명이 쉽지 않았었는데, CDH의 판별버전(Decisional Version), 즉 DDH 가정이 이용되기 시작하면서 표준 모델(standard model)에서의 증명이 좀 더 쉬워졌다. DDH를 이용한 대표적인 것으로 Cramer-Shoup의 공개키 암호시스템이 있다[4]. Cramer-Shoup의 암호시스템은 처음으로 DDH 가정을 근거로 표준모델에서 IND-CCA2 (Indistinguishable under Adaptive Chosen Ciphertext Attacker) 증명이 된 공개키 암호시스템으로의 의미가 있다. Decisional DH문제에 관한 Dan Boneh의 소개가

접수일(2009년 7월 13일), 수정일(2009년 9월 16일),
게재확정일(2009년 10월 8일)
* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. (2008-F-036-01, 익명성기반의 U-지식 정보보호기술개발)
† 주저자, nyang@inha.ac.kr
‡ 교신저자, khlee@suwon.ac.kr

ANTS에 실린 적이 있으므로 참고하기 바란다[3]. 또한, Bao 등은 Diffie-Hellman문제의 여러 가지 변형에 대한 안전성을 고찰했고,[5] Pointcheval 등은 이 논문에서 제시한 문제와 비슷한 동기로 대화식 DH 문제를 3자간 패스워드 기반의 인증 프로토콜을 설계하는데 사용했다. 하지만, 이 논문에서 제안하는 것과는 달리 공격자가 선택한 다른 베이시스(chosen basis DH)를 이용한 문제이다.

이 논문에서는 CDH가정에 안전성을 기초로 하는 공격자가 참여하는 새로운 문제를 정의하고 이의 안전성을 증명한다. 이 새로운 문제는 암호 프로토콜의 설계에서 프리미티브로 이용될 수 있다. 이 논문에서는 하나의 응용 예로 이 문제를 직접 이용한 identification 기법을 보인다. 또한, 이 문제의 판별 버전(decisional version)에 대해서도 살펴본다.

II. 대화식 CDH 가정

이 절에서는 공격자에게 제어할 수 있는 약간의 이득을 줌으로써, 다양한 암호프로토콜의 표준 모델 증명에서 이용하기 쉬운 CDH의 변형 문제를 제시하고, 이의 안전성에 대해 살펴본다.

$\mathbb{G}$: 소수 위수 q를 갖는 그룹
q: 소수
p: $rq+1$ 인 소수
g, h는 $\mathbb{G}$의 생성자.
τ: 보안수준 파라미터

2.1 iCDH 가정(Interactive Computational Diffie-Hellman Assumption)

$h=g^s$인 s를 모르는 공격자가 임의로 선택한 m에 대해, 문제출제자가 $(\gamma,\ h^a)$를 주었을 때, 공격자가 $(mg^\gamma)^a$을 $1/2^\tau$보다 큰 확률로 구할 수는 없다. 여기서 γ는 공격자가 m을 제시(commit)한 후에 문제출제자가 선택함에 유의하라.

$$\mathrm{iCDH}_{A,g(1^k)} = \Pr\left[\left.\begin{array}{c}\mathbb{G}\leftarrow g(1^k);\\ g,h\leftarrow\mathbb{G};\\ a\leftarrow\mathbb{Z}_q^*;\\ m\leftarrow A(\mathbb{G},g,h);\\ \gamma\leftarrow\{1,\cdots,2^\tau-1\}\end{array}\right| : A(\mathbb{G},g,h,h^a,\gamma)=(mg^\gamma)^a\right]\le 2^{-\tau}$$

증명. 1. CDH 가정에 의해 $g^s=h$ 인 s를 모른다면, h^a로부터 g^a는 구할 수 없다.[1] … (*)

2. 다음과 같은 공격자의 존재를 가정하자.

iCDH문제를 풀 수 있는 확률이 p이고,
$p>1/2^\tau$ 이다.

3. 다음과 같이 (*)에 대한 모순을 보인다.
   a. 공격자의 성공확률이 p이므로, $1/p$ 번 실행해서 공격자가 적어도 한 번은 성공적인 출력을 내는 실험을 시행한다.
   b. 시뮬레이터는 이 첫번째 실행에서 공격자가 성공적으로 $y=(mg^\gamma)^a$를 출력하는 지점을 기록한다. 그리고 그때까지의 입출력을 모두 기록한다.
   c. 공격자를 재설정(rewind)한다.
   d. 성공적으로 iCDH의 답을 출력하는 지점 바로 직전까지 첫 번째 실행에서 기록한 것과 같은 입력을 공격자에게 준다. 공격자는 같은 출력시퀀스를 줄 것이다.
   e. 성공적으로 출력하는 지점에서 첫번째 실행에서의 입력과는 다른 입력(γ')을 준다.
   f. p^2 확률로 그 지점에서 공격자가 성공할 것이고 이때의 출력은 $y'=(mg^{\gamma'})^a$가 된다.
   g. 이제 시뮬레이터는 $(y/y')^{1/(\gamma-\gamma')}=g^a$를 출력한다.

4. 따라서 iCDH를 성공적으로 공격하는 공격자를 이용하면 h^a로부터 g^a를 구할 수 있게 된다. 이는 h^a로부터 g^a를 구할 수 없다는 가정에 모순이 되고, 이는 공격자에 대한 가정이 틀렸음을 의미한다. 따라서 공격자의 이득은 $1/2^\tau$로 제한된다. □

최근의 암호프로토콜들은 더욱 더 복잡해지고 있고, 이들의 안전성을 증명하는 일은 매우 어려워지고 있다. 결국, random oracle 모델, generic 모델, algebraic 모델 등을 도입하면서 공격자의 능력을 줄이는 방식으로 증명의 틀을 바꾸는 방향으로 가거나, 아니면 난제에 대한 가정(Hardness assumption)을 더 많이 만들어 내서 결국 더 많은 가정을 하는 방향으로 가고 있다. 이 논문에서 새롭게 정의한 대화식 CDH문제는 더 많은 가정을 하지 않고도 표준 모델에서 증명을 쉽게 할 수 있도록 하는 프리미티브가 될 수 있다. 왜냐하면, CDH, DDH문제와는 달리 공격

1) 참고로, 이는 co-CDH가정과는 다르다. co-CDH가정에서는 g와 h가 각각 다른 그룹의 생성자이다.

자의 입력이 iCDH 문제의 한 요소가 되고, 이는 암호 알고리즘과는 달리 대화형식의 메시지 주고받음이 있는 암호프로토콜의 성질과 잘 부합하기 때문이다

III. Identification 기법

앞서 정의한 iCDH 문제는 그 자체로 다음과 같은 사용자 확인(identification) 프로토콜로 정의할 수 있다.

시스템 파라미터: 증명자와 확인자는 사용자 확인 프로토콜을 수행하기 전에 다음과 같은 파라미터를 시스템 관리자로 부터 받아 저장한다.

$\mathbb{G}$: 소수 위수 q를 갖는 그룹
q: 소수
p: $p=rq+1$ 인 소수
g: $\mathbb{G}$의 생성자
$1/2^{\tau}$: soundness 확률

키 생성: 증명자는 $s\in Z_q^*$ 를 랜덤하게 선택해서 비밀키로 하고, 자신의 공개키 h를 다음과 같이 계산한다.

$$h=g^s \mod p$$

3.1 사용자 확인 프로토콜

증명자가 확인자에게 s를 알고 있음을 증명하기 위해서 다음의 프로토콜을 수행한다.

1. 증명자는 확인자에게 $a=g^r$을 전송한다. 여기서 $r\in_R\mathbb{Z}_q^*$.
2. 확인자는 증명자에게 $b=g^y$, c 을 전송한다. 여기서 $y\in_R\mathbb{Z}_q^*$, $c\in_R\{1,2,\cdots,\tau\}$
3. 증명자는 확인자에게 $d=(ah^c)^y$를 전송한다.
4. 확인자는 만약 $a=d^{1/y}h^{-c}$이면 증명자의 증명을 인정하고, 그렇지 않다면 종료한다.

여기서 h는 증명자의 공개키 정보로, 프로토콜 시작 전에 인증서와 함께 확인자에게 전송될 수도 있고 1단계에서 a와 함께 전송될 수도 있다.

3.2 안전성 증명

위 프로토콜에 대한 안전성 증명은 completeness, soundness, simulatability의 세 가지로 이루어진다.

정리 1. (Completeness) s를 알고 있는 사용자는 항상 위의 identification 프로토콜을 통과한다.

증명. s를 알고 있으므로, 다음과 같이 항상 $d=(ah^c)^y$를 계산할 수 있다.

$$b^{r+sc}=b^r b^{sc}=g^{yr}h^{cy}=(ah^c)^y=d$$ □

정리 2. (Soundness) s를 모르는 사용자가 위의 identification 프로토콜을 통과할 확률은 $1/2^{\tau}$보다 작거나 같다.

증명. 2절의 증명과 같다.

정리 3. (Simulatability) 위의 프로토콜은 s에 관한 아무런 knowledge도 유출하지 않는다.

증명. s를 아는 증명자의 도움 없이, 원래의 프로토콜과 구별 불가능한(indistinguishable) 트랜스크립트를 만들 수 있다. 즉, 원래 프로토콜의 트랜스크립트와 완전히 같은 트랜스크립트를 확인자 혼자서 만들 수도 있는데, 이는 트랜스크립트에 비밀 정보 s가 포함되어 있지 않으므로 가능 하다. 즉, 확인자 혼자서 y, r, c를 랜덤하게 고르면 비밀키 s가 필요하지 않기 때문에 트랜스크립트 $[a=g^r, b=g^y, c, (ah^c)^y]$를 생성할 수 있다. □

3.3 성능 분석

이 논문에서 제안한 사용자 확인 기법은 증명자에게 두 번(그중 한 번은 idle time에 전처리 가능), 그리고 확인자에게 두 번(그 중 한 번은 idle time에 전처리 가능)의 지수 승 연산을 필요로 한다. Schnorr 기법과 비교했을 때, 증명자에게 한 번의 지수 승을 더 요구한다. 통신량을 계산해 보면 $3\lg p+\lg\tau$ 비트만큼이 필요하지만, g^y를 전송하는 대신 $H(g^y)$를 전송하면 $2\lg p+\tau+$(1해쉬값) 만큼의 데이터 전송이 필요하다. 이는 Schnorr 기법과 비교하면, $\lg p$ 비트만큼의 통신량을 더 요구한다.

이를 전자 서명으로 바꾸기 위해서는 Fiat-Shamir의 테크닉을 이용하면 되는데, 이 식별기법에서는 확인자가 보내는 메시지가 c만이 아닌 g^y를 같이 전송하므로 쉽지 않다. 하지만, g^y를 서명 확인자의 공개키로 y를 비밀키로 하면 강한 수신자 지정 서명 기

법(Strong Designated Verifier Signature)로 변환할 수 있다. 거의 모든 수신자 지정 서명 기법은 Schnorr 기법을 변형해서 설계되었고[7], 이 논문에서 제시하는 프로토콜을 이용하는 경우 더 짧은 수신자 지정 서명 기법이 될 것이다.

Ⅳ. iDDH 가정

이 절에서는 iCDH 문제의 판별 버전(decisional version)에 대해서 살펴본다.

DDH 가정은 $(g, h, g^x, h^{x'})$에서 $x = x'$인 DDH tuple과 $x \neq x'$인 무작위 조합(random tuple)을 구별하지 못한다는 것을 의미한다. 이에 반해, 새로운 문제의 판별 버전(decisional version)은 공격자가 선택한 m에 대해서 문제출제자는 $(g, h, g^y, (mh^\gamma)^{y'}, \gamma)$를 문제로 출제한다. 이때, 각각 1/2의 확률로, $y = y'$이거나 $y \neq y'$이다. iDDH가정은 공격자가 $y = y'$인지 맞출 확률은 $1/2 + 1/2^\tau$ 이다.

iDDH 문제에서는 DDH에서와 달리, 공격자가 먼저 임의대로 $m \in G$을 선택하면 iDDH문제의 출제자(oracle 또는 문제출제자)는 $(h^a, (mg^\gamma)^{a'}, \gamma)$를 문제로 제시한다. 이때, 공격자는 $a = a'$인지 $a \neq a'$인지 대답해야 하고, 공격자의 이득은 $1/2 + 1/2^\tau$ 보다 작거나 같다는 것이 iDDH 가정이다. 엄밀하게는 다음과 같이 정의 할 수 있다.

$$\mathrm{Rand}_{A,g(1^k)} = \Pr\left[\begin{pmatrix} \mathbb{G} \leftarrow g(1^k); \\ g, h \leftarrow \mathbb{G}; \\ a \leftarrow \mathbb{Z}_q^*; \\ b \leftarrow \mathbb{Z}_q^* \setminus a; \\ \gamma \leftarrow 1, \cdots, 2^\tau - 1 \end{pmatrix} : A(\mathbb{G}, g, h, h^a, (mg^\gamma)^b, \gamma) = 1\right]$$

$$\mathrm{iDDH}_{A,g(1^k)} = \Pr\left[\begin{pmatrix} \mathbb{G} \leftarrow g(1^k); \\ g, h \leftarrow \mathbb{G}; \\ a \leftarrow \mathbb{Z}_q^*; \\ \gamma \leftarrow 1, \cdots, 2^\tau - 1 \end{pmatrix} : A(\mathbb{G}, g, h, h^a, (mg^\gamma)^a, \gamma) = 1\right]$$

$$|\mathrm{iDDH}_{A,g(1^k)} - \mathrm{Rand}_{A,g(1^k)}| = 2^{-\tau} \text{ for } \mathbb{G} \text{ and for all PPT algorithms } A.$$

증명. 공격자는 m을 선택할 수 있으므로, 만약 $m = hg^{-\gamma}$를 선택한다면 iDDH문제는 h^a, h^b가 되어 공격자는 쉽게 문제를 풀 수 있다. 하지만, γ는 m이 선택된 이후에(일종의 commitment) 문제출제자에 의해 랜덤하게 선택되므로 예측 불가능하고 저렇게 선택할 확률은 $1/2^\tau$ 가 된다.

공격자가 $1/2^\tau$보다 높은 확률로 성공하지 못함을 증명하는 것은 iCDH의 증명과 다르다. 직관적으로 볼때, iDDH 문제는 DDH문제와 $1/2^\tau$ 만큼의 이득을 공격자에게 준다는 것 이외에는 같다. 왜냐하면, DDH문제의 g, h는 문제출제자에 의해 랜덤하게 선택된 $\mathbb{G}$의 생성자(generator)이고 이때 $(g^x, h^{x'})$이 무작위 조합(random tuple)인지 DDH 조합(tuple)인지 알 수 없다는 것이 DDH 가정인데, 비슷하게 iDDH에서 mg^γ도 무작위로 선택된 생성자이기 때문이다. 공격자의 이득은 m을 적절히 선택함으로써 mg^γ를 특별한 형태로 만들 수 있다는 것 이외에는 없다. 즉, m을 잘 선택해서 mg^γ의 h에 대한 표현(representation)을 알 수 있게 한다는 이득 뿐이다. 그렇지 않다면 mg^γ 자체가 무작위로 선택된 $\mathbb{G}$의 생성자가 되므로 DDH와 같아진다. 공격자가 mg^γ의 h에 대한 표현(representation)을 알기 위한 유일한 방법은 m을 $hg^{-\gamma}$형태로 선택해서 g부분을 소거시키는 것뿐이다. 이렇게 할 수 있는 확률은 $1/2^\tau$보다 작다. □

Ⅴ. 결 론

이 논문에서는 Computational Diffie- Hellman 가정에 안전성을 둔 새로운 문제를 제시했고, 이의 응용으로 새로운 identification기법을 보였다. 또한, 이 문제의 안전성을 증명했다. Schnorr identification기법이 암호프로토콜의 광범위한 영역에서 이용되는 것처럼 이 문제도 암호프로토콜을 설계할 때 새로운 암호 프리미티브로 이용될 수 있으리라 기대한다. 앞으로는 이 프리미티브를 다양한 암호프로토콜에 응용해 보고, 이 프리미티브의 판별 버전(decisional version)의 응용에 대해서도 연구할 계획이다.

참 고 문 헌

[1] W. Diffie and M.E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[2] T. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Transactions on Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[3] D. Boneh, “The decision Diffie-Hellman problem,” Proc. of the Third Algorithmic Number Theory Symposium, LNCS 1423, pp. 48-63, 1998.

[4] R. Cramer and V. Shoup, “Design and Analysis of Practical Public-Key Encryption Schemes Secure Against Adaptive Chosen Ciphertext Attack,” SIAM J. Computing, vol. 33, no. 1, pp. 167-226, Jan. 2003.

[5] F. Bao, R.H. Deng, and H. Zhu, “Variations of Diffie-Hellman Problem,” Proc. of ICICS, LNCS 2836, pp. 301-312, 2003.

[6] M. Abdalla and D. Pointcheval, “Interactive Diffie-Hellman Assumptions with Applications to Password- Based Authentication,” Proc. of Financial Cryptography, LNCS 3570, pp. 341-356, 2005.

[7] 김승주, 김경신, 박성준, 원동호, “영지식 수신자 지정 서명 방식,” 정보보호학회논문지, 6(1), pp. 15-24, 1996년 2월.