땋임군에서의 개인식별기법의 제안

김진, 김광조*

*국제정보보호기술연구소

*한국정보통신대학원대학교, 공학부

A New Identification Scheme Based on Conjugacy Problem

Zeen Kim and Kwangjo Kim*

*International Research center for Information Security (IRIS)

*School of Engineering, Information and Communications Univ. (ICU)

요 약

2000년 고기형 등이 발표한 땋임군상에서의 공개키 암호시스템은 후속적으로 다양한 이론적 분석 및 응용기법이 연구되고 있다. 땋임군에서의 공개키 암호화기법과 서명기법은 기존에 제안되었으나 개인식별기법은 제안된 바가 없다. 본 논문에서 우리는 땋임군에서의 서명기법에 바탕을 둔 개인식별기법을 제안하고 그 안전성을 증명한다.

I. 서론

땋임암호(braid cryptosystem)은 2000년 고기형 등 [1] 이 CRYPTO 2000에서 제안하였다. 땋임군에서의 공액문제(conjugacy problem)의 어려움에 기반을 두었으며 새로운 공개키 암호 시스템으로 주목을 받았다. 이후 차재춘 등 [2] 이 땋임암호의 구현 결과를 제시하였고, 서명기법 [3], 의사난수성 연구 [4], 공액문제의 해결기법 [5, 6] 등 현재까지 활발한 연구성과를 보이고 있다.

개인식별기법은 암호학적 응용의 한가지로 증명자가 자신의 신원을 검증자에게 비밀정보의 누설없이 확인시키는 방법이다. Fiat-Shamir가 최초의 개인식별기법을 제안하였고, 그 뒤로 Schnorr, 김명선 등이 새로운 개인식별기법들을 꾸준히 제안하였다.

본 논문은 땋임군에서의 개인식별기법을 제안하고, 그 기법이 증명가능한 안전성을 보장함을 보인다. 또한 기존의 기법과의 개인식별기법의 요구사항면에서 어떠한 특징을 지니고 있는지를 비교, 분석한다. 논문의 구성은 우선 2장에서 땋임군에서의 서명기법과 기존의 개인식별기법들을 소개하고, 3장에서 제안하는 땋임군에서의 개인식별기법을 소개한다. 4장에서는 제안 기법이 증명가능한 안전성을 지님을 보이고 마지막 5장에서 결론을 내린다.

II. 관련연구

1. 땋임암호에서의 서명기법

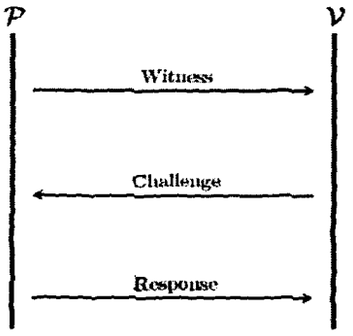
고기형 등은 [3]에서 틈(gap)을 갖는 땋임군에서의 서명기법을 제안하였다. 이러한 군은 공액찾기문제(conjugacy searching problem)와 공액매칭문제(conjugacy matching problem)는 계산적으로 해결불가능하나 공액결정문제(decision conjugacy problem)을 해결하는 알고리즘이 존재하는 군이다.

2. 기존의 개인식별기법

본 절에서는 영지식 개인식별기법(zero-knowledge identification)에 대해서 설명하고, 기존에 제안된 개인식별기법을 소개한다.

2.1 영지식 개인식별기법

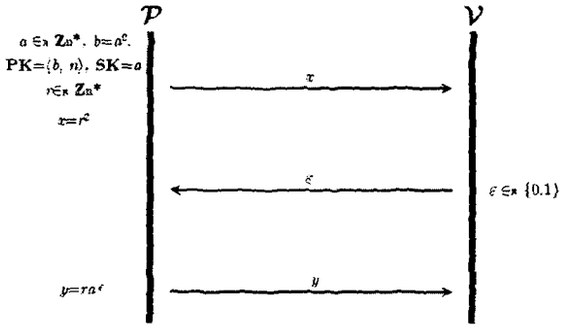
영지식 개인식별기법은 우선 키생성 알고리즘을 통해 공개키와 비밀키쌍을 출력한뒤, 증명자(P)와 검증자(V) 사이의 3회에 걸친 교신(그림 1)을 t번 반복하는 과정을 통해서 검증자는 해당 증명자의 신원을 확인할 수 있게 하는 기법이다. 이러한 개인식별기법은 신원위조공격방법의 성공확률을 최소화 할 수 있다는 특징이 있다.



(그림 1) 영지식 개인식별기법의 중간인터랙션

2.2 Fiat-Shamir

Fiat과 Shamir는 CRYPTO '86에서 소인수분해의 어려움에 기반한 개인식별기법을 제안하였다[7]. 이 기법은 우선 키생성 알고리즘이 동작하여 두 개의 서로 다른 소수의 곱인 원소 $a \in Z_n^*$를 랜덤하게 선택하고, $b=a^2$ 를 계산한다. 키생성 알고리즘은 공개키값으로 $\langle b, n \rangle$, 비밀키값으로 a를 출력한다. 이후 t번동안 중간인터랙션을 반복한다. 중간 인터랙션의 구체적인 방법은 (그림 3)과 같다. 검증자는 $y^2 = x \cdot b^e$ 인 경우 accept를 그렇지 않은 경우 reject를 출력한다.



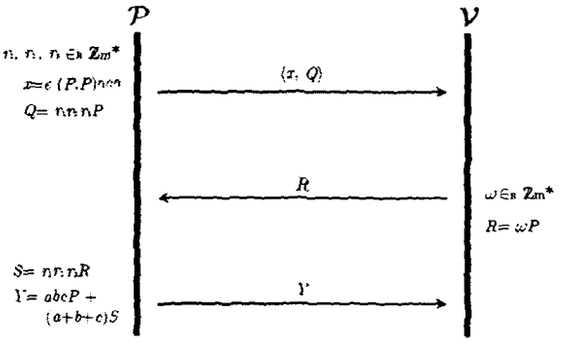
(그림 2) Fiat-Shamir 식별기법

이 기법은 소인수분해 문제가 어려운 경우 능동적 공격자에대해 안전하다.

2.2 Kim-Kim 개인식별기법

ACISP 2002에서 김명선과 김광조는 Weil-pairing을 사용하여 쌍일차 디피-헬만 문제의 어려움에 기반한 개인식별기법을 제안하였다[8].

키생성 알고리즘은 위수가 m인 (m은 큰 소수) 두 개의 순환군 G_1, G_2를 생성하고, 쌍일차함수 $e: G_1 \times G_1 \rightarrow G_2$를 생성한다. 그리고 G_1의 생성원 $P \in G_1$을 생성한다. 그리고 랜덤한 값 $a, b, c \in Z_m^*$를 선택한 뒤 를 계산한다. 키생성 알고리즘은 공개키로 $\langle G_1, G_2, P, aP, bP, cP, e, v \rangle$를, 비밀키로 $\langle a, b, c \rangle$를 출력한다. 이후 t번 동안 중간 인터랙션을 행한다. 중간 인터랙션의 구체적인 방법은 (그림 3)과 같으며, 검증자는 $x = e(P, Q)$와 $e(Y, P) = v \cdot e(aP + bP + cP, Q)^{\omega}$ 둘 모두 만족하는 경우 accept를 그렇지 않은 경우 reject를 출력한다.



(그림 3) Kim-Kim 식별기법

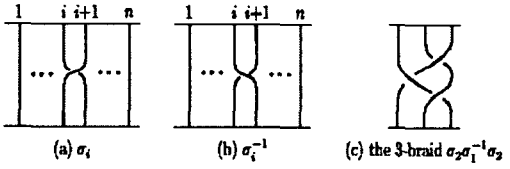
저자들은 제안기법이 능동적 공격자에 대하여 안전함을 증명하였고, 증명자의 사전 계산량과 증명자와 검증자 양쪽의 온라인 계산 오버헤드에서 기존 기법들보다 효율적임을 설명하였다.

3. 땋임군에서 정의된 어려운 문제들

본 절에서는 땋임군 상에서의 어려운 문제들을 기술한다. 우선 문제들을 소개하기 전에 땋임군과 본 논문에서 사용하게될 기호에 대해서 소개한다.

3.1 땋임군

땋임군은 기하학적인 땋임으로부터 정의된 비가환 무한군이다. 쉽게 말해서 땋임군 B_n은 n개의 끈이 막대기에 한쪽 끝을 묶은 상태에서 아래로 쳐진 n개의 끝을 서로 꼰 다음, 끈의 밑을 다른 막대기에 묶은 상태를 군의 원소로 정의한 것이다. (그림 4)는 땋임 군의 두선을 꼰 경우와 그 역원과 B_3 내의 한 원소를 나타낸 것이다.



(그림 4) 땋임군의 표현

이제 기본적인 개념들과 용어를 소개한다. 땋임군 B_n의 두 원소 x, y가 공액(conjugate)이라는 것은 $y=a^{-1}xa$ 를 만족하는 적당한 $a\in B_n$ 가 존재함을 말하고, $x\sim y$ 로 표기한다.

3.2 공액문제들

이제 땋임군에서 정의된 어려운 문제들을 소개한다.

- **Conjugacy Search Problem (CSP)**
  - Instance : $(x, y) \in B_n \times B_n$ such that $y=a^{-1}xa$ for some $a \in B_n$
  - Objective : Find $b \in B_n$ such that $y=b^{-1}xb$

- **Conjugacy Decision Problem (CDP)**
  - Instance : $(x, y) \in B_n \times B_n$
  - Objective : Determine whether $x \sim y$

- **Matching Conjugacy Search Problem (MCSP)**
  - Instance : A CSP-hard pair $(x, x') \in B_n \times B_n$, $y \in B_n$
  - Objective : Find $y' \in B_n$ such that $y \sim y'$, $xy \sim xy'$

- **Matching Triple Search Problem (MTSP)**
  - Instance : A CSP-hard pair $(x, x') \in B_n \times B_n$, $y \in B_n$
  - Objective : Find a triple $(\alpha, \beta, \gamma) \in B_n \times B_n \times B_n$ such that $\alpha \sim x$, $\beta \sim \gamma \sim y$, $\alpha\beta \sim xy$, $\alpha\gamma \sim x'y$

이들 중 제안기법은 **CSP는 해결불가능하고 CDP는 해결가능한 땋임군에서 정의된다.** 또한 제안기법의 안전성을 MTSP의 어려움에 그 기반을 두고 있다. 이들 문제 사이의 관계는 [3]에 정리되어 있다.

III. 제안기법

이 장에서는 틈을 가진 땋임군에서의 개인식별 기법을 제안한다. 우리가 제안하는 기법은 고기형 등의 서명기법에 기반하고 있으며, 그 안전성 역시 동일하다는 점이 증명된다.

제안 알고리즘은 키생성, 영지식 개인식별기법을 이용하고 있으며, 구체적 기법은 아래와 같다.

- **키생성**

  Public key : CSP-hard pair $(x, x') \in B_n \times B_n$

  Secret key : a $(x' = a^{-1}xa)$

- **$\mathcal{P}$ sends to $\mathcal{V}$**

  $\mathcal{P}$ choose s at random and compute $X=s^{-1}xs$, $X'=a^{-1}Xa$

  $\mathcal{P}$ sends X, X'

- **$\mathcal{V}$ sends to $\mathcal{P}$**

  $\mathcal{V}$ choose r at random

  $\mathcal{V}$ sends r

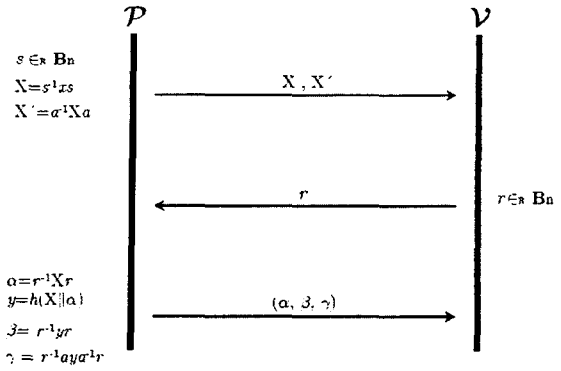
- **$\mathcal{P}$ sends to $\mathcal{V}$**

  $\mathcal{P}$ computes $\alpha=r^{-1}Xr$, $y=h(X\|\alpha)$, $\beta = r^{-1}yr$, $\gamma = r^{-1}ayar^{-1}r$

  $\mathcal{P}$ sends (α, β, γ)

- **$\mathcal{V}$ outputs accept or reject**
  - **accept** *if* $x \sim X$, $\alpha \sim X$, $\beta \sim \gamma \sim y$, $\alpha\beta \sim Xy$, $\alpha\gamma \sim X'y$
  - **reject** : *otherwise*

아래의 (그림 5)는 제안기법의 중간인터랙션을 나타내고 있다.



(그림 5) 제안기법

IV. 안전성 분석

이 장에서는 제안기법의 안전성을 증명한다. 제안기법의 안전성은 땋임군에서의 서명기법과 동일함을 증명하고, 나아가서 제안된 개인식별기법에서 신원위조(impersonation)가 가능한 공격자가 직접 땋임군에서의 MTSP를 해결할 수 있을 보인다.

[정리 1] *제안기법을 (t,q_I,ε)-신원위조할 수 있는 공격자는 [3]의 서명에서 (t',q_S,ε')-알고리즘으로 서명값을 위조가능하다.*

(증명 개요) 만약 제안 기법이 수동적공격자의 신원위조공격에 대하여 (t,q_I,ε)-안전하다고 가정하자. 신원위조자 I는 (t,q_I,ε)-공격자라고 둘 수 있다. 이제 우리는 [3]의 서명기법이 (t',q_S,ε')-안전하지 않음을 보이고, t',ε',q_S의 값을 구할 것이다. 먼저 서명기법의 위조자 F는 공개키 PK를 입력받아서 신원위조자 I에게 전달한다.

<Phase 1>
신원위조자 I는 X_i를 서명위조자 F를 이용하여 서명오라클에게 질문하고, 그 결과값 $d_i=(\alpha_i,\beta_i,\gamma_i)$을 넘겨받는다. 이러한 과정을 여러 차례 반복한 뒤 공개된 신원 X를 출력한다. 단, 여기서 $X\neq X_i$ 이다.

<Phase 2>
I는 X에 대한 몇가지 사본신원을 질문한다. 서명알고리즘은 Δ회 영지식 프로토콜을 갖고 있으므로 시뮬레이터 S가 존재한다. S의 출력값은 서로 주고받은 메시지 (Cmt, Ch, Rsp)이다. I가 질문을 하면 F는 S로 시뮬레이션을 시행한다. 시뮬레이션의 결과값이 (Cmt, Ch, Rsp)라고 두면, F는 이를 I에게 전달한다.

<Phase 3>
이제 I는 거짓 증명자(cheating prover)가 되어 검증자에게 자신의 신원을 증명한다. 이때 검증자는 F가 된다. 첫 번째 작동을 끝낸뒤 F는 I를 reset하고 다시 프로토콜을 동작한다. 이 두 번의 경우로 출력된 사본신원을 (Cmt1, Ch1, Rsp1), (Cmt2, Ch2, Rsp2)라고 두자.
Bellare와 Paracio가 [9]에서 소개한 **reset lemma**에 의해 우리는 비밀값 $d=(\alpha,\beta,\gamma)$를 구할 수 있다. 이상을 통해 주어진 메시지 X에 대한 서명쌍 $(X,(\alpha,\beta,\gamma))$를 구하게된다.

이상의 서명위조자가 서명위조에 성공하는 데 걸리는 시간은,

$t'=2t+poly(k)$, $q_S=q_I$, $\varepsilon'\geq(\varepsilon-\frac{1}{\Delta})^2$이 된다. ■

[정리 2] *[3]의 서명기법이 (t,q_S,ε')에 대해 안전하지 않으면 MTSP를 해결하는 (t',ε')-알고리즘을 생성할 수 있다.*

위 정리는 [3]에서 그 완전한 증명이 주어져 있다.

[정리 3] *제안기법을 (t,q_I,ε)-신원위조할 수 있는 수동적 공격자는 MTSP를 해결하는 (t',ε')-알고리즘을 생성할 수 있다.*

(증명) [정리 1]과 [정리 2]로부터

$t' = 2t + poly(k)$, $\varepsilon'' \geq \frac{(\varepsilon - \frac{1}{\Delta})^2}{q_I}$ 임을 쉽게 이끌어낼 수 있다. ■

이상을 통해 제안기법이 수동적 공격자의 신원 위조공격에 대해 안전함이 증명되었다.

V. 결론 및 향후 연구과제

본 논문에서 우리는 땋임군의 MTSP의 어려움에 기반한 개인식별기법을 제안하고 수동적 공격자에 대한 안전성을 증명하였다. 개인식별기법은 암호학의 주요 응용 중의 하나로 본 기법이 땋임군에서의 암호시스템 응용부분의 발전에 기여할 것을 본다.

아직 제안기법이 능동적 공격자에 대해 안전한지 여부에 관한 고찰이 필요하고, 능동적 공격자에 대해 안전한 땋임군에서의 개인식별기법을 제안할 예정이다.

참고문헌

[1] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang and C. S. Park, "New Public-Key Cryptosystem Using Braid Groups," *Advances in Cryptology - CRYPTO 2000*, LNCS 1880, pp. 166-183, Springer-Verlag, 2000.

[2] J. C. Cha, K. H. Ko, S. J. Lee, J. W. Han and J. H. Cheon, "An Efficient Implementation of Braid Groups," *Advances in Cryptology - Asiacrypt 2001*, LNCS 2248, pp. 144-156, Springer-Verlag, 2001.

[3] K. H. Ko, D. H. Choi, M. S. Cho, and J. W. Lee, "New Signature Scheme Using Conjugacy Problem," Preprint ; http://eprint.iacr.org/2002/168

[4] E. K. Lee, S. J. Lee, and S. G. Hahn, "Pseudorandomness from Braid Groups," *Advances in Crptology - CRYPTO 2001*, LNCS 2139, pp. 486-502, Springer-Verlag, 2001.

[5] E. K. Lee and J. H. Park, "Cryptanalysis of the public-key encryption based on braid groups," *Advances in Cryptology - Eurocrypt 2003*, LNCS 2656 , pp. 477-490 , Springer-Verlag, 2003.

[6] J. H. Cheon and B. Jun, "A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem," *Advances in Cryptology-CRYPTO 2003*, LNCS 2729, Springer-Verlag, 2003.

[7] A. Fiat and A. Shamir, "How to prove yourself: pratical solutions to identification and signature problems", *Advances in Cryptology-Crypto'86*, LNCS 263, Springer-Verlag, pp. 186-194, 1987.

[8] M. Kim and K. Kim, "A new identification scheme based on bilinear Diffie-Hellman Problem," *7th Australasian Conference on Information Security and Privacy - ACISP '02*, LNCS 2384, pp. 362-378, Springer-Velrag, 2002.

[9] M. Bellare and A. Palacio, GQ and Schnorr identification schemes ; proofs of security against impersonation under active and concurrent attacks, Advances in Cryptology - CRYPTO 2002, LNCS 2442, pp. 162-177, Springer-Verlag, 2002

[10] M. Abdalla, J. An, M. Bellare, and Namprempre,. "From identification to signatures via the Fiat-Shamir transform : minimizing assumptions for security and forward-security," *Advances in Cryptology - EUROCRYPT'02*, LNCS 2332, pp. 418-433, Springer-Velrag, 2002.

[11] V. Shoup, "On the security of a practical identification scheme," *J. Cryptology* 12, pp. 247-260, Springer-Velrag, 1999.

[12] C. Schnorr, "Security of 2^t-root identification and signatures," *Advances in Cryptology - Crypto '96*, LNCS 1109, pp. 143-156, Springer-Velrag, 1996.