안전하고 효율적인 이진 필드상의 페어링 알고리즘[1)]

최두호 한동국 김호원

한국전자통신연구원

{dhchoi,christa,khw}@etri.re.kr

Efficient and Secure Pairing Algorithm over Binary Fields

Choi, Dooho Han, Dong-Guk Kim, Howon

Electronics and Telecommunications Research Institute(ETRI)

요약

최근 PKI-less 공개키 암호 시스템에 대한 연구가 진척되면서, 페어링(Pairing) 기반의 암호 시스템이 주목을 받고 있다. 페어링 기반의 암호 시스템은 두 개의 타원 곡선 상의 점을 유한체의 값으로 보내는 양방향 선형성(Bilinearity)을 가지는 페어링 함수를 기반으로 구성되는 암호 시스템이다. 페어링 기반의 암호 시스템 구현을 위해서는 페어링 연산 알고리즘이 필수적이며, 효율적인 페어링 연산을 위한 많은 연구가 진행되고 있다. 이러한 페어링 알고리즘에도 기존의 타원곡선 스칼라곱 알고리즘에서 야기되었던 부채널 공격이 동일하게 적용되기 때문에, 안전한 페어링 알고리즘을 위해서는 부채널 공격에 대한 저항성을 갖는 알고리즘이 필요하다.

이에 본 논문에서는 부채널 공격에도 안전하면서 비교적 효율적인 이진 필드 상의 페어링 알고리즘을 제시한다. 본 페어링 알고리즘은 기존의 부채널 공격 저항성을 갖는 페어링 알고리즘 중 가장 효율적인 알고리즘에 비해 효율성이 17% 정도 향상되었다.

1. 서론

최근 타원 곡선상의 페어링은 ID 기반 암호화 기법[1,2], ID 기반 서명[3,4,5], 3-party 키 공유 기법[6], 짧은 서명 기법[7], ID-기반 인증 키 공유 기법[8] 등 다양한 암호 프로토콜에 적용되고 있다. 페어링을 이용한 암호 프로토콜의 주요 구현 어려움은 페어링 연산으로부터 기인하게 때문에, 효율적인 페어링 연산 구현에 대한 다양한 방법들이 제시되고 있다. Barreto et al.[9]과 Galbraith et al.[10]은 페어링 연산의 기본 알고리즘인 Miller 알고리즘[11]에서 불필요한 연산을 제거함으로써 효율적인 연산 방안을 제시하였다. Duursma and Lee[12]는 위수 3인 Field 상의 페어링 연산에 대한 공식을 제시하였고, Kwon[13]은 Binary Field 상의 페어링에 대해 유사한 결과를 유도하였다.

Tate 페어링 연산에서 중심 루프 계산을 짧게 하기 위해 Barreto et al.[14]은 초특이 타원 곡선상의 Eta 페어링 개념을 도입하였으며, 더 일반적으로 Hess et al.[15]은 일반적인 타원 곡선 상의 Ate 페어링으로 확장시켰다.

Granger et al.[16]은 위수 3인 Field 상의 Tate 페어링 연산에서 Final exponentiation을 사용하지 않고도 유일한 페어링 결과값 표현이 가능함을 증명하였으며, Shirase et al.[17]은 이를 GPS(Granger-Page-Stam) 변환이라 명명하고, 위수 3인 Field 상의 Duursma-Lee 알고리즘과 η_T 페어링에 본 변환을 적용하는 방안을 제안하였다.

부채널 공격(Side channel attacks)은 대개 암호 연산이 수행되면서 비밀정보와 중간값들과 연관되어서 발생하는 부채널 정보 - 시간, 전력 소모량, 전자기파 등 -를 이용하염 암호 시스템을 공격하는 공격 기법이다[18,19]. 페어링 알고리즘에 대한 부채널 공격에 대해서는 Page and Vercauteren[20], Whelan and Scott[21], Kim et al.[22] 등과 같은 연구 결과들이 있다. [22]에서 Kim et al.은 이진 필드상의 η_T 페어링에 대한 부채널 공격 가능성에 대해 조사하였다.

부채널 공격에 안전한 페어링 알고리즘은 [20, 21, 22, 23] 등에서 제안되었다. [20]에서는 페어링 함수의 양방향 선형성이 비밀인 타원 곡선 점을 감추기 위해 이용되었다. [23]에서는 Scott은 BKLS 알고리즘[9]에서 Miller 변수에 임의의 값을 곱하는 방법을 제안하였다. [21]에서는 알고리즘의 효율성을 위해서는, 이러한 임의의 값이 Miller 변수 뿐만 아니라 알고리즘의 모든 중간 값에 곱해져야 한다는 것을 제시하였다. [22]에서 Kim et al.은 Randomized Projective Coordinate(RPC) 방법을 Barreto et al.의 η_T 알고리즘에 직접 적용하였으며, Kim et al.의 방법이 여타의 다른 부채널 공격 방지 알고리즘보다 효율적임을 입증하였다.

본 논문에서는 Barreto et al. 알고리즘의 변형 알고리즘을 제안하고, 본 변형된 알고리즘에 RPC 방법을 적용하여 Kim et al. 알고리

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술 개발사업의 일환으로 수행하였음. [2005-S-088-03, 안전한 RFID/USN을 위한 정보보호 기술]

즘보다 17% 정도 더 효율적인 부채널 공격 방지 η_T 페어링 알고리즘을 제안한다. 본 논문의 구성은 다음과 같다. 먼저, 2장에서 이진 필드상의 타원 곡선의 페어링에 대한 정의를 살펴보고, 3장에서 Barreto et al.의 η_T 페어링 알고리즘의 변형 알고리즘을 제시하고, 변형된 알고리즘에 RPS 방법을 적용한다. 4장에서는 본 알고리즘의 필드 곱셈량을 계산하여 Kim et al.의 알고리즘보다 효율적임을 입증한다. 마지막으로, 5장에서는 본 논문의 결론을 도출한다.

2. 이진 필드의 타원 곡선 상의 페어링

본 장에서는 이진 필드 F_{2^m} 의 초특이 타원 곡선 상의 Tate 페어링[9, 13]과 Barreto at al.의 η_T 페어링[14]의 정의에 대해 살펴보고자 한다. 기본적으로 Tate 페어링과 η_T 페어링은 일반적인 유한체상에서 정의될 수 있으나, 본 논문에서는 이진 필드상의 페어링에 중점을 두기 때문에, 본 장에서는 이진 필드상의 페어링의 정의로만 제한하여 설명한다.

F_{2^m} 의 초특이 타원 곡선 상의 Tate 페어링은 다음과 같이 정의된다.

$$\tau_N : E_b(F_q)[l] \times E_b(F_q)[l] \rightarrow F_{q^k}^* / (F_{q^k}^*)^{q^2+1},$$
$$\tau_N(P,Q) = f_{N,P}(\psi(Q)),$$

여기서 $q = 2^m$, $N = 2^{2m}+1$ 이며, $\psi : E_b(F_q) \rightarrow E_b(F_{q^k})$는 distortion 함수이다. 이 때, $f_{N,P}$ 는 자신의 principal divisor $(f_{N,P})$ 가 $N(P)-(NP)-(N-1)O$ 와 동치인 유리 함수를 나타낸다. 그리고, F_{2^m}상의 페어링을 위한 타원곡선 E_b 는 $Y^2+Y=X^3+X+b,\ b=0$ or 1로 정의된다.

Barreto et al.[14]에 의해 정의된 F_{2^m}상의 η_T 페어링은 다음과 같이 정의된다.

$$\eta_T : E_b(F_q)[l] \times E_b(F_q)[l] \rightarrow F_{q^k}^* / (F_{q^k}^*)^N,$$
$$\eta_T(P,Q) = f_{T,P}(\psi(Q)),$$

여기서, $q = 2^m, N = 2^m + 1 + \epsilon 2^{(m+1)/2}$이고, $T = 2^{(m+1)/2} + \epsilon$ 이다. 이 때, ϵ은 다음과 같이 정의된다.

$$\epsilon = \begin{cases} -1 & (m = 1,7 \bmod 8, b = 1) \\ \quad \text{or} & (m = 3,5 \bmod 8, b = 0) \\ 1 & otherwise \end{cases}$$

상기 Tate 페어링과 η_T 페어링의 정의에 따라, BKLS 알고리즘[9]을 적용하면, η_T 페어링 알고리즘이 Tate 페어링 알고리즘에 비해 2배의 효율성을 기진다. 따라서, 본 논문에서는 η_T 페어링 알고리즘에 집중하여 부채널 공격 방지 기법인 RPC 방법을 적용한다.

3. 효율적인 부채널 공격 방지 η_T 페어링 알고리즘

이진 필드상의 타원 곡선의 η_T 페어링 알고리즘을 위해 다음과 같은 이진 필드 F_q, $q = 2^m$, m: 홀수 상의 타원 곡선을 정의한다.

$$E_b : Y^2 + Y = X^3 + X + b,\ b = 0,1.$$

타원 곡선 E_b의 embedding degree $k = 4$[24, 13, 14] 이고, F_q의 확장체 F_{q^4}는 다항 기저 $\{1, s, t, st\}$로 표현 가능하다. 여기서, 기저 s와 t의 관계식은 다음과 같다.

$$s^2 + s + 1 = 0,\ t^2 + t + s = 0.$$

그리고, 본 타원 곡선에서의 distortion 함수는 $\psi(x,y) = (x+s^2, y+xs+t)$로 정의된다. 이 때, 주어진 $P = (\alpha, \beta)$에 대해 $2^i P = (\alpha_i^{(2i)}, \beta_i^{(2i)})$를 만족한다. 여기서, $(x_i, y_i) = (x+i, y+ix+\epsilon_i)$, 을 의미하고, $\alpha^{(2i)}$나 $\beta^{(2i)}$는 α^{2^i}과 β^{2^i}를 각각 의미한다(보다 상세한 설명은 [13, 14]를 참조). 마지막으로 ϵ_i는 다음과 같이 정의된다.

$$\epsilon_i = \begin{cases} 0 & \text{if } 0,1 \bmod 4 \\ 1 & otherwise \end{cases}.$$

이 때, Barreto at al.[14]은 다음과 같은 η_T 페어링 알고리즘을 제시하였다.

Barreto at al.'s η_T Pairing on E_b

Input: $P = (\alpha, \beta)$ and $Q = (x, y)$
Output: $\eta_T(P, \psi(Q))$
1. $w \leftarrow \alpha + (m-1)/2$
2 $f \leftarrow w \cdot (x+\alpha+1) + y + (\beta + b + \epsilon_{(m+1)/2})$
$\quad + (w+x)s + t$
3. **for** $i = 0$ **to** $(m-1)/2$ **do**
4. $\quad w \leftarrow \alpha + (m+1)/2,\ \alpha \leftarrow \sqrt{\alpha},\ \beta \leftarrow \sqrt{\beta}$
5. $\quad g \leftarrow w \cdot (\alpha + x + (m+1)/2) + y + (\beta +$
$\quad (1-(m+1)/2)\alpha + \epsilon_{(m-1)/2}) + (w+x)s + t$
6. $\quad f \leftarrow f \cdot g$
7. $\quad$ **if** $i < (m-1)/2$ **then**
8. $\quad\quad x \leftarrow x^2,\ y \leftarrow y^2$
9. $\quad$ **end if**
10. **end for**
11. **return** $f^W = f^{(2^{2m}-1)(2^m+1-\epsilon 2^{(m+1)/2})}$

상기 알고리즘에서 루프 안에서 실행되는 4번 항목과 5번 항목을 합치면 다음과 같은 수식을 얻을 수 있다.

$$F := f_0 + f_1 s + t.$$

여기서, $f_0 = w(\alpha,\beta) \cdot x + y + c(\alpha,\beta)$, $f_1 = x + w(\alpha,\beta)$ 이고,

$$w(\alpha,\beta) = \left(\alpha + \frac{(m+1)}{2}\right),$$
$$c(\alpha,\beta) = \alpha^{3/2} + \frac{(m+1)}{2}\alpha + \alpha^{1/2} + \frac{(m+1)}{2} + \epsilon_{(m-1)/2}.$$

이다. 상기 수식에서 $c(\alpha,\beta)$는 다음과 같이 변형될 수 있다.

$$= (\alpha^3+\alpha)^{1/2} + \frac{(m+1)}{2}\alpha + \beta^{1/2} + \frac{(m+1)}{2} + \epsilon_{(m-1)/2}$$
by the Weierstrass equation of $E_b : Y^2+Y = X^3+X+b$,
$$= (\beta^2+\beta+b)^{1/2} + \frac{(m+1)}{2}\alpha + \beta^{1/2} + \frac{(m+1)}{2} + \epsilon_{(m-1)/2}$$
$$= \frac{(m+1)}{2}\alpha + \beta + \frac{(m+1)}{2} + b + \epsilon_{(m-1)/2}$$
$$= \frac{(m+1)}{2}w(\alpha,\beta) + \beta + b + \epsilon_{(m-1)/2},$$

즉, $c(\alpha,\beta) = \frac{(m+1)}{2}w(\alpha,\beta) + \beta + b + \epsilon_{(m-1)/2}$임을 알 수 있다. 따라서, 상기 알고리즘에서 메인 루프 부분이 다음과 같이 변형된 η_T 페어링 알고리즘을 얻을 수 있다.

Modification of main loop of η_T Pairing Algorithm

3. **for** $i=0$ **to** $(m-1)/2$ **do**
4. $w \leftarrow \alpha + (m+1)/2$
5. $g \leftarrow w \cdot x + y + (\frac{(m+1)}{2}w + \beta + b + \epsilon_{(m-1)/2}) + (w+x)s + t$
6. $f \leftarrow f \cdot g$
7. **if** $i < (m-1)/2$ **then**
8. $\alpha \leftarrow \sqrt{\alpha}$, $\beta \leftarrow \sqrt{\beta}$, $x \leftarrow x^2$, $y \leftarrow y^2$
9. **end if**
10. **end for**

본 변형된 η_T 페어링 알고리즘은 원래의 Barreto at al.의 알고리즘과 동일한 곱셈량 효율성을 가진다. 이제, 본 변형된 알고리즘에 RPC 방법을 적용한다. 본 알고리즘의 입력값이 타원 곡선 점 $P=(\alpha,\beta)$, $Q=(x,y)$기 때문에, 랜덤 Projective Coordinate로 P점, Q점 그리고, P,Q점 동시에 바꿀 수 있다. 그러나, Kim et al.[22]은 Q점을 바꾸는 것이 가장 효율적임을 증명하였기 때문에, 우리는 Q점을 다음과 같이 랜덤 Projective Coordinate로 변형하여 부채널 공격 방지 η_T 페어링 알고리즘을 구성 한다.

$$(x,y) => (\bar{x},\bar{y},\bar{z}) = (\bar{z}x, \bar{z}y, \bar{z}),\ \bar{z} \in F_q^*.$$

따라서, 본 변형 η_T 페어링 알고리즘에 $x \leftarrow \bar{x}/\bar{z}$, $y \leftarrow \bar{y}/\bar{z}$를 적용하면 다음과 같은 부채널 공격 방지 η_T 페어링 알고리즘을 얻을 수 있다.

다음 장에서는 제안된 부채널 공격 방지 η_T 페어링 알고리즘의 효율성을 분석하여 기존의 가장 효율적인 알고리즘인 Kim et al.[22]의 제안 방법보다 곱셈량 효율성이 더 향상되었음을 분석한다.

Input: $P=(\alpha,\beta)$ and $Q=(x,y)$.
Output: $\eta_T(P,\psi(Q))$.
1: Choose $\bar{z} \in \mathbb{F}_q^*$ at random
2: $\bar{x} \leftarrow \bar{z}x$, $\bar{y} \leftarrow \bar{z}y$
3: $w \leftarrow \alpha + \frac{(m-1)}{2}$
4: $f \leftarrow w \cdot (\bar{x} + \bar{z} \cdot (\alpha+1)) + \bar{y} + \bar{z} \cdot (\beta + b + \epsilon_{(m+1)/2}) + (\bar{z} \cdot w + \bar{x})s + \bar{z}t$
5: **for** $i = 0$ to $(m-1)/2$ **do**
6: $w \leftarrow \alpha + \frac{(m+1)}{2}$
7: $g \leftarrow w \cdot \bar{x} + \bar{y} + \bar{z} \cdot (\frac{(m+1)}{2}w + \beta + b + \epsilon_{(m-1)/2}) + (\bar{z} \cdot w + \bar{x})s + \bar{z}t$
8: $f \leftarrow f \cdot g$
9: **if** $i < (m-1)/2$ **then**
10: $\alpha \leftarrow \sqrt{\alpha}$, $\beta \leftarrow \sqrt{\beta}$, $\bar{x} \leftarrow \bar{x}^2$, $\bar{y} \leftarrow \bar{y}^2$, $\bar{z} \leftarrow \bar{z}^2$
11: **end if**
12: **end for**
13: **return** $f^W = f^{(2^{2m}-1)(2^m+1-\epsilon 2^{(m+1)/2})}$

<제안된 부채널 공격 방지 η_T 페어링 알고리즘>

4. 제안된 알고리즘의 효율성 분석

Barreto et al.의 알고리즘과 우리의 변형 알고리즘은 F_q 상의 곱셈량의 변화는 전혀 없기 때문에, 부채널 공격 방지 기법을 적용했을 때, 새로이 추가되는 곱셈량을 계산함으로써, Kim et al.[22] 기법과의 곱셈 효율성을 비교할 수 있다. 제안된 알고리즘의 총 필드 곱셈량은 다음과 같다.

1. 알고리즘 2번 항목 : 2번의 필드 곱셈
2. 알고리즘 4번 항목 : 3번의 필드 곱셈
3. 알고리즘 7번 항목 : 3번의 필드 곱셈
4. 알고리즘 8번 항목 : 9번의 필듭 곱셈(자세한 계산은 [22]의 Appendix 1 참조)

따라서, 총 곱셈량은 $12 \cdot \frac{(m+1)}{2}M + 5M$ 이기 때문에, $6(m+1)M + 5M$ 이다. 여기서, M은 F_q상의 한 번의 곱셈에 필요한 연산량을 의미한다. 그런데, Barretor et al. 알고리즘과 우리의 변형 η_T 알고리즘의 곱셈 연산량은 동일하게 $3.5(m+1)M + 1M$ [22]이기 때문에, 제안된 부채널 공격 방지 η_T 알고리즘의 추가되는 곱셈 연산량은 $2.5(m+1)M + 4M$이 된다.

결론적으로, 본 제안된 알고리즘은 $m = 239$의 경우, Kim et al.의 기법에 비해 17%의 추가 곱셈 연산량 감소 효과가 있다. 다음 표는 기존의 부채널 공격 방지 이진 필드상의 η_T 페어링 알고리즘의 추가되는 곱셈 연산량 비교 표이다(본 비교표의 상위 4개에 대한 자세한 설명은 [22]를 참조).

부채널 공격 방지 기법	추가되는 곱셈량
Page-Vercauteren (randomized private value) [20]	$12mM$
Page-Vercauteren (blinding public value) [20]	$3.5(m+1)M+\alpha$
Scott (randomizing intermediate value) [23]	$4(m+1)M+5M$
Kim et al. (RPC on Barreto et al. algorithm) [22]	$3(m+1)M+4M$
Our proposed Algorithm	$2.5(m+1)M+4M$

상기 표에 의하면 현재까지 제안된 방법들 중, 본 제안 기법이 가

장 곱셈 효율성이 높음을 알 수 있다.

5. 결 론

본 논문에서는 이진 필드상의 η_T 페어링에 대해 살펴보고, Barreto at al.의 페어링 알고리즘을 변형하였다. 본 변형 알고리즘은 기본적으로 Barreto at al. 알고리즘과 유사한 곱셈량 효율성을 가지지만, 본 알고리즘에 부채널 공격 방지를 위해 RPC 방법을 적용할 경우에는 기존의 Barreto at al.의 알고리즘에 RPC 방법을 적용하는 것에 비해 17% 정도 곱셈 효율성이 향상됨을 알 수 있었다. 이는, 기존의 알고리즘의 작은 변형이 부채널 공격 방지 알고리즘에서는 의미 있는 차이를 야기할 수도 있음을 시사한다.

[참고문헌]

[1] D. Boneh and M. Franklin, *Identity Based Encryption from the Weil Pairing*, SIAM J. of Computing, Vol.32, No.3, pp.586-615, 2003.

[2] R. Sakai and M. Kasahara, *ID based cryptosystems with pairing on elliptic curve*, Cryptography ePrint Archive, Report 2003/054, 2003. http://eprint.iacr.org/2003/054.

[3] J.C. Cha and J.H. Cheon, *An Indentity-Based Signature from Gap Diffie-Hellman Groups*, PKC 2003, LNCS 2567, pp.18-30, 2003.

[4] F. Hess, *Exponent group signature schemes and efficient identity based signature schems based on pairing*, SAC 2002, LNCS 2595, pp.310-324, 2002.

[5] K.G. Paterson, *ID-based signature from pairings on elliptic curves*, Electronics Letters, Vol.38, No.18, pp.1025-1026, 2002.

[6] A. Joux, A *One Round Protocol for Tripartite Diffie-Hellman*, Journal of Cryptology, Vol.17, No.4, pp.263-276, 2004.

[7] D. Boneh, B. Lynn, and H. Shacham, *Short Signatures from the Weil Pairing*, Journal of Cryptology, Vol.17, No.4, pp.297-319, 2004.

[8] N.P. Smart, *An identity based authentication key agreement protocol based on pairing*, Electronics Letters, Vol.38, No.13, pp.630-632, 2002.

[9] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairing-based cryptosystems*, CRYPTO 2002, LNCS 2442, pp.354-368, 2002.

[10] S.D. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate pairing*, ANTS V, LNCS 2369, pp.324-337, 2002.

[11] V. Miller, *Short Programs for Functions on Curves*, unpublished manuscript, 1986.

[12] I. Duursma and H.S. Lee, *Tate pairing implementation for hyperelliptic curves* $y^2 = x^p - x + d$, Asiacrypt 2003, LNCS 2894, pp.111-123, 2003.

[13] S. Kwon, *Efficient Tate Pairing Computation for Elliptic Curves over Binary Fields*, ACISP 2005, LNCS 3574, pp.134-145, 2005.

[14] P.S.L.M. Barreto, S. Galbraith, C. O'hEigeartaigh and M. Scott, *Efficient Pairing Computation on Supersingular Abelian Varieties*, Preprint 2005, to appear in Designs, Codes and Cryptography.

[15] F. Hess, N. Smart, and F. Vercauteren, *The eta pairing revisited*, IEEE Trans. Inf. Theory. 52 no. 10 pp.4595-4602, 2006.

[16] R. Granger, D. Page, and M. Stam, *Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three*, IEEE Transactions on Computers, Vol.54, No.7, pp.852-860, July 2005.

[17] M. Shirase, T. Takagi, and E. Okamoto, *Some Efficient Algorithms for the Final Exponentiation of* η_T *Pairing*, Cryptography ePrint Archive, Report 2006/431, 2006. http://eprint.iacr.org/2006/431.

[18] P. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, CRYPTO 1996, LNCS 1109, pp.104-113, 1996.

[19] C. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*, CRYPTO 1999, LNCS 1666, pp.388-397, 1999.

[20] D. Page and F. Vercauteren, *Fault and Side-Channel Attacks on Pairing Based Cryptography*, Cryptology ePrint Archive, Report 2004/283, 2005. http://eprint.iacr.org/2004/283.

[21] C. Whelan and M. Scott, *Side Channel Analysis of Practical Pairing Implementations: Which Path is More Secure?*, Cryptography ePrint Archive, Report 2006/237, 2006. htt://eprint.iacr.org/2006/237.

[22] T. H. Kim, T. Takagi, D.-G. Han, H. W. Kim and J. Lim, *Side Channel Attacks and Countermeasures on Pairing Based Cyrptosystems over Binary Fields*, *CANS 2006*, LNCS 4301, pp.168-181, 2006.

[23] M. Scott, *Computing the Tate Pairing*, CT-RSA 2005, LNCS 3376, pp.293-304, 2005.

[24] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.