通信情報保護學會誌
第9卷 第1號, 1999. 3

# 이산대수 문제에 기반한 암호 방식의 안전성에 관한 연구

오 수 현*, 이 형 규*, 김 승 주**, 원 동 호*

## 요 약

본 고에서는 이산대수 문제의 어려움에 바탕을 둔 암호 프로토콜의 안전성에 영향을 미치는 여러 가지 요소들에 대하여 고찰하였다. 본 고의 내용은 크게 두 가지로 요약할 수 있다. 첫째 이산대수 문제를 계산하는 알고리즘들을 살펴본 후, 이 알고리즘들이 암호 프로토콜에 어떻게 영향을 미치는가에 대해서 시스템 파라미터를 기준으로 살펴보았고, 둘째 프로토콜 자체의 문제점에 대해 분석하였다. 따라서 본 논문은 이산대수 문제에 기반을 둔 암호 시스템의 전반적인 이해와 안정성 분석 및 시스템 설계에 도움을 줄 수 있으리라 기대된다.

## 1. 서 론

최근 컴퓨터의 보급과 인터넷의 활성화로 인해 네트워크 상에서의 정보 보호에 대한 관심이 높아지고 있다. 또한 현재 이러한 정보의 보호에 가장 많이 이용되는 기술이 바로 암호학이다. 암호학은 계산상 풀기 어려운 문제들에 기반하고 있는데, 그 대표적인 것으로 이산대수 문제(discrete logarithm problem)와 소인수 분해 문제(factorization problem)를 들 수 있다. 이 문제들은 다항식 시간(polynomial time)으로 풀 수 있는 알고리즘이 아직까지 존재하지 않는다는 점에서 매우 어려운 문제로 알려져 있으나 그 복잡도(complexity)에 대한 어떤 하한선(asymptotic lower bound on the complexity)도 증명이 되지 않고 있다. 따라서 시스템의 설계는 알려진 최선의 방법을 바탕으로 안전성을 확보할 수 있도록 그 파라미터들을 결정하는 것이 보통이다.

일반적으로 이산대수 문제는 다음과 같이 정의할 수 있다.

정의 1. (이산 대수 문제 (***discrete logarithm problem***)) 이산대수 문제는 위수(order)가 $p-1$인 순환 그룹(finite cyclic group) G, G의 원시원소 $\alpha$와 G의 원소 $\beta$가 주어졌을 때, $\alpha^x = \beta$를 만족하는 x(단, $0 < x \leq p-1$)를 계산하는 것으로, 이 x를 원시원소 $\alpha$에 대한 $\beta$의 이산대수(discrete logarithm)라 부른다.

본 고에서는 이산대수 문제에 바탕을 둔 공개키 암호 방식들이 갖는 문제점을 살펴보고 이를 해결하기 위한 방법들을 알아보기로 한다. 먼저 2장에서는 이산대수 문제 자체를 푸

* 성균관대학교 전기전자 및 컴퓨터공학부
** 한국 정보보호 센터

는 알고리즘들에 대해 살펴보고, 3장에서는 이산대수 문제를 바탕으로 하는 공개키 암호 방식들에 사용되는 공개 파라미터들의 안전성에 대한 분석을 한다. 다음으로 4장에서는 이산대수 문제에 바탕을 둔 디지틀 서명 방식의 안전성에 대해 살펴보고, 5장에서는 특수 디지틀 서명방식의 안전성에 대해 분석하고, 6장에서는 키 분배 프로토콜의 안전성에 대해 알아보고 마지막으로 7장에서는 그밖의 공격방법을 통해 이산대수 문제에 기반한 암호 시스템의 안전성을 분석하고자 한다.

## 2. 이산대수 문제를 푸는 알고리즘

### 2.1 임의의 그룹에 적용할 수 있는 알고리즘

지금까지 이산대수 문제를 푸는 많은 알고리즘들이 제안되었으며 이들은 크게 다음의 세 가지 범주로 나눌 수 있다. 첫째는 알고리즘이 그룹의 어떤 특정한 성질도 이용하지 않으므로 임의의 그룹에도 적용할 수 있는 방법으로 소모적 공격(exhaustive search)이나 Shanks의 baby-step/giant-step 알고리즘을 들 수 있다. 그러나 baby-step/giant-step[10] 알고리즘의 경우, 군의 위수가 n일 때 $O(\sqrt{n})$의 계산량을 가지는 방법으로 n이 $2^{120}$이상이면 이산대수를 풀 수 없다. 보다 실용적인 것으로 같은 시간에 훨씬 적은 메모리로 동작하는 Pollard rho[23] 알고리즘이 있으나 이 경우는 그룹의 위수를 알고 있어야 한다는 조건이 있다. 이밖에도, 이산대수 x의 범위인 w (단, b < x < b+w)가 알려져 있는 경우 적용할 수 있는 방법인 Pollard lambda알고리즘[23]이 있다. Pollard's rho 알고리즘이 임의의 범위에 있는 이산대수 x를 계산하는 반면, Pollard lambda 알고리즘은 이산대수 x의 범위를 알 때, Pollard's rho 알고리즘을 적용시키는 것이라 할 수 있다.

#### 12) 소모적 공격(exhaustive search) 알고리즘

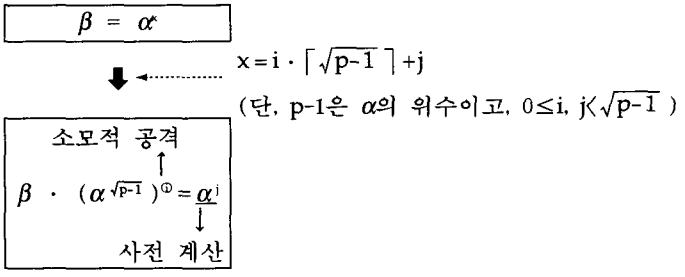
(가) 알고리즘

- 입 력 : 위수가 p-1인 순환 그룹 G의 원시원소 $\alpha$와 G의 원소 $\beta$
- 출 력 : $\beta = \alpha^x \pmod p$의 이산대수 x
- 과 정 : $\alpha^x = \beta \pmod p$를 만족하는 $\beta$를 구할 때까지 $\alpha^0, \alpha^1, \alpha^2, \cdots$ 를 계산한다.

#### 2) Baby-step / giant-step 알고리즘

(가) 개 요

baby-step / giant-step 알고리즘은 소모적 공격의 시간과 메모리 사이의 trade-off를 고려한 방법이다 (개념도 2.1 참조).




[개념도 2.1] baby-step / giant-step 알고리즘

(나) 알고리즘

- 입 력 : 위수가 p-1인 순환그룹 G의 원시원소 $\alpha$와 G의 원소 $\beta$
- 출 력 : $\beta = \alpha^x \pmod p$의 이산대수 x
- 과 정 :
  ① $m \leftarrow \lceil \sqrt{p-1} \rceil$으로 놓는다.
  ② $0 \le j < m$에 대하여 각 항목이 $(j, \alpha^j \bmod p)$인 표를 만들고 정렬한다.
  ③ $\alpha^{-m}$을 계산하고 $\gamma \leftarrow \beta$로 놓는다.
  ④ i는 0부터 m-1까지 다음을 수행한다.
    (ㄱ) 표의 두 번째 항목이 $\gamma$와 일치하는 것이 있는지 검사한다.
    (ㄴ) $\gamma = a^j$ 이면 $x = i \cdot m + j$을 리턴한다.
    (ㄷ) $\gamma \leftarrow \gamma \cdot a^{-m}$로 놓는다.

(다) 예 제

p = 113, 원시원소 $\alpha = 3$일 때, baby-step/giant-step 알고리즘을 사용하여 $Z_{113}^*$에서의 원소 $\beta = 57$의 이산대수 $\log_3 57$를 계산하는 방법은 다음과 같다.

① $m \leftarrow \lceil \sqrt{p-1} \rceil = 11$.
② 항목이 $(j, \alpha^j \bmod p)$인 $(0 \le j < 11)$를 표를 만든다.

| j | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $3^j \bmod 113$ | 1 | 3 | 9 | 27 | 81 | 17 | 51 | 40 | 7 | 21 | 63 |

위의 표를 다음과 같이 정렬한다.

| j | 0 | 1 | 8 | 2 | 5 | 9 | 3 | 7 | 6 | 10 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $3^j \bmod 113$ | 1 | 3 | 7 | 9 | 17 | 21 | 27 | 40 | 41 | 63 | 81 |

③ $\alpha^{-1} = 3^{-1} \bmod 113 = 38$과 $\alpha^{-m} = 3811 \bmod 113 = 58$을 계산한다.
④ 표의 두 번째 항목에 일치하는 값을 얻을 때까지 $i = 0, 1, 2, \cdots$ 에 대하여 $\beta \cdot \alpha^{-m \cdot i} \bmod 113$ 을 계산한다.

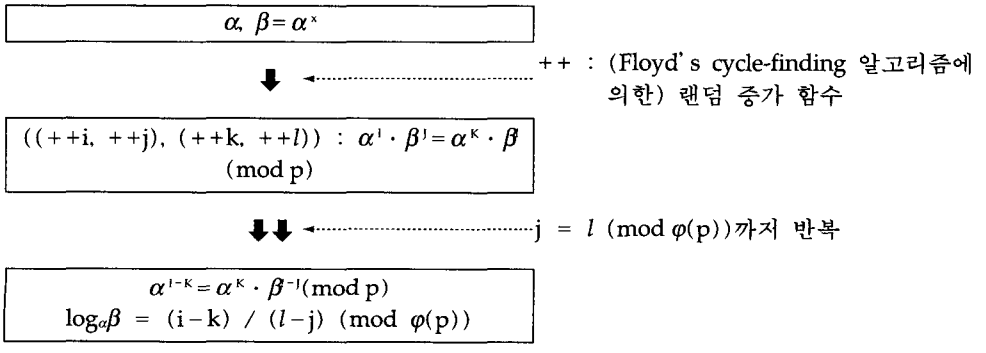
| j | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\gamma = 57 \cdot 58^i \bmod 113$ | 57 | 29 | 100 | 37 | 112 | 55 | 26 | 39 | 2 | 3 |

따라서, $\beta \cdot \alpha^{-9m} = 3 = \alpha^1$, $\beta = \alpha^{100}$ 이므로, $\log_3 57 = 100$.

3) Pollard's rho 알고리즘

(가) 개 요

이산대수 문제를 풀기 위한 Pollard's rho 알고리즘은 baby-step / giant-step 알고리즘과 같은 수행시간(running time)을 가지면서, 아주 적은 양의 메모리를 필요로 하는 랜덤화된 알고리즘이다 (개념도 2.2 참조).




[개념도 2.2] Pollard's rho 알고리즘

(나) 알고리즘

위수가 p-1인 순환 그룹 G를 다음과 같이 크기가 비슷한 3개의 서브 그룹 $S_1$, $S_2$, $S_3$ 으로 나눈다 (단, $x_0=1$ 이고 $1 \notin S_2$).

$$x_{i+1} = f(x_i) \overset{def}{=} \begin{cases} \beta \cdot x_i, & \text{if } x_i \in S_1, \\ x_i^2, & \text{if } x_i \in S_2, \\ \alpha \cdot x_i, & \text{if } x_i \in S_3, \end{cases} \quad (1)$$

또한, $x_i = \alpha^{a_i} \cdot \beta^{b_i}$를 만족하는 두 정수 $a_i$, $b_i$를 다음과 같이 정의한다 (단, $a_0=0$, $b_0=0$ 이고 $i \geq 0$ 이다).

$$a_{i+1} = \begin{cases} a_i, & \text{if } x_i \in S_1, \\ 2a_i \pmod{p-1}, & \text{if } x_i \in S_2, \\ a_i + 1 \pmod{p-1} & \text{if } x_i \in S_3, \end{cases} \quad (2)$$

$$b_{i+1} = \begin{cases} b_i + 1 \pmod{p-1} & \text{if } x_i \in S_1, \\ 2b_i \pmod{p-1}, & \text{if } x_i \in S_2, \\ b_i & \text{if } x_i \in S_3, \end{cases} \quad (3)$$

이제, Floyd의 cycle-finding 알고리즘을 이용해서 $\alpha^{a_i} \cdot \beta^{b_i} = \alpha^{a_{2i}} \cdot \beta^{b_{2i}}$ 을 만족하는 쌍 $((a_i, b_i), (a_{2i}, b_{2i}))$를 찾으면 이산대수 문제의 해를 구할 수 있다.

● 입 력 : 위수가 소수인 순환그룹 G의 원시원소 $\alpha$와 G의 원소 $\beta$

● 출 력 : $\beta=\alpha^x \pmod{p}$의 이산대수 x

● 과 정 :

① $x_0 \leftarrow 1$, $a_0 \leftarrow 0$, $b_0 \leftarrow 0$ 로 놓는다.

② i = 1, 2, … 에 대하여 다음을 수행한다.

(ㄱ) 사전에 계산한 $x_{i-1}$, $a_{i-1}$, $b_{i-1}$ 과 $x_{2i-2}$, $a_{2i-2}$, $b_{2i-2}$, 방정식 (1), (2), (3)을 사용하여 $x_i$, $a_i$, $b_i$과 $x_{2i}$, $a_{2i}$, $b_{2i}$를 계산한다.

(ㄴ) 만약 $x_i = x_{2i}$, 이면 다음을 수행한다. :

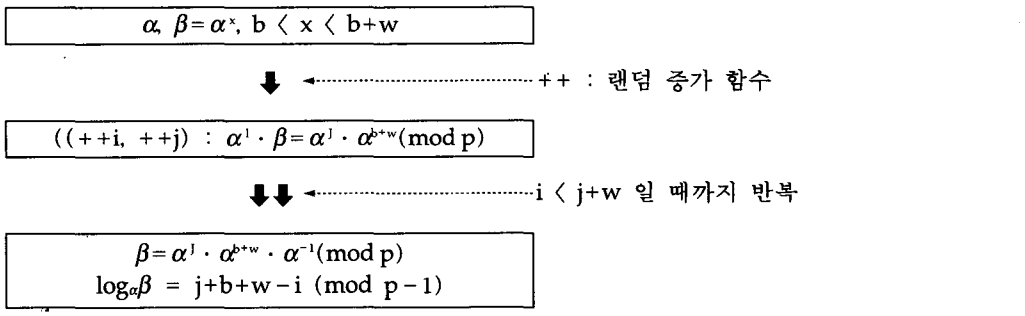
$\gamma \leftarrow b_i - b_{2i} \pmod{p-1}$로 놓는다. 만약 $\gamma = 0$ 이면 알고리즘은 실패로 끝난다 ;

그렇지 않으면, $x = \gamma^{-1} \cdot (a_{2i} - a_i) \pmod{p-1}$을 계산하고 x를 리턴한다.

4) Pollard's lambda 알고리즘

(가) 개 요

Pollard lambda 알고리즘은 이산대수 x가 $b<x<b+w$ 범위 안에 있다는 것을 알 때, 이산대수 $x \pmod{p-1}$(단, $ord(\alpha)=p-1$)를 구하는 알고리즘이다.




[개념도 2.3] Polladr's lambda 알고리즘

(나) 알고리즘

● 입 력 : $b \le x < b+w$가 알려진 GF(p)상의 원시원소 $\alpha$와 $\beta = \alpha x \pmod p$

● 출 력 : $\beta = \alpha^x \pmod p$의 이산대수 x

● 과 정 :

① x가 $b < x < b+w$ 범위 안에 있다는 것을 알고 있다고 가정한다.

② $\beta_0' = \alpha^{b+w}$, $\beta_0 = \beta$에 대해 수열 T, W를 계산한다.

수열 T : $\beta_0'$, $\beta_1'$, …, $\beta_N'$,

수열 W : $\beta_0$, $\beta_1$, …, $\beta_M$

단, $\beta_{i+1}' = \beta_i' \cdot \alpha^{f(\beta_i')}$

(여기서, $f(\beta_i')$ : 랜덤 증가 함수 )

③ $\beta_M$, $\beta_N'$에 대해 $\log_\alpha(\beta_N')$, $\log_\alpha(\beta_M)$을 계산한다.

$$\log_\alpha(\beta_N') = \log_\alpha(\beta_0') + d_N',$$

단, $d_N' = \sum_{i=0}^{N'-1} f(\beta_i') \bmod p-1$

$$\log_\alpha(\beta_M) = \log_\alpha(\beta_0) + d_M,$$

단, $d_M = \sum_{i=0}^{N'-1} f(\beta_i') \bmod p-1$

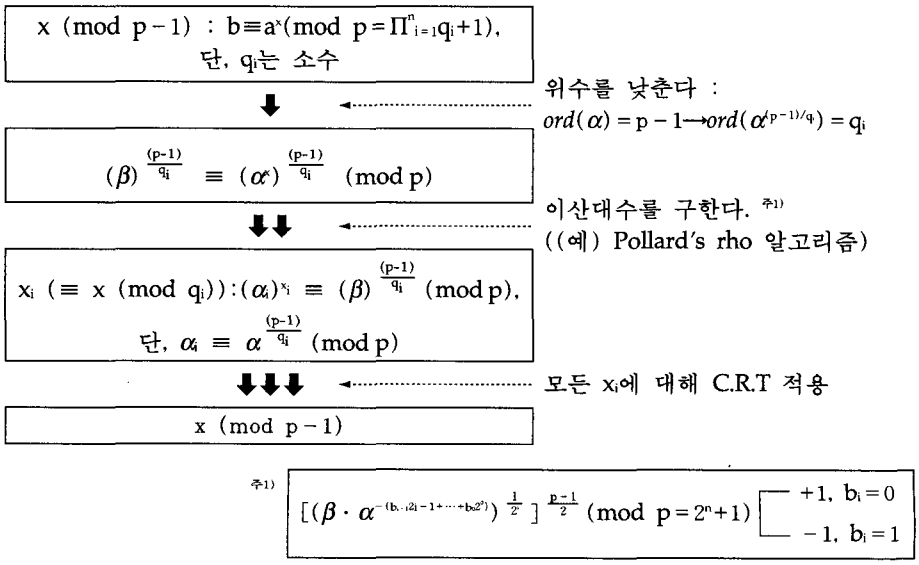
④ $d_M > w+d_N'$일 때 까지 수열 T, W 검사

⑤ $\beta_M = \beta_N'$ 이면 $x = b+w+d_N' - d_M \pmod{p-1}$ 가 된다.

## 2.2 위수가 smooth인 그룹에 적용할 수 있는 알고리즘

두 번째 범주로 그룹의 위수가 작은 소수들로만 이루어진(smooth) 그룹에 적용할 수 있는 알고리즘으로 Pohlig-Hellman과 Silver 등이 제안한 방법이 있다. Pohlig-Hellman 알고리즘[22]은 그룹의 위수가 작은 소수의 곱으로만 이루어져 있을 때 각각의 prime 서브 그룹상에서 이산대수를 구한 후 중국인의 나머지 정리(Chinese Remainder Theorem)를 이용하여 전체 그룹에서의 이산대수를 계산하는 방법이다. 만일 그룹 $G = GF(p)^*$, p는 소수 혹은 그 멱승인 경우 $ord(G) = p-1$ 이므로 위의 방법에 의한 이산대수 계산을 어렵게 하기 위해서는 $p-1$이 최소한 하나 이상의 큰 소수를 인수로 포함하도록 소수 p를 선택해야 할 것이다.

1) Pohlig-hellman 알고리즘




[개념도 2.4] Pohlig-Hellman 알고리즘

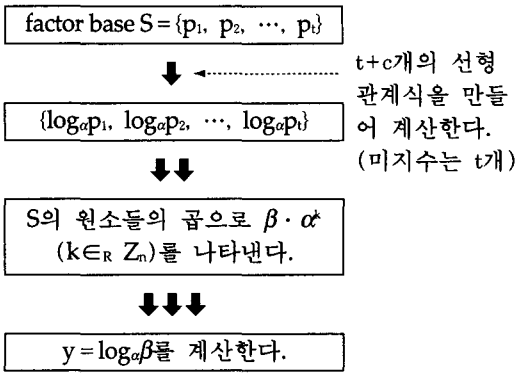
### 2.3 Factor-base를 이용하는 알고리즘

마지막으로 factor base를 이용하여 이산대수를 구하는 방법으로 Index-calculus 알고리즘[15]이 있다. 여기서 factor base라는 것은 그룹 G의 부분 집합들 중에서, 그 부분 집합의 원소들의 곱으로 그룹 G의 모든 원소를 표현할 수 있을 때, 그 부분 집합 S를 factor base라 한다. 이 방법은 L. Adleman의 논문 "A subexponential algorithm for the discrete logarithm problem with applications with cryptography"에서 기본적인 알고리즘이 발표된 이래 이에 대한 많은 변형과 개선 방안들이 제안되어 왔으나, 아직까지는 유한체(finite field) GF(p), GF(pk)나 허수 이차체(imaginary quadratic field)의 클래스 그룹(class group) 등으로 적용이 제한되어 있다. 그러나 Index calculus 방법은 위 방법중에 유일하게 sub-exponential time 알고리즘으로, 구조체상의 이산대수 문제를 푸는 알고리즘으로는 가장 강력한 방법으로 알려져 있다. 그러나 이 방법은 주어진 그룹의 구조에 의존하며 타원곡선 위의 이산대수에 대해서는 아직까지 불가능하다고 알려져 있다.

#### 1) Index-calculus 알고리즘

(가) 개 요

Index-calculus 알고리즘은 지금까지 알려진 알고리즘들 중 이산대수 문제를 푸는 가장 효율적인 알고리즘이다. 그러나 이 방법은 모든 그룹에 적용할 수는 없고, 이 방법을 적용할 수 있는 그룹에서는 subexponential-time 알고리즘을 제공한다 (개념도 2.5 참조).




[개념도 2.5] Index-calculus 알고리즘

(나) 알고리즘

- 입 력 : 위수가 p−1인 순환 그룹 G의 원시원소 α와 G의 원소 $\beta$
- 출 력 : $\beta = \alpha^x \pmod p$의 이산대수 x
- 과 정 :
  ① (**factor base S 선택**) S의 원소들의 곱으로 G안의 모든 원소를 효율적으로 표현할 수 있는 성질을 갖는 G의 부분집합 $S=\{p_1, p_2, \cdots, p_t\}$를 선택한다.
  ② (**S의 원소들의 이산대수를 포함하는 선형관계식**)
  (ㄱ) $0<k\le p-1$에서 난수 k를 선택하고 $\alpha^k$을 계산한다.
  (ㄴ) S안의 원소들의 곱으로 $\alpha^k$을 나타내도록 한다.

$$\alpha^k = \prod_{i=1}^{t} p_i^{c_i},\ c_i \ge 0 \qquad (1)$$

성공적이라면, 선형 관계식을 얻기 위하여 방정식 (1)의 양변에 $\log\alpha$를 취한다.

$$k \equiv \sum_{i=1}^{t} c_i \log_\alpha p_i \pmod{p-1}. \qquad (2)$$

(ㄷ) (2) 형태의 관계가 얻어질 때까지 ②.(ㄱ)과 ②.(ㄴ)를 반복한다. (c는 주

어진 t+c개의 방정식이 높은 확률로 유일한 해를 가질 수 있도록 작은 양정수를 선택한다.)

③ (S안의 원소의 이산대수 찾기) 모듈러 n을 가지고, $1 \le i \le t$에 대하여 $\log_\alpha p_i$의 값을 얻기 위하여 단계 ②에서 구한 (2)의 형태의 t+c개(미지수가 t개)의 선형 관계식을 푼다.

④ (x 계산)

(ㄱ) $0 < k \le p-1$에서 난수 k를 선택하고 $\beta \cdot \alpha^k$를 계산한다.

(ㄴ) $\beta \cdot \alpha^k$를 S의 원소들의 곱으로 표현한다.

$$\beta \cdot \alpha^k = \prod_{i=1}^{t} p_i^{d_i}, \ d_i \ge 0. \qquad (3)$$

만약, s의 원소들의 곱으로 표현할 수 없다면, 단계 ④.(ㄱ)을 반복한다. 그렇지 않으면, 방정식 (3)의 양변의 이산대수를 사용하여 $\log_\alpha \beta = (\sum_{i=1}^{t} d_i \cdot \log_\alpha pi - k) \bmod p-1$을 만들고, $x = (\sum_{i=1}^{t} d_i \cdot \log_\alpha pi - k) \bmod p-1$을 계산하고 x를 리턴한다.

(다) 예제

$p=229$이고 위수가 228인 $Z_{229}^*$의 원시원소가 $\alpha=6$일 때, Index-calculus 알고리즘을 사용하여 $\beta=13$의 이산대수를 구하는 경우, $\log_6 13$은 다음과 같이 계산할 수 있다.

① 다섯 개의 소수로 이루어진 factor-base S를 선택한다. : S = {2, 3, 5, 7, 11}

② factor-base의 원소들로 얻을 수 있는 여섯 개의 관계식은 다음과 같다.

$6^{100} \bmod 229 = 180 = 2^2 \cdot 3^2 \cdot 5$

$6^{18} \bmod 229 = 176 = 2^4 \cdot 11$

$6^{12} \bmod 229 = 165 = 3 \cdot 5 \cdot 11$

$6^{18} \bmod 229 = 154 = 2 \cdot 7 \cdot 11$

$6^{143} \bmod 229 = 198 = 2 \cdot 3^2 \cdot 11$

$6^{206} \bmod 229 = 210 = 2 \cdot 3 \cdot 5 \cdot 7$

이 관계식들로 factor-base안의 원소들의 이산대수 값을 포함하는 다음의 여섯 개의 방정식을 만들 수 있다.

$100 \equiv 2 \cdot \log_6 2 + 2 \cdot \log_6 3 + \log_6 5 \pmod{228}$

$18 \equiv 4 \cdot \log_6 2 + \log_6 11 \cdot \pmod{228}$

$12 \equiv \log_6 3 + \log_6 5 + \log_6 11 \pmod{228}$

$62 \equiv \log_6 2 + \log_6 7 + \log_6 11 \pmod{228}$

$143 \equiv \log_6 2 + 2 \cdot \log_6 3 + \log_6 11 \pmod{228}$

$206 \equiv \log_6 2 + \log_6 3 + \log_6 5 + \log_6 7 \pmod{228}.$

③ 미지수가 5개인 여섯 개의 선형 시스템을 풀면 $\log_6 2 = 21$, $\log_6 3 = 208$, $\log_6 5 = 98$, $\log_6 7 = 107$, $\log_6 11 = 162$를 구할 수 있다.

④ $k=77$이 선택되었다고 하면, $\beta \cdot \alpha^k = 13 \cdot 6^{77} \bmod 229 = 147 = 3 \cdot 7^2$이므로, 다음과 같이 계산할 수 있다.

$\log_6 13 = (\log_6 3 + 2 \cdot \log_6 7 - 77) \bmod 228 = 117.$

## 3. 공개 파라미터들의 안전성

### 3.1 weak 모듈라에 바탕을 둔 공격 방법

이산대수 문제에 기반한 암호 시스템에서 사용하는 모듈라 p의 특징을 이용하여 이산대수 값을 구해내는 방법들이 존재한다. 먼저, $p = p_1 \cdot p_2 \cdot \cdots \cdot p_i + 1$과 같이 p-1이 작은 소수들의 곱으로 이루어져 있고 원시 원소 $\alpha$의 위수가 p-1이면 Pohlig-Hellman의 알고리즘을 사용하여 이산대수를 계산할 수 있고, 이러한 공격을 막기 위하여 p-1이 큰 소수를 인자로 갖도록 $p=2qw+1$과 같이 선택하고 $\alpha$의 위수가 p-1이면 Oorschot의 공격방법에 의해 x (mod w)를 계산해 낼 수 있게된다. 또한 이러한 공격들을 막기 위하여, p-1이 큰 소수를 인자로 갖고($p=2qw+1$), $\alpha$의 위수가 q가 되

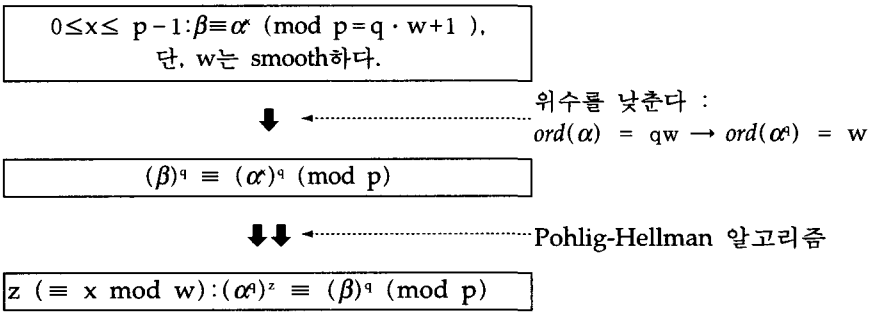
도록 p를 선택하면, 임채훈의 공격방법에 의해 x를 계산할 수 있다.

지금까지의 공격 방법은 적절하지 못한 공개 파라미터들에 의해 비밀키 x를 구하고자 하는 공격 방법들이었으나, 그 밖에 Vaudenay는 센터가 부정한 방법으로 공개 파라미터들을 생성함으로써 비밀키 x를 구하지 않고도 해쉬 함수의 충돌 쌍을 찾아내어 DSS 서명을 위조할 수 있다는 것을 제안하였다.

1) Pohlig-Hellman decomposition을 사용하는 Oorschot의 공격 방법[1]

모듈라 p가 $p=qw+1$ (단, w는 smooth)의 형태일 때, $ord(\alpha)=p-1=qw$이고, qw가 전체적으로 smooth하지는 않기 때문에 Pohlig-Hellman 알고리즘을 적용시킬 수 없지만, $\beta \equiv \alpha^x \pmod p$의 양변에 q승을 해주면, $ord(\alpha^q)=w$가 되고 w는 smooth 하므로 Pohlig-Hellman 알고리즘을 적용하여 $x \pmod w$를 구할 수 있게된다. (개념도 3.1 참조)

(가) 개 요




[개념도 3.1] Pohlig-Hellman decomposition을 사용하는 Oorschot의 공격 방법

(나) 예 제 (New middleperson attack)

$p-1=qw$(단, w는 smooth하다), $\alpha$:원시원소

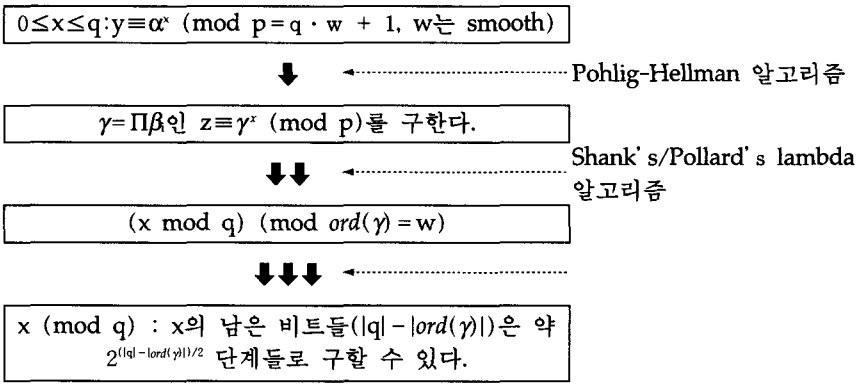
| Alice | | Alice | Alice | Alice |
|---|---|---|---|---|
| $a \in_R Z_{p-1}$ | $\alpha^a$ ⟵ | | $\alpha^b$ ⟵ | $b \in_R Z_{p-1}$ |
| $K_{AB} = (\alpha^{bq})^a$ | $(\alpha^b)^q$ ⟶ | | $(\alpha^a)^q$ ⟶ | $K_{AB} = (\alpha^{aq})^b$ |
| | | compute,<br>$a=\log_{\alpha^q}(\alpha^a)^q$<br>$b=\log_{\alpha^q}(\alpha^b)^q$<br>$K_{AB}=\alpha^{abq}$ | | |

2) 임채훈 등의 "key recovery attack"[14]

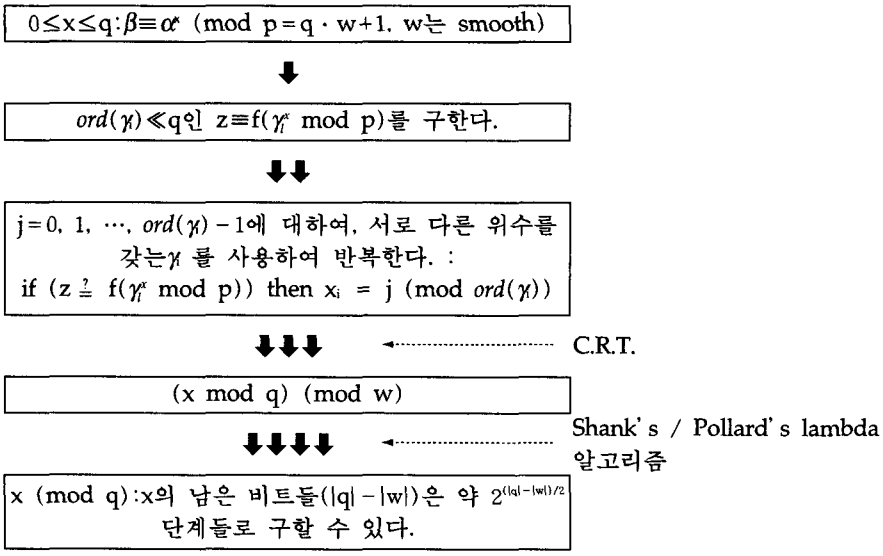
기본적인 개념은 작은 수를 위수로 갖는 원소를 이용한 공격방법이다. 여기에서는 prime order 서브 그룹을 사용하는 어떤 시스템에서 공개키의 검사가 이루어지지 않으면 작은 수를 위수로 갖는 원소를 이용한 공격이 가능하다는 것을 보여준다. Diffie-Hellman 키 분배를

이용한 암호통신에서 이 공격이 어떻게 행해 지는가를 아래 예제를 통해 설명해 줄 것이다.

(가) 개 요



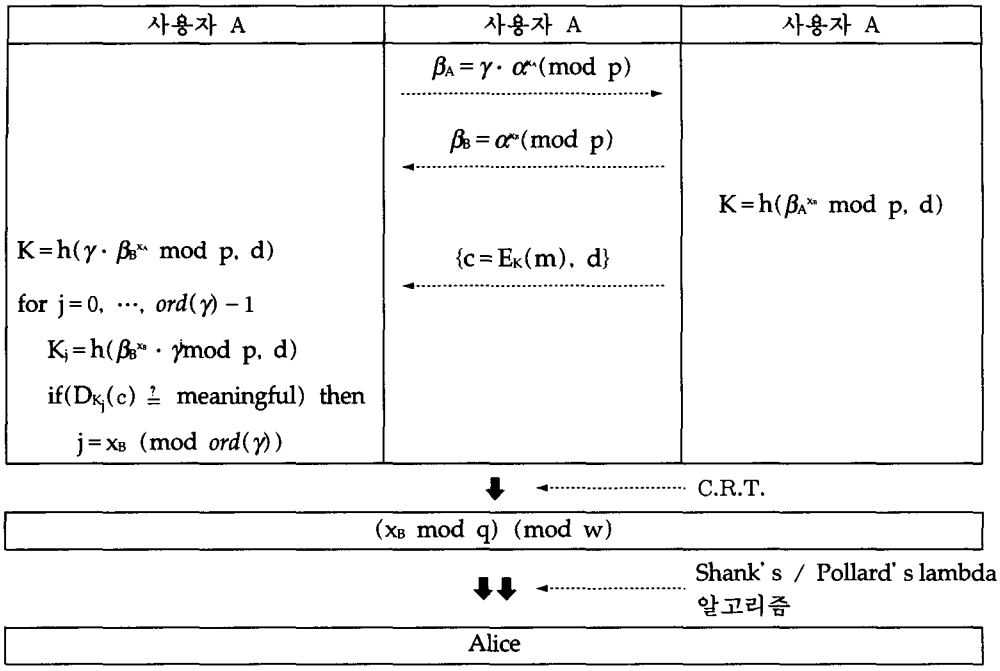

[개념도 3.2] Key-recovery attack( I )




[개념도 3.3] Key-recovery attack( II )

(다) 예 제

사용자 A의 공개키를 $\beta_A = \alpha^{x_A} \pmod{p}$, 사용자 B의 공개키를 $\beta_B = \alpha^{x_B} \pmod{p}$라 할때, 다음과 같은 방법으로 상대방의 비밀키를 계산해 낼 수 있다.

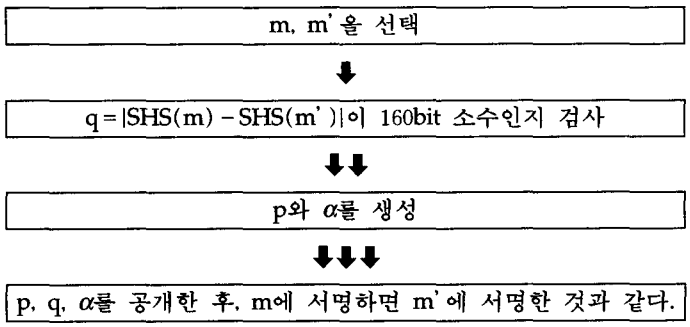



3) Vaudenay의 "hidden collisions"[24]

지금까지 설명한 공격방법들은 프로토콜에 적절하지 않은 공개 파라미터를 사용함으로써 이로 인해 이산대수를 구하는 방법들이었다. 이러한 공격방법 외에, 센터가 부정한 방법으로 공개 파라미터들을 생성함으로써 특정 메시지에 대한 DSS 서명을 위조할 수 있다는 것을 Vaudenay가 제안하였다.([개념도 3.4] 참조)

먼저, 센터는 서로 다른 문장 m, m'을 선택한 후 두 문장의 해쉬 값의 차가 소수가 되는지를 검사하여 이를 만족하는 값을 q로 선택한다. 그리고 나서 이에 따라 p, g를 생성하고 p, q, g를 공개한다. 만일 사용자가 문서 m에 서명을 할 경우, m과 m'는 동일한 해쉬값을 가지므로 센터는 쉽게 m'에 대한 사용자의 서명을 획득할 수 있게 된다.

(가) 개 요



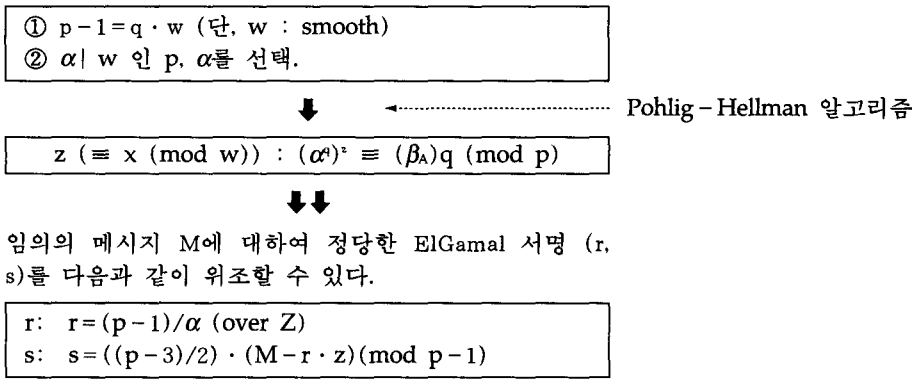

[개념도 3.4] Hidden collision

### 3.2 weak 원시원소에 기반한 공격 방법

이산대수 문제에 기반한 암호 시스템에서는 모듈라 p 뿐만 아니라, 원시원소 $\alpha$도 적절하게 선택하여야 한다. Bleichenbacher는 ElGamal 서명 시스템에서 $p=q \cdot w+1$ (단, w는 smooth) 일 때, $\alpha$|w가 되는 weak 원시원소 $\alpha$를 사용할 경우 사용자의 비밀키를 모르고도 다음과 같은 방법으로 ElGamal 서명을 위조할 수 있다는 것을 지적하였다.

1) Bleichenbacher의 ElGamal 서명 위조에 대한 공격[2]

(가) 개 요




[개념도 3.5] Bleichenbacher의 ElGamal 서명 위조에 대한 공격

정 리 1. w가 smooth일 때 $p-1=q \cdot w$라 하고 사용자 A의 공개키를 $\beta_A$라 하자. 만약 ① 원시원소 $\gamma=c \cdot q$ $(0<c<w)$ 이고 ② $\gamma^t=\alpha \pmod p$를 만족하는 정수 t를 알고 있다면, 주어진 M에 대하여 정당한 ElGamal 서명 (r, s)를 계산할 수 있다.

(증명) 먼저, z를 구하는 방정식은 다음과 같다.

$$\alpha^{qz}=(\beta_A)^q \pmod p$$

$p-1=q \cdot w$ 이므로, $\alpha^q$에 의해 생성된 서브그룹 H의 위수는 w가 된다. w는 smooth이므로, Pohlig-Hellman 알고리즘을 사용하여 이산대수 z를 구하는 것이 가능하다.

$r=\gamma^t$라 하면, $s=t \cdot (M-\gamma \cdot z) \pmod{p-1}$

이 된다. 이제 다음의 식이 성립하므로, (r, s)는 메시지 M에 대한 정당한 서명이 된다.

$$r^s (y_A)^r=(\gamma)^{t(M-\gamma z)} \cdot (\beta_A)^{\beta}=(\gamma)^{(M-cqz)} \cdot (\beta_A)^{cq}$$
$$=\alpha^{(M-cqz)} \cdot \alpha^{cqz}=\alpha^M \pmod p.$$

따름정리 2. $\alpha$가 smooth이고 $p-1$을 나누면 임의의 메시지 M에 대하여 정당한 ElGamal 서명을 위조하는 것이 가능하다.

(증명) $\gamma=(p-1)/\alpha$(over Z) 이고 $t=(p-3)/2$(over Z)이라 하자. 그러면 다음의 두식이 성립한다.

① $\gamma=cq(0<c<w)$

② $\gamma^t=\gamma^{(p-1)/2-1}=\gamma^{(p-1)/2} \cdot \gamma^{-1}=(-1) \cdot \gamma^{-1}=(-1) \cdot (\frac{p-1}{\alpha})^{-1}=(-1) \cdot (p-1)^{-1} \cdot (\alpha^{-1})^{-1}=(-1) \cdot (-1)^{-1} \cdot \alpha = \alpha \pmod p.$

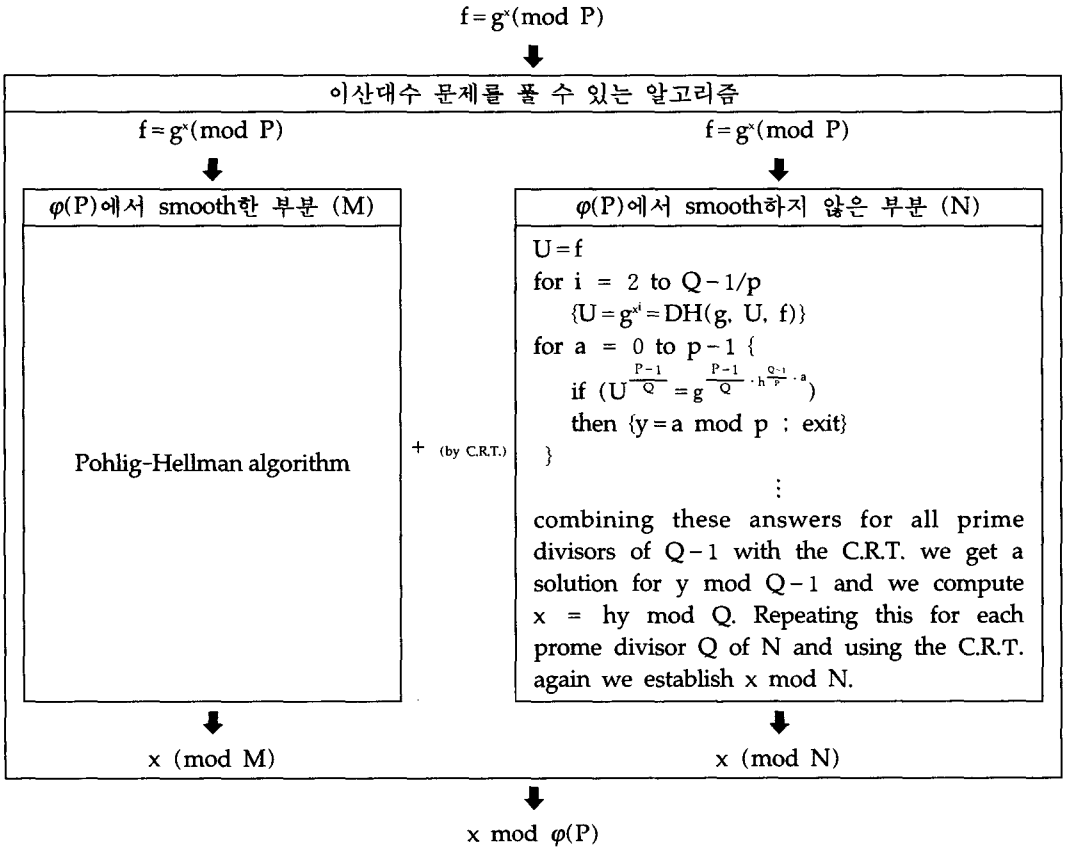
따라서, 정리 1.에 의해 모든 메시지 M에

대한 서명을 위조할 수 있다.

### 3.3 안전성이 증명 가능한 공개 파라미터

#### 1) 특정 소수에 대한 Diffie-Hellman 문제의 안전성[3]

이산대수 문제를 풀면 Diffie-Hellman 문제는 쉽게 해결할 수 있다. 하지만 Diffie-Hellman 문제를 해결한다고 해서 이산대수를 풀 수 있는 알고리즘은 아직까지 알려진 바가 없다. 하지만 특별한 경우, 즉 $p-1$의 Euler 함수 $\varphi(p-1)$이 작은 소수들만으로 이루어진 경우(smooth한 경우)에 대해서는 Diffie-Hellman oracle을 이용하면 이산대수 문제를 확률론적 다항식 시간 안에 풀 수 있는 알고리즘을 설계할 수 있으므로, 두 문제, 이산대수 문제와 Diffie-Hellman 문제는 그룹 $GF(p)^*$에 대해 동등한 난이도를 갖는다고 할 수 있다. 그러나 $\varphi(p-1)$이 작은 소수들로만 이루어진 경우라도 이산대수 문제를 쉽게 풀 수 있는 알고리즘은 아직까지 알려져 있지 않으므로 최소한 이와 같은 소수 p에 대해서는 Diffie-Hellman 문제가 이산대수 문제만큼 어렵다는 증명이 된 셈이다. 만일 $\varphi(p-1)$이 smooth한 경우에 이산대수 문제를 푸는 알고리즘과 Diffie-Hellman oracle을 이용하여 $\varphi(\varphi(p-1))$이 smooth한 경우의 이산대수 문제를 푸는 알고리즘을 설계할 수 있다면, 이와 같은 과정을 반복하면 결국 일반적인 이산대수 문제를 쉽게 풀 수 있는 방법이 있거나 Diffie-Hellman 문제를 푸는 것이 어려운 소수 p가 존재한다는 결론에 도달하게 될 것이다.



(가) 알고리즘

● 가 정 : ① P:큰 소수

② $\varphi(P)=P-1$
$=M\times N$ (단, M:smooth 함, N ( = Q×…):smooth하지 않음)
$=M\times(Q\times\cdots)$

③ $\varphi(\varphi(P))=\varphi(P-1)$
$=\varphi(M)\times\varphi(N)$
$=\varphi(M)\times(\varphi(Q)\times\cdots)$
(단, $\varphi(Q)$( = p×…) :smooth 함)
$=\varphi(M)\times((Q-1)\times\cdots)$
$=\varphi(M)\times((p\times\cdots)\times\cdots)$

④ $x=h^y \pmod Q$ (단, h는 GF(Q)* 상의 원시원소)

● Diffie-Hellman oracle을 이용한 이산대수 문제를 풀 수 있는 알고리즘의 설계:

### 3.4 효율적인 공개 파라미터

1) 지수의 크기에 따른 이산대수 문제의 안전성[21]

(가) 개 요

〈표 3.1〉은 Pohlig-Hellman의 알고리즘을 적용하여 이산대수를 계산할 수 없는 소수에 대해, 공격자의 계산 능력과 공격 성공률을 나타낸 것이다. 이로 인하여 p=2q+1 형태의 소수와 같은 안전성을 제공하면서 수행 속도를 개선하기 위하여 원시원소 $\alpha$의 위수가 큰 소수 q (단, $ord(\alpha)=q$) 가 되도록 prime order 서브 그룹을 사용한다. 소수의 안전성은 부분적인 Pohlig-Hellman 알고리즘과 Pollard's lambda 알고리즘 등을 적용하여 $(1/2)\cdot\max(u-k, \log(qr))$ 비트로 나타난다 (단, $x\approx 2^u$, k:유출된 정보의 비트, $q_r$:가장 큰 n(위수)의 소인수). 따라서, 보통 상업적으로 안전하다고 사용되는 비도 80비트를 유지하기 위해서는 160비트의 q를 사용하여야 한다 (예 : DSA에서 160비트의 소수 q를 사용한다).

〈표 3.1〉 1024비트 소수에 대해 의 계산능력을 가진 공격자의 이산대수 문제에 대한 공격 성공률

| 공격자의 능력 $2^c$ | 지수의 크기 u (비트) | | | | | | |
|---|---|---|---|---|---|---|---|
| | 64 | 96 | 128 | 160 | 192 | 224 | 256 |
| $2^{24}$ | 81% | 45% | 18% | 10% | 1% | 0% | 0% |
| $2^{32}$ | 100% | 68% | 38% | 25% | 12% | 2% | 1% |
| $2^{40}$ | 100% | 84% | 55% | 32% | 22% | 7% | 2% |

## 4. 디지틀 서명방식에 대한 공격 방법

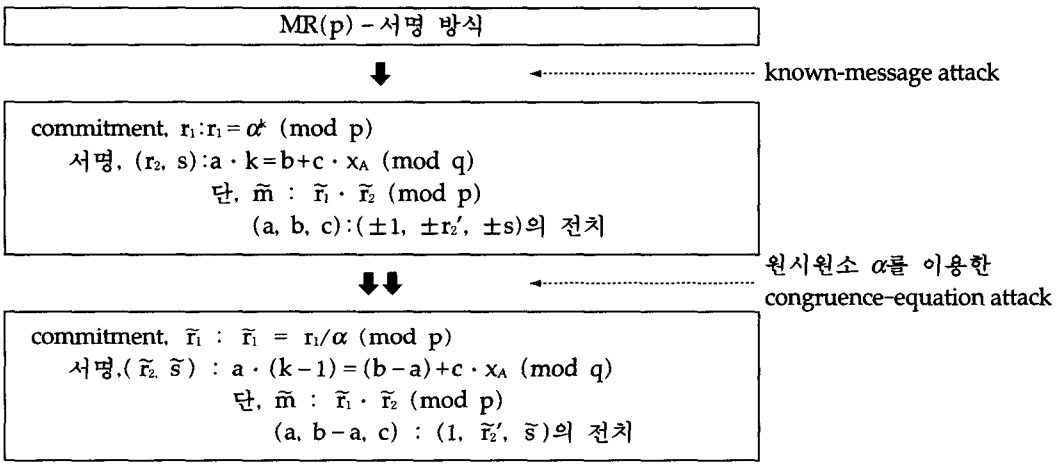
### 4.1 Nyberg-Rueppel 서명방식의 문제점

Nyberg-Rueppel은 이산대수 문제에 기반한 메시지 복원형 디지틀 서명방식을 제안하였다. 이러한 메시지 복원형 디지틀 서명 방식은 특히 1-pass (상호)인증 키 교환 프로토콜로 쉽게 확장될수 있는 특징을 갖는다. 그러나 Atsuko Miyaji는 다음과 같은 Nyberg-Rueppel의 서명방식의 네가지 문제점을 지적하였다.

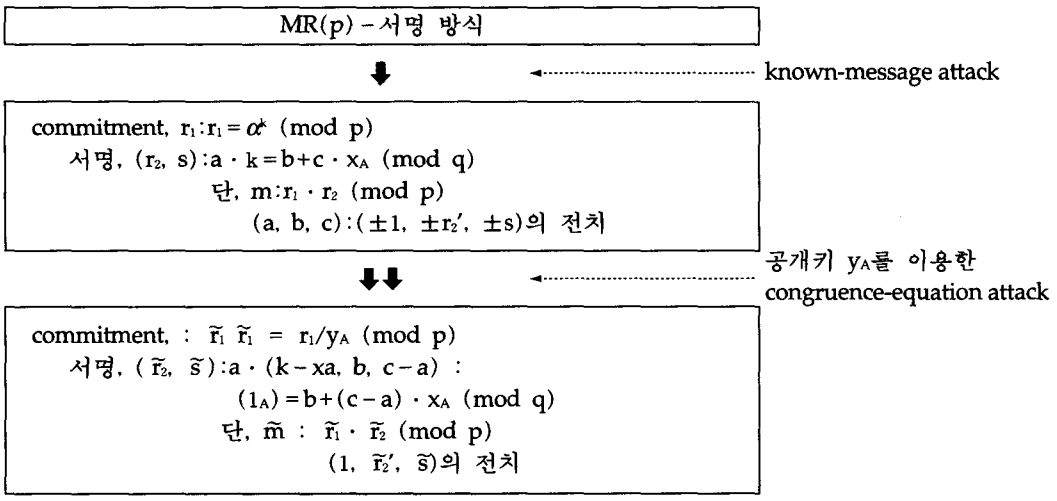
- ***congruence-equation attack*** : 서명 방정식을 조작하여 known message attack을 사용하여 existential forgery를 얻는다 (개념도 4.1. 4.2 참조).
- ***homomorphism attack*** : congruence-equation attack을 확장한 것으로 chosen message attack으로 임의의 메시지를 위조할 수 있다 (개념도 4.3 참조).
- ***redundancy attack*** : Redundancy를 이용하여 known message attack으로 existential forgery를 얻는다 (개념도 4.4 참조).
- ***recovery-equation attack*** : 아무런 입력없이 검증식을 이용하여 existential forgery를 얻는다 (개념도 4.5 참조).

1) Miyaji의 "congruence-equation attack"[18]

(가) 개 요




[개념도 4.1] congruence-equation attack( I )




[개념도 4.2] congruence-equation attack( II )

(나) 예 제

NR(p)-서명 방식이 다음과 같을 때, Congruence-equation 공격을 적용하면 다음과 같이 서명을 위조할 수 있다.

NR(p)-서명 방식 :

| 사용자 A | | 검증자 |
|---|---|---|
| random $k \in_R Z_q$<br>$r_1 = \alpha^k \pmod p$<br>$r_2 = r_1^{-1} \cdot m \pmod p$<br>$r_2' = r_2 \pmod q$<br>$s = k - x_A \cdot r_2' \pmod q$ | $(r_2, s)$ ⋯⋯▸ | $m = \alpha^s y_A^{r_2'} r_2 \pmod p$ |

이때, 임의의 메시지 m에 대한 서명 $(r_2, s)$를 알고 있을 때 (*known-message attack*), $\tilde{m}$, $\tilde{r_1}$, $\tilde{r_2}$, $\tilde{s}$ 를 다음과 같이 설정하면, 메시지에 대한 $\tilde{m}$에 대한 서명 $(\tilde{r_2}, \tilde{s})$를 위조할 수 있다 (*existential forgery*).

NR(p)-서명 방식에 대한
Congruence-equation attack :

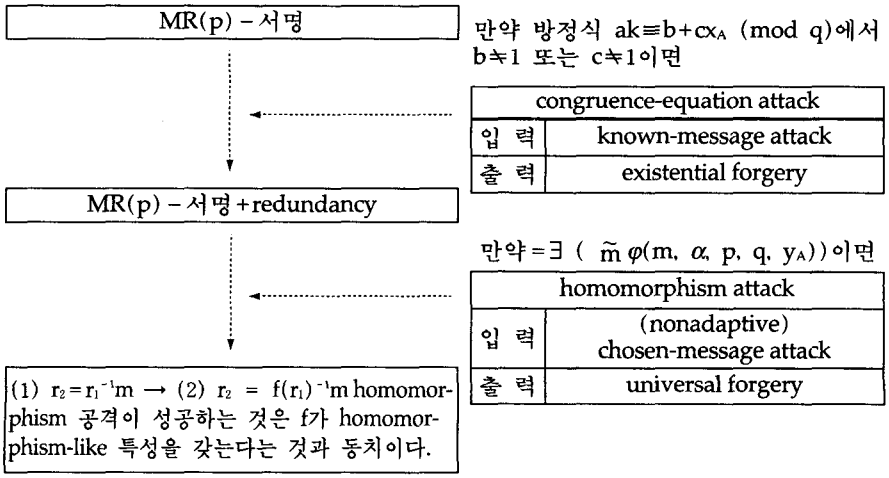
- 입 력 : 임의의 메시지 m, 서명 $(r_2, s)$
- 출 력 :
  ① $\tilde{r_1}\ (mr_2^{-1})g^{-n} = r_1 g^{-n} = \alpha^{k-n} \pmod p$ (단, $n \in Z_q$)
  ② $\tilde{m} = m\alpha^{-n} \pmod p$이라 하면,
  → ***existential forgery***
  $\tilde{r_2} = r_2 \pmod p$
  $\tilde{s} = s - n \pmod q$
  ③ $(\tilde{r_2}, \tilde{s})$ : $\tilde{m}$의 서명

2) Miyaji의 "homomorphism attack"[18]

앞에서 보았듯이, Nyberg-Rueppel의 MR(p)-서명 방식은 congruence-equation 공격에 의해 existential forgery를 얻어낼 수 있다. 이를 방지하기 위해, 서명 방식에 redundancy를 추가하면 이러한 공격은 쉽게 막을 수가 있다. 그러나, redundancy를 추가하더라도 homomorphism attack을 이용하면 (non-adaptively) chosen message attack으로 universal forgery를 얻어낼 수가 있다.

따라서, 이러한 공격을 막기 위해서는 아래 개념도 4.2의 방정식 (2)에서의 함수 f가 non-homomorphic한 특성을 갖도록 설계해야 한다. 또한, homomorphism 공격방법은 그 성격에 의해 NR(p)-서명 방식의 대표적인 응용분야인 키 교환 프로토콜에도 쉽게 적용할 수 있다.

(가) 개 요




[개념도 4.3] homomorphism attack

(나) 예 제

1-pass 키 교환 프로토콜이 다음과 같을 때, homomorphism 공격 방법을 적용시키면, chosen-message attack에 의해 공격자는 사용자 A의 비밀키를 모르고도 다음과 같이 세션키를 설정할 수 있게된다.

1-pass 키 교환 방식 :

| 사용자 A | | 사용자 B |
|---|---|---|
| 난수 $k \in_R Z_q$<br>$m = \alpha^K \pmod p$<br>$(r_2, s)$ : by NR(p) - 서명<br>세션키 $K_{AB}$ :<br>$K_{AB} = y_B^K = \alpha^{aK} \pmod p$ | $(r_2, s)$ ⋯⋯▸ | $m = \alpha^a y_A^{r_2} r_2 = \alpha^K \pmod p$<br><br>세션키 KAB :<br>$K_{AB} = m^{x_B} = \alpha^{Kx_B} \pmod p$ |

1-pass 키 교환 방식에 대한 homomorphism attack :

공격자는 메시지 m을 다음과 같이 선택하여 사용자 A로부터 메시지 m에대한 NR(p)-서명 $(r_2, s)$를 받아낸다 (chosen-message attack).

$$l \in Z_q,\ m = \alpha^l \pmod p$$

그리고 나서, 난수 $x \in_R Z_q$ 를 선택하고, $\tilde{m}$를 다음과 같이 정한다.

$$\tilde{m} = \alpha^x = m\alpha^{x-l} \pmod p$$

이때, $n = l - x$ 라 하면, 메시지 $\tilde{m} = \alpha^n \pmod p$의 NR(p) - 서명 $(\tilde{r_2}, \tilde{s})$를 위조할 수 있게 된다.

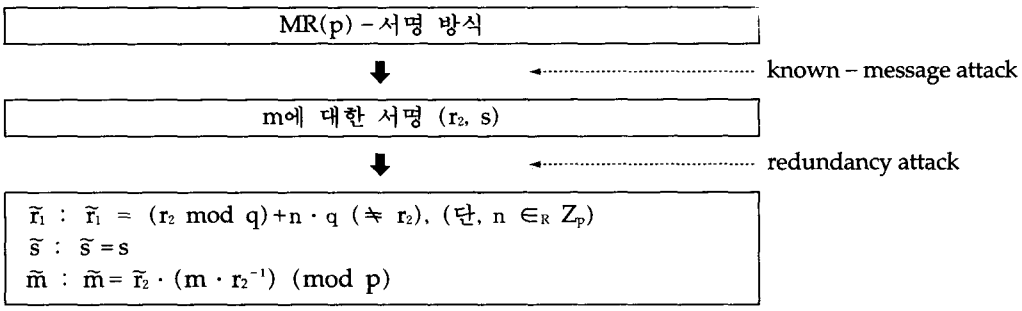
다음으로, 공격자는 사용자 B에게 $(\tilde{r_2}, \tilde{s})$를 전송하면, 다음과 같은 방법으로 둘 사이의 세션키 $K_{AB}$를 만들 수 있게된다.

$$K_{AB} = y_B^K = \alpha^{aKx} \pmod p$$
$$= m^{x_B} = \alpha^{Kx_B} \pmod p$$

3) Miyaji의 "redundancy attack"[19]

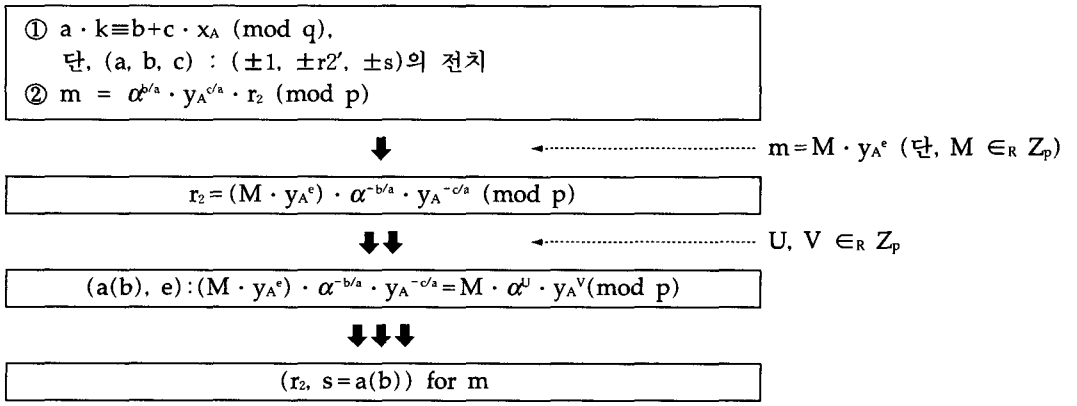
Redundancy attack은 known-message attack으로 얻어진 m에 대한 서명 $(r_2, s)$로 부터 $Z_p$ 상에서는 서로 다른 값을 갖지만, $Z_q$상에서는 $r_2$와 같은 값을 갖는 $\tilde{r_2}$를 계산하여, 다른 메시지 $\tilde{m}$에 대한 서명 $(\tilde{r_2}, \tilde{s})$를 위조하는 것이다.

(가) 개요




[개념도 4.4] redundancy attack

4) Miyaji의 "recovery-equation attack"[19] (가) 개 요




[개 념 도 4.5] recovery-equation attack

(나) 예 제

NR(p)-서명 방식이 다음과 같을때, recovery-equation 공격방법을 적용하면 아무런 입력 없이도 메시지 m에 대한 서명을 위조할 수 있게된다.

NR(p)-서명 방식:

| 사용자 A | | 검증자 |
|---|---|---|
| 난수 k ∈R $Z_q$<br>$r_1=\alpha^k$ (mod p)<br>$r_2=r_1^{-1} \cdot m$ (mod p)<br>$r_2'=r_2$ (mod q)<br>$s=k-x_A \cdot r_2'$(mod q) | ($r_2$, s) ⟶ | $m=\alpha^s y_A^{r_2'} r_2=\alpha^k$ (mod p) |

NR(p)-서명 방식에 대한 Recovery-equation attack:

● 입 력 : 없음.

● 출 력 :

① M ∈R $Z_p$, U, V ∈R $Z_q$

② 메시지 m=M · $y_A^e$ (mod p) 라 하자.

③ $r_2=M \cdot \alpha^U \cdot y_A^V$ (mod p) 로 놓는다.

④ i) a · k≡b+c · $x_A$(mod q)↔k=s+$x_A$ · $r_2'$ (mod q)
⇒(a=1, b=s, c=$r_2'$)

ii) $(M \cdot y_A^e) \cdot \alpha^{-b/a} \cdot y_A^{-c/a}$(mod p) = $M \cdot \alpha^U \cdot y_A^V$ (mod p)
$M \cdot \alpha^{-b/a} \cdot y_A^{e-c/a}$(mod p) = M · $\alpha^U \cdot y_A^V$ (mod p)
$M \cdot \alpha^{-s} \cdot y_A^{e-r2'}$(mod p) = M · $\alpha^U \cdot y_A^V$ (mod p)

iii) ∴ s=−U, e=V+$r_2'$

⑤ ∴($r_2=M \cdot \alpha^U \cdot y_A^V$, s=−U) for $m=M \cdot y_A^{V+r_2}$

## 5. 특수 디지틀 서명방식에 대한 공격 방법

### 5.1 부인방지 서명방식의 안전성 분석

일반적인 디지틀 서명방식은 서명문과 서명자의 공개키만을 사용하여 서명의 정당성을 확인할 수 있는 자체 인증 기능을 갖고 있다. 이러한 공개키 암호 시스템을 이용한 일반적인 디지틀 서명 방식은 공개키가 모든 사용자에게 공개되므로 누구든지 서명의 진위를 확인할 수 있게되어 필요 이상의 과다한 인증 기능을 제공하게 되며 이로 인해 개인의 이익 또는 사생활이 노출될 가능성이 있게 된다. 따라서 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 인증을 위해서는 반드시 서명자의 도움을 받아야 하는 서명 방식을 부인방지 서명 방식[5][6]이라 한다.

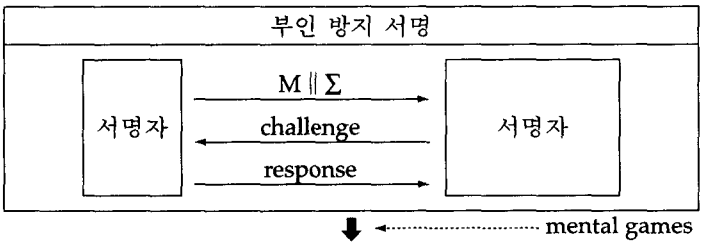
그러나, Yvo Desmedt은 secure mental game(개념도 5.1 참조)과 divertible zero-knowledge 방식(개념도 5.2 참조)을 사용하여 서명자가 모르는 다수의 검증자들도 서명자로부터 서명의 정당성을 확인받을 수 있는 방법이 존재한다는 것을 지적하였다. 즉, 부인방지 서명 방식의 본래의 목적과 달리 서명자가 자신이 발행한 서명의 남용을 통제할 수 없게된다.

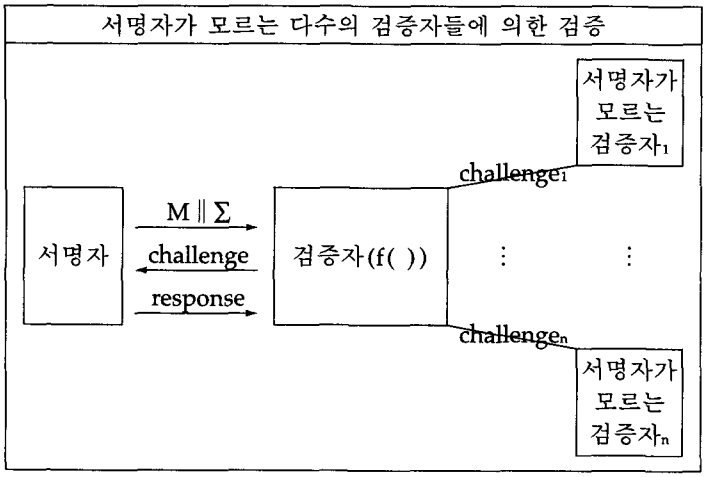
#### 5.1.1 서명자가 모르는 다수의 검증자들에 의한 검증[7][9]

1) "distributed secure mental games" 방식을 사용하는 방법

본래의 부인 방지 서명방식의 확인 과정은 개념도 5.1의 그림과 같이 서명자와 검증자간의 challenge/response 프로토콜을 통해 서명의 정당성을 검증자에게 확인시켜 주는 절차가 필요하다. 그러나, 이때 검증자가 challenge 값을 서명자가 지정하지 않은 다수의 또 다른 검증자들의 challengei 값으로 부터 계산하여 프로토콜을 수행할 경우, 서명자가 모르는 다수의 검증자들도 서명의 정당성을 확인 받을 수 있게된다. 그러나 challengei 값들을 통해 challenge 값을 계산하는 과정에서 서명자가 모르는 검증자들 중 한 사람이라도 서명자와 공모를 하게 된다면, 검증자들은 challenge/response 프로토콜의 결과를 신뢰할 수 없게된다. 따라서 이러한 문제점을 해결하기 위하여 검증자가 secure mental game을 이용하여 challenge 값을 계산하게 되면, 다수의 검증자들은 프로토콜의 결과를 신뢰할 수 있게된다. (단, 여기서의 secure mental game이란 다수의 사람들이 각각의 입력을 통해 어떠한 결과를 계산해내지만, 각각의 사람들은 자신의 입력값과 계산의 결과값 외에, 다른 사람의 입력값에 대해서는 전혀 알 수 없는 암호학적 알고리즘을 말한다.)

(가) 개 요





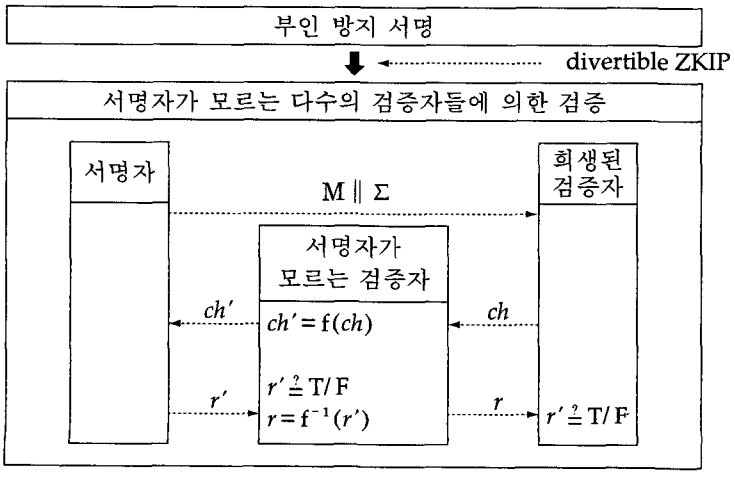

※ challenge=f(challenge$_1$, ···, challenge$_n$) where,
f( ) is "distributed secure mental games"

[개념도 5.1] "distributed secure mental games" 방식을 사용하는 방법

2) "divertible zero-knowledge proofs"를 이용하는 방법

(가) 개 요

앞에서 설명하였듯이, 부인 방지 서명방식에서 서명의 정당성을 확인 시켜주는 확인 과정은 서명자와 검증자 사이의 영지식 대화형 증명 프로토콜(ZKIP)을 통해 이루어진다. 그러나 이때, 서명자가 모르는 검증자가 서명자와 검증자간의 통신에 끼어 들어, challenge/response 값을 개념도 5.2에서와 같이 변형시키면 서명자와 검증자 사이 뿐만 아니라, 서명자와 서명자가 모르는 검증자 사이에도 ZKIP이 성립하여(이러한 것을 divertible ZKIP이라 한다.) 서명의 정당성을 확인 받을 수 있게 된다.



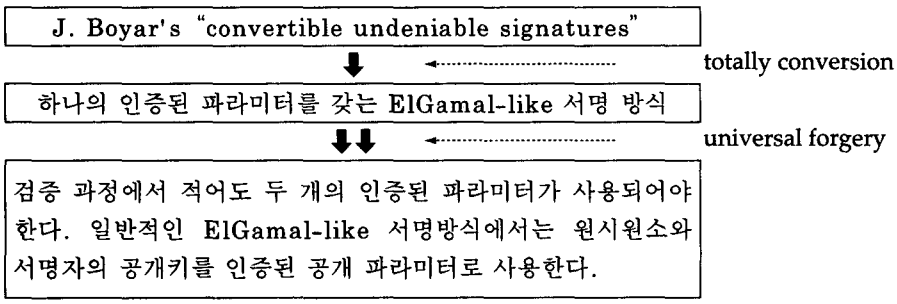

※ (f, $f^{-1}$)is "divertible ZKIP function"

[개념도 5.2] "divertible zero-knowledge proofs" 이용하는 방법

### 5.2 convertible한 부인방지 서명방식의 안전성 분석[17]

J. Boyar는 서명자의 비밀키 중 일부를 노출시킴으로써 특정 부인 방지 서명 또는 전체 부인 방지 서명을 보통의 디지틀 서명으로 변환시킬 수 있는 서명 방식인 convertible한 부인방지 서명방식[4]을 제안하였다. 그러나 Markus Michels 등은 검증 과정에서 하나의 인증된 공개 파라미터만을 사용하는 ElGamal 형 부인방지 서명방식은 total conversion을 한 후에는 임의의 메시지에 대한 서명의 위조가 가능하다는 것을 지적하였다 (개념도 5.3 참조).

(가) 개 요




[개념도 5.3] convertible한 부인방지 서명방식의 안전성 분석

## 6. 키분배 프로토콜에 대한 공격 방법

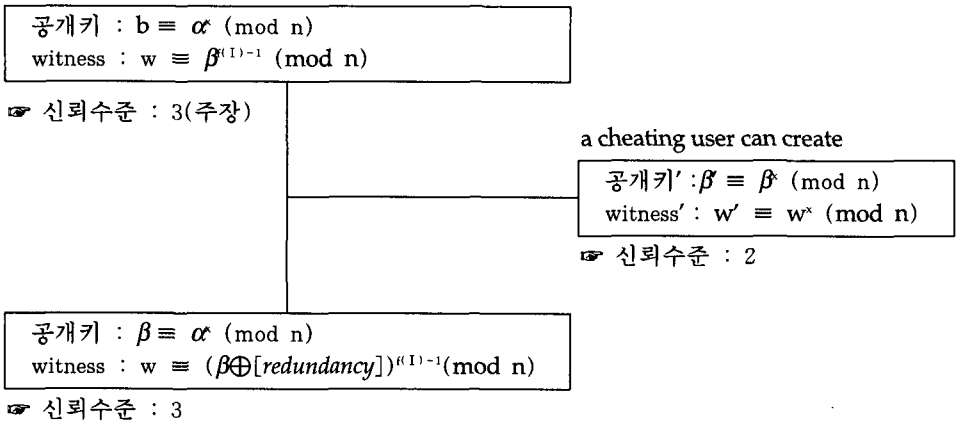
### 6.1 Saeednia의 자체인증 공개키 기반 키 분배 프로토콜의 안전성 분석[12]

ACISP(Australasian Conference on Information Security and Privacy)'96 국제학술회의에서, S. Saeednia등은 통신량과 계산량이 적은 효율적인 개인식별 정보(ID-based)에 기반한 키분배 프로토콜과 자체 인증 공개키(self-certified public key)에 기반한 키분배 프로토콜을 제안하였다.

더욱이 그들이 제안한 자체 인증 공개키에 기반한 방식은, M. Girault의 방식과 비교할 때, 사용자의 (공개키, 개인식별정보) 쌍으로부터 사용자의 공개키를 파생하는데 추가적인 TTP(Trusted Third Party)의 공개키를 필요로 하지 않는다는 장점이 있다.

김승주 등은 S. Saeednia 등의 키 분배 방식에서 일단 TTP로부터 자체 인증 공개키를 발급 받으면 이로부터 누구라도 자신의 개인식별정보에 대응하는 또 다른 자체 인증 공개키를 위조할 수가 있으므로, 그들의 주장과는 달리, M. Girault가 제안한 신뢰수준 3을 만족하지 않음을 지적하였다 (개념도 6.1 참조).

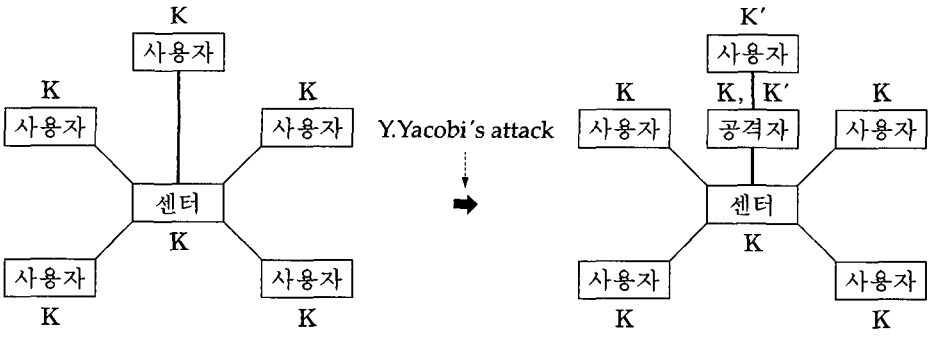
(가) 개 요




[개념도 6.1] Saeednia의 자체인증 공개키 기반 키 분배 프로토콜의 안전성 분석

### 6.2 Koyama-Ohta의 ID -기반 회의용 키 분배 프로토콜의 안전성 분석[25]

Koyama와 Ohta는 Crypto'87 국제 회의에서 개인식별 정보에 근거한 (identity based) 회의용 키 분배 프로토콜을 제안하였다. 그들은 ring형, complete graph형, star형 등 세 가지 형태의 키 분배 방식을 제안하였는데, 이 중에서 star형이 가장 실용적이므로 회의용 키분배 방식으로 제일 적합하다. 그러나 Y. Yacobi는 Koyama-Ohta의 star형 키 분배 방식이 능동적인 공격자의 middleperson attack으로부터 안전하지 않음을 지적하였다. 즉, 능동적인 공격자는 star형 네트워크에서 센터와 사용자 사이에 위치하여 센터에게 있어서는 사용자를, 사용자에게 있어서는 센터를 각각 흉내내어 서로 간의 공통키를 공유할 수 있게 된다. 더욱이 이 경우에 센터와 능동적인 공격자 사이에 공유된 키는 해당 그룹의 나머지 구성원과도 대응된다 (개념도 6.2 참조).




[개념도 6.2] Koyama-Ohta의 ID -기반 회의용 키 분배 프로토콜의 안전성 분석

## 7. 기타 공격 방법

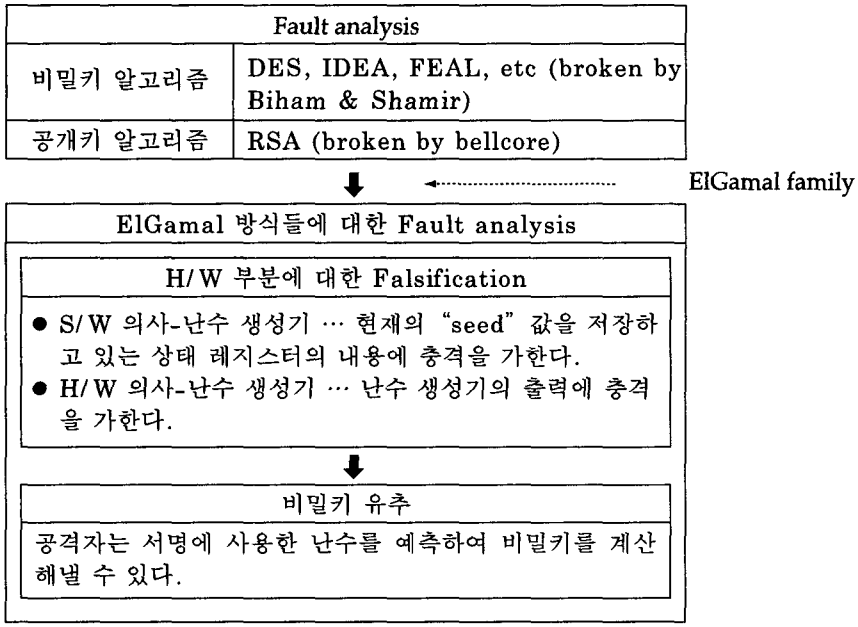
### 7.1 ElGamal형 서명 방식에 대한 fault analysis[26]

Fault analysis란 tamper-proof 장치에 특별한 형태의 물리적인 충격을 가하여 스마트 카드의 내부 연산 과정에 영향을 주거나 레지스터에 저장된 비밀키의 일부를 변형시킴으로써, 잘못된 결과 값을 얻어내어 이로부터 비밀키와 관련된 정보를 유추해내는 공격방법을 말한다.

Biham과 Shamir는 DES, IDEA, FEAL 등과 같은 비밀키 알고리즘의 fault analysis를 제안하였고, Bellcore 연구소에서 공개키 알고리즘 중 RSA 방식의 fault analysis에 대한 연구를 하였다.

그후에 AsiaCrypto'96에서 Yuliang Zheng은 스마트 카드의 난수 생성기에 충격을 가하는 방식으로 ElGamal 방식들에 대한 fault analysis를 제안하였다. (개념도 7.1 참조)

(가) 개 요




[개념도 7.1] ElGamal형 서명 방식에 대한 fault analysis

## 8. 결 론

본 고에서는 이산대수를 구하는 알고리즘과 이산대수 문제에 기반한 암호 프로토콜 자체의 안전성 등으로 나누어 이산대수 문제에 기반한 암호 시스템의 안전성에 관한 여러 가지 문제점들을 살펴보았다. 본 고에서 고찰한 바와 같이 안전한 암호 시스템을 설계하기 위해서는 안전한 공개 파라미터들의 선택과 더불어 프로토콜 자체의 안전성에도 많은 주의를 기울여야 한다. 따라서, 본 연구는 기존에 제안된 이산대수 문제에 기반한 여러가지 암호 시스템의 안전성 분석 및 앞으로 개발될 새로운 암호 시스템의 설계에 많은 도움을 줄것으로 사료된다.

## 참 고 문 헌


[1] R. Anderson and S. Vaudenay, "Minding your p's and q's", In Advances in Cryptology - ASIACRYPT'96, LNCS 1163, Springer-Verlag, 1996, pp.15-25.

[2] D. Bleichenbacher, "Generating ElGamal signatures without knowing the secret key", In Advances in Cryptology - EUROCRYPT'96, LNCS 1070, Springer-Verlag, 1996, pp.10-18.

[3] B. den Boer, "Diffie-Hellman is as strong as discrete log for certain primes", In Advances in Cryptology - CRYPTO'88, LNCS, Springer-Verlag, 1988, pp. 530-539

[4] J. Boyar, D. Chaum, I. Damgard and T. Pedersen, "Convertible undeniable signature", In Advances in Cryptology - CRYPTO'90, LNCS, Springer-Verlag, 1990, pp. 195-207.

[5] D. Chaum and H. Antwerpen, "Undeniable signature", In Advances in Cryptology - CRYPTO'89, LNCS, Springer-Verlag, 1989, pp. 212-216.

[6] D. Chaum, "Zero-knowledge undeniable signature", In Advances in Cryptology - EUROCRYPT'90, LNCS, Springer-Verlag, 1990, pp. 459-464.

[7] D. Chaum, "Some weaknesses of "eaknesses of undeniable signatures" In Advances in Cryptology - EUROCRYPT'92, LNCS, Springer-Verlag, 1992, pp. 554-556.

[8] D. Copersmith, A.M. Odlzyko, R. Schroeppel, "Discrete logarithms in GF(p)", Algorithmica, 1, pp. 1-15, 1986.

[9] Y. Desmedt and M.Yung, "Weaknesses of undeniable signature scheme" In Advances in Cryptology - EUROCRYPT'92, LNCS, Springer-Verlag, 1992, pp. 205-218.

[10] R. Heiman, "A note on discrete logarithm with special structure", In Advances in Cryptology-EUROCRYPT'92, LNCS 658, 437-448, 1993.

[11] M.E. Hellman, J.M. Reyneri, "Fast computation of discrete logarithms in GF(q)", In Advances in Cryptology - Proceeding of CRYPTO'82, pp. 3-13, 1983.

[12] 김승주, 오수현, 원동호, "Saeednia 키 분배 프로토콜의 안전성 분석 및 개선", 한국통신학회 하계종합학술발표회 논문집 제17권/1호, 1998, pp.1001-1004.

[13] Knuth, The Art of Computer Programming - Sorting and Searching, volume 3, Addison-Wesley, Reading, Massachusetts, 1973.

[14] C.H.Lim and P.J.Lee, "A key recovery attack on discrete log-based schemes using a prime order subgroup", In Advances in Cryptology - CRYPTO'97, LNCS 1294, Springer-Verlag, 1997, pp.249-263.

[15] McCurely, "The discrete logarithm problem", C. Pomerance, editor, Cryptology and Computational Number Thoery, volume 42 of Proceeding of Symposia in Applied Mathematics, pp. 49-74, American Mathematical society, 1990.

[16] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, "Handbook of Applied

Cryptography", CRC Press, pp.103-113.

[17] M. Michels, H. Petersen and P. Horster, "Breaking and repairing a convertible undeniable signature scheme", Proc. of 3rd ACM Conference on Computers and Communications Security, ACM Press, 1996, pp.148-152.

[18] A. Miyaji, "Weakness in message recovery signature schemes based on discrete logarithm problems 1", IEICE Japan Tech. Rep., ISEC95-11, 1994, pp. 47-57.

[19] A. Miyaji, "Weakness in message recovery signature schemes based on discrete logarithm problems 2", IEICE Japan Tech. Rep., ISEC95-35, 1994, pp. 31-38.

[20] A.M. Odlyzko, "Discrete logarithms and smooth polynomials", G.L. Mullen and P.j-s. Shiue, editors, Finite Fields : Theory, Applications and algorithms, volume 168 of contemporary Mathematics, 269-278, American Mathematical society, 1994.

[21] P.C. van Oorschot and Michael J.Wiener, "On Diffie-Hellman Key Agreement with Short Exponents", In Advances in Cryptology - EUROCRYPT'96, LNCS 1070, Springer-Verlag, 1996, pp.332-343

[22] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance", IEEE Trans. Inform. Theory, IT-24(1), 1978, pp.106-110

[23] J.M. Pollard, "Monte Carlo method for index computation (mod p)", Mathematics of Computation, 32, pp. 918-924, 1978.

[24] S. Vaudenay, "Hidden collision on DSS", In Advances in Cryptology - CRYPTO'96, LNCS 1109, Springer-Verlag, 1996, pp.83-88.

[25] Y. Yacobi, "Attack on the Koyama-Otha Identity based Key distribution scheme", In Advances in Cryptology - CRYPTO'87, Springer-Verlag, 1987, pp. 429-433

[26] Y. Zheng, T.Matsumoto, "Breaking Smart Card Implementation of ElGamal signature and its variants", In Advances in Cryptology - ASIACRYPT'96, LNCS 1163, Springer-Verlag, 1996, (rump session).

[27] 한국전자통신연구소 (연구수행기관 : 포항공과대학), "모듈라 멱승에 바탕을 둔 키이 분배방식에 관한 연구", 최종연구보고서

[28] 오수현, 김승주, 원동호, "특수 디지틀 서명 방식의 상호관계 모델링에 관한 연구", 한국통신학회 하계종합학술발표회 논문집 제17권/1호, 1998, pp.989-992.

## □ 著者紹介


오 수 현

1998년 2월 성균관대학교 정보공학과 졸업(공학사)
1998년 3월 ~ 현재 성균관대학교 전기전자 및 컴퓨터 공학부 석사 과정

이 형 규

1996년 2월 성균관대학교 정산업공학과 졸업(공학사)
1998년 3월 ~ 현재 성균관대학교 전기전자 및 컴퓨터 공학부 석사 과정

김 승 주

1994년 2월 성균관대학교 정보공학과 졸업(공학사)
1996년 2월 성균관대학교 정보공학과 대학원 졸업(공학석사)
1999년 2월 성균관대학교 정보공학과 대학원 졸업(공학박사)
1999년 ~ 현재 한국정보보호센터 선임연구원

원 동 호

1976년 2월 성균관대학교 전자공학과 졸업(공학사)
1978년 2월 성균관대학교 대학원 졸업(공학석사)
1988년 2월 성균관대학교 대학원 전자공학과(공학박사)
1978년 4월 ~ 1980년 3월 한국전자통신연구소 연구원
1985년 9월 ~ 1986년 8월 일본 동경공대 객원 연구원
1982년 3월 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 교수
1996년 4월 ~ 1998년 4월 정보화 추진위원회 자문위원
1999년 ~ 현재 한국통신정보보호학회 부회장
1999년 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 학부장
1999년 ~ 현재 성균관대학교 정보통신대학원 원장

※ 주관심 분야 : 암호이론, 정보이론