NFC 모바일 결제 시스템에서 Bilinear Pairing을 이용한 효율적인 인증 메커니즘

진흔이, 최경, 채기준
이화여자대학교 컴퓨터공학과
e-mail : chloexiny@ewhain.net, cbk0907@ewha.ac.kr, kjchae@ewha.ac.kr

An Efficient Authentication Scheme using Bilinear Pairing in NFC-enabled Mobile Payment System

Xinyi Chen, Kyong Choi, Kijoon Chae
Department of Computer Science, Ewha Womans University

요 약

NFC(Near Field Communication)는 10cm 이내의 거리에서 무선기기 간의 통신을 가능케 해주는 기술로 13.56 Mhz RF(Radio Frequency) 주파수 대역을 이용한 비접촉식 근거리 무선통신의 한 종류이다. 올해 출시되는 대부분의 스마트 폰에서 NFC 기능을 탑재하며, NFC기반의 모바일 결제 서비스가 가장 유망한 결제 방식으로 주목 받고 있다. 소비자는 NFC 모바일 단말기를 가지고 판매자의 POS(Point of Sale) 단말기와 근접 통신을 통해 결제를 진행하는 방식으로 다른 무선 통신 방식 (RFID, Bluetooth 등)보다 보안 취약성이 높지 않지만, 기존의 RFID 환경에서 일어날 수 있는 기술적 취약점과 비슷한 유형의 위협이 충분히 발생할 수 있으므로 유효한 보안 기술이 필요하다. 본 논문은 안전한 NFC 모바일 결제 환경을 구축하기 위한 공개키 알고리즘인 타원곡선 암호 ECC(Elliptic Curve Cryptosystem)를 적용한 Bilinear Pairing을 활용해서 효율적이고 보안성도 강력한 인증 메커니즘을 제안한다.

1. 서론

NFC(Near Field Communication)는 13.56MHz의 주파수 대역을 사용하는 비접촉식 근거리 무선통신 규격으로 10cm 이내 거리에서 낮은 전력으로 무선통신을 할 수 있는 기술이다[1]. NFC 통신 방식은 능동통신과 수동통신 두 가지로 구분되며 스마트카드와 달리 양방향 통신이 가능하다. 통신 장치가 ISO(International Standards Organization) 1444규격에 따라 Card emulation, Reade/Write, P2P(Peer-to-Peer), 3가지 모드로 동작한다. 이런 동작 모드를 기반해서 모바일 결제, 스마트 포스터, 개인 간 데이터 전송 등의 다양한 애플리케이션 개발이 가능하다. 또한 실생활과 연계된 복잡한 정보활동에 대한 해결책으로 모든 타입의 사용자 기기에 대해서 “touch-and-start” 형식으로 직관적 연결이 가능하다[2]. 가장 큰 규모의 시장으로 주목 받고 있는 NFC기반의 모바일 결제시장인 경우 구글, 애플 등 기존의 플랫폼 사업자와 이동통신 사업자들을 중심으로 모바일 결제시장을 선점하기 위한 노력들이 활발히 전개되고 있다[3]. NFC 모바일 단말기를 이용하면 소비자와 판매자 사이에 금융 결제를 편하게 진행할 수 있다. 이때에 이동통신사와 신용카드에서 NFC 단말상에 존재하는 소비자 결제 정보를 이동 통신망을 통해 송수신하고, 송수신되는 정보가 사용자 결제정보이기에 데이터 송수신이 공격자에게 노출되는 것을 방지하기 위한 강력한 보안기술 적용이 필요하다.

본 논문은 NFC 기술의 특징을 기반으로 하여 안전하고 편리한 모바일 금융결제 서비스를 제공하기 위해 타원곡선 암호 방식 ECC(Elliptic Curve Cryptosystem)를 이용해서 Bilinear Pairing키를 생성하고 빠른 시간에 소비자와 판매자가 동시에 인증할 수 있는 새로운 메커니즘을 제안한다.

2. NFC보안 관련 연구

무선 통신 방식(RFID, Bluetooth 등)에 비해 NFC 통신은 장치 간 통신 거리가 짧아서 보안 취약성이 높지 않다. 하지만 기존의 RFID 환경에서 일어날 수 있는 도청(Eavesdropping), 데이터 변조(Corruption) 수정(Modification) 삽입(Insertion), 중간자 공격(Man-in-the-Middle-Attack) 등 위협이 NFC 환경에서 충분히 발생할 수 있으므로 유효한 보안 기술이 필요하다. 2009년에 G. V. Damme과 K. Wouters[4]는 NFC 모바일 폰으로 실험하면서 통합 암/복호화 방식을 사용해서 Offline NFC 모바일 결제 시스템을 제안했다. 2011년에 H. C. Cheng과 W. W. Liao[5]는 NFC Read/Write 모드에 대한 RSA 공개키 기반 키 관리 및 인증 메커니즘을 제안했으며 S. Tamrakar, J. E. Ekberg와 N. Asokan[6]는 NFC 모바일 결제 아키텍처에 공인인증서를 적용하여 사용자 신분 인증을 제공하는 프로토콜을 제안했다. 하지만 이에 대한 선행 연구들은 공개키 기반으로 NFC 모바일 결제를 빠른 시간에 인증하기 어렵고 모바일

이 논문은 2012 년도 이화여자대학교 Ewha Global Top 5 Project 연구비 지원에 의한 연구임.

결제 이용자만 인증하고 판매자 인증없이 거래를 진행한 단점이 있다. 또한, E. Husni와 Kuspriyanto[7]는 제안한 Tag-to-Tag NFC 프로토콜에 결제 상대방에 대한 상호 인증을 제공하지만 대칭키와 사용자 비밀번호를 동시에 이용하므로 NFC와 같은 활성화 높은 환경에 판매자마다 사용자의 키를 저장하는 시스템적 적용이 어려운 문제점이 존재한다. 현재 NFC 보안 기술은 NFC Forum을 중심으로 ECMA(Electronic Computer Manufacturers Association) 표준을 기반으로 한 개인 간 금융 거래 및 데이터 공유에 관한 활용이 연구되고 있다. 이와 관련하여 NFC 단말기에서 공개키와 개인키를 기반으로 타원곡선에서 암호 알고리즘을 적용한 보안 프로토콜을 지원한다[8]. 그러나 Bilinear Pairing을 이용해서 ECC 암호방식을 사용하는 일반적인 경우, 센서 네트워크[9], 모바일 네트워크[10], RSA기반한 인증[11] 분야에 적용한 연구들이 있지만 NFC 모바일 결제 시스템에 적용한 연구는 아직 없다. Bilinear Pairing은 Pair-wise키를 생성하고 키 pairing을 이용해서 빠르고 편리하게 인증하는 알고리즘으로써 Additive그룹 G_1과 Multiplicative그룹 G_2를 가지고 Mapping을 한다: $\hat{e} = G_1 \times G_1 \rightarrow G_2$. 그룹 G_1은 그 표기가 $G_1 = \langle P \rangle$이고 다음 세 가지 성질을 만족하는 방식이다. 여기서 q는 G_1의 order이고 P는 G_1의 generator이다.

1) Bilinearity:
   - $\hat{e}(aP_1, P_2) = \hat{e}(P_1, P_2)^a = \hat{e}(P_1, aP_2)$
   - $\hat{e}(aP_1, bP_2) = \hat{e}(P_1, P_2)^{ab}$
   - $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q)\,\hat{e}(P_2, Q)$
2) Non-degeneracy: $\hat{e}(P, Q)=1$ 이면 P는 무한원점 (O)이다.
3) Efficiency: $\hat{e}(P, Q)$의 계산이 효율적인 알고리즘이다.

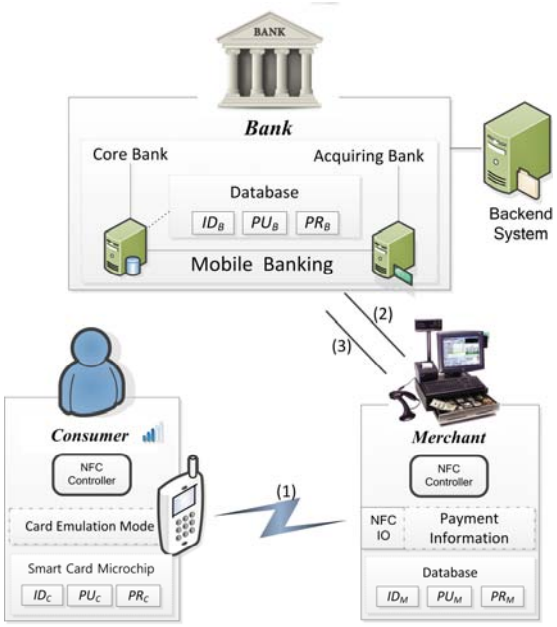
이론적인 Bilinear Pairing의 성질을 만족하는 알고리즘을 실현 가능하게 한 것은 ECC의 Tate Pairing과 Weil Pairing이었고 인증은 타원곡선 위의 점 G, 공개키(PU_K) = 개인키(PR_K) · G가 주어지면 인증을 실시할 A, B상호간에 $\hat{e}(PR_{KA}, PU_{KB}) = \hat{e}(PU_{KA}, PR_{KB})$가 성립하는지를 인증함으로써 쉽게 진행할 수 있다. 제안한 메커니즘은 Bilinear Pairing의 특성을 이용하며 이 관점에서 출발하여 pairing키를 생성하고 빠른 시간에 인증을 실시하면서 보안성과 효율성을 동시에 제공한다.

3. 제안한 NFC에 기반한 모바일 결제 메커니즘

본 논문에서는 NFC기반 모바일 결제 시스템은 소비자(Consumer), 판매자(Merchant), 은행(Bank) 세 엔티티로 구성된 시스템 구조를 가지며, Bilinear Pairing을 NFC 환경에 적합하게 적용한 모바일 결제 인증 메커니즘을 제안한다.

3.1 시스템 구조

NFC기반 모바일 결제 시스템의 구성은 (그림 1)과 같다. 이 시스템 환경에서, 제안한 NFC 모바일 결제 인증 메커니즘은 거래를 진행하는 상대방 - 소비자와 판매자 둘 다 서로를 신뢰하지 않고 상호 인증은 제 3자 은행에게 인증 정보를 보내주고 은행에서 소비자와 판매자를 인증해 준다. 인증을 성공한 후 은행이 소비자와 판매자에게 인증과 거래에 대한 성공결과 메시지를 전달하는 과정으로 마친다.



(그림 1) NFC기반 모바일 결제 시스템 구조

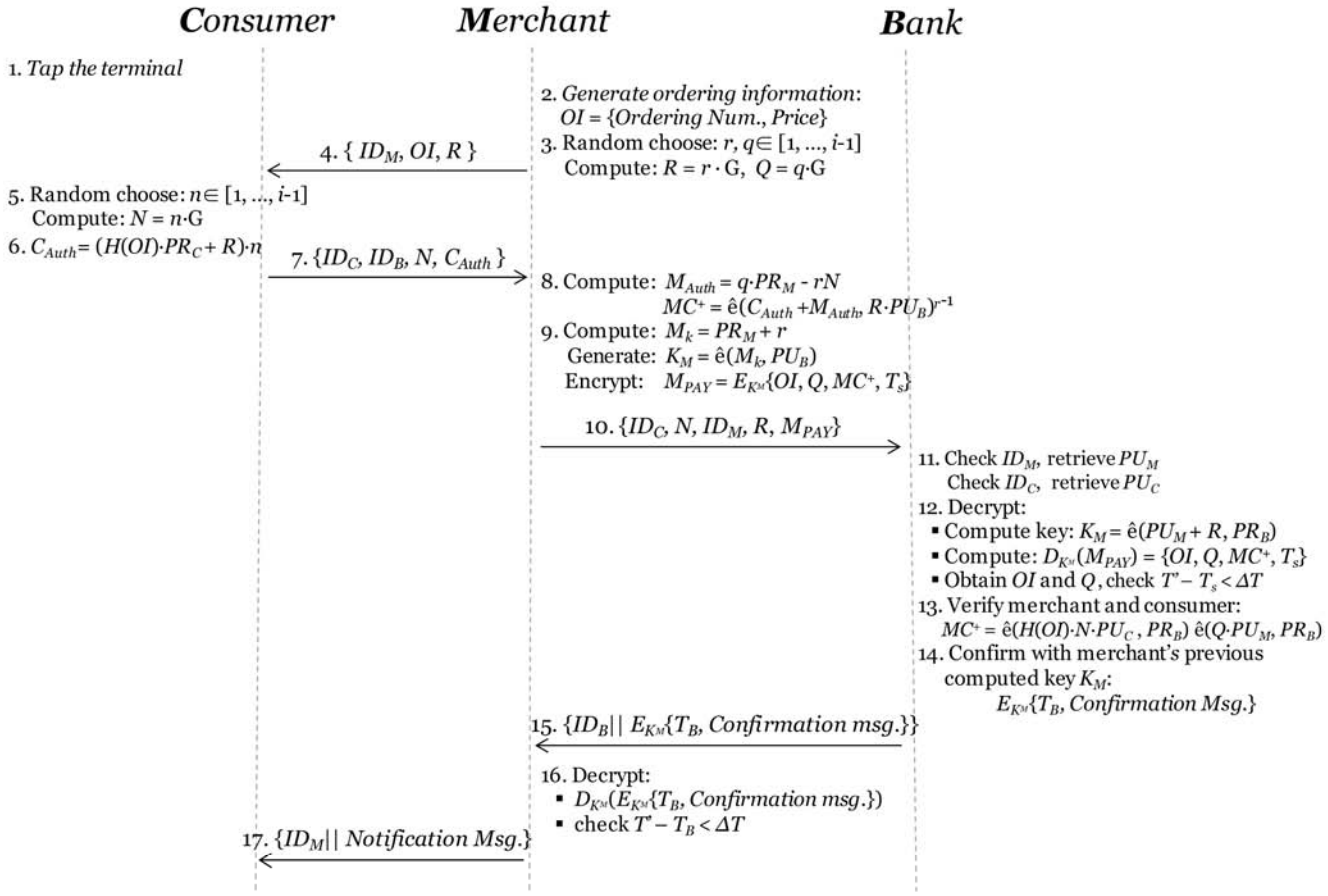
여기서 제안한 메커니즘에 사용된 표기법은 <표 1>과 같다.

<표 1> 사용된 표기법

표기	설명
ID_C	*Consumer* (소비자 *C*)의 아이디
ID_M	*Merchant* (판매자 *M*)의 아이디
ID_B	*Bank* (은행 *B*)의 아이디
PU_C, PR_C	소비자의 공개키와 개인키
PU_M, PR_M	판매자의 공개키와 개인키
PU_B, PR_B	은행의 공개키와 개인키
OI	*Ordering Information*(주문내역), 주문번호와 제품 가격 등 포함
G	타원곡선에 랜덤으로 선택한 점
C_{Auth}	소비자에 대한 인증 정보
M_{Auth}	판매자에 대한 인증 정보
MC^+	소비자와 판매자의 인증 정보
K_M	판매자가 만든 암호키
M_{PAY}	키 K_M을 이용해서 결제정보와 인증 정보 등을 암호한 결과
E_{KM}, D_{KM}	키 K_M을 이용한 암/복호 함수
$H()$	단방향 해쉬 함수

NFC 모바일 단말기를 이용해서 결제를 진행하기 전에 사전 요구사항은 아래와 같다.

- 각 소비자의 NFC 폰은 ECC 공개키(PU_C)와 개인키(PR_C)를 가진다: $PU_C = PR_C \cdot G$.
- 각 판매자는 ECC 공개키(PU_M)와 개인키(PR_M)를 가진다: $PU_M = PR_M \cdot G$.
- 은행은 ECC 공개키(PU_B)와 개인키(PR_B)를 가진다: $PU_B = PR_B \cdot G$.
- 각 소비자와 각 판매자는 은행의 아이디(ID_B)와 공개키(PU_B)를 알고 있다.
- 은행은 각 소비자의 NFC 폰 아이디(ID_C)와 공개키(PU_C), 각 판매자의 아이디(ID_M)와 공개키(PU_M)를 알고 있다.



(그림 2) 제안한 모바일 결제 인증 메커니즘

3.2 제안한 모바일 결제 인증 메커니즘

모바일 결제를 인증하기 위해 제안한 프로토콜은 (그림 2)와 같이 소비자와 판매자 사이의 비접촉 통신과, 은행을 통해 소비자와 판매자를 인증하는 두 과정으로 구성한다. 소비자가 결제하기 위해 판매자에게 자신의 인증 정보를 넘겨주고, 판매자가 자신의 인증 정보를 추가하고 소비자에게 받은 인증 정보와 같이 은행에게 전송하고 나서 은행 측에서 두 정보에 대한 인증을 진행한다. 구체적인 과정은 다음과 같다.

Step 1 Consumer: NFC 폰을 이용해서 판매자의 POS(Point of Sale) 단말기를 통해 주문한다.

Step 2 Merchant: 소비자가 주문한 제품에 대한 판매 정보 *OI*를 생성. **OI* = {주문 번호(*Ordering Number*), 상품 가격(*Price*)}

Step 3 Merchant: [1, …, *i*-1]에서 정수 값 *r*, *q*를 랜덤으로 선택한 후, 공개 파라미터 G를 이용해서 $R = r \cdot G$, $Q = q \cdot G$를 계산한다.

Step 4 Merchant → Consumer: 소비자에게 생성한 판매정보 *OI*와 자신의 아이디 ID_M과 난수 값 *R*을 보낸다.

Step 5 Consumer: [1, …, *i*-1]에서 정수 값 *n*를 랜덤으로 선택한 후, 공개 파라미터 G를 이용해서 $N = n \cdot G$를 계산한다.

Step 6 Consumer: 안전한 결제를 위한 자신의 신분을 표시할 수 있는 인증 정보 C_{Auth}를 계산 하고,

$$C_{Auth} = (H(OI) \cdot PR_C + R) \cdot n$$

부인방지를 위해 소비자는 판매자에게 받은 판매정보 *OI*에 대한 자신의 개인키 PR_C를 이용해 사인($H(OI) \cdot PR_C$)을 한다.

Step 7 Consumer → Merchant: 판매자에게 자신의 아이디ID_C, 지불할 은행 아이디ID_B, 난수값*R*, 그리고 인증 정보 C_{Auth}를 보낸다.

Step 8 Merchant: 받은 정보에 대해 다음과 같은 계산을 한다.

$$M_{Auth} = q \cdot PR_M - rN$$
$$MC^+ = \hat{e}(C_{Auth} + M_{Auth}, R \cdot PU_B)^{r-1}$$

M_{Auth}는 판매자 자신의 인증 정보이고, MC^+는 나중에 편리하게 인증하기 위해 받은 소비자의 인증 정보 C_{Auth}를 추가한 후 pairing한 결과이다.

Step 9 Merchant: 암호키 K_M을 만들기 위해 판매자 자신의 개인키 PR_C를 사용 M_k라는 값을 먼저 계산한 후 K_M을 이용해서 메시지를 암호화(M_{PAY})한다. 계산은 다음과 같다.

$$M_k = PR_M + r$$
$$K_M = \hat{e}(M_k, PU_B) \quad \text{;암호키 생성}$$
$$M_{PAY} = E_{K_M}\{OI, Q, MC^+, T_s\} \text{; 메시지 암호}$$

Step 10 Merchant → Consumer: 판매자는 은행에게 소비자의 신분정보를 넘겨주면서 자신의 아이디를 붙여서 둘 다 인증할 수 있는 정보와 함께 암호 메시지를 보낸다.

$\{ID_C, N, ID_M, R, MC^+, M_{PAY}\}$

Step 11 Bank: 판매자에서 정보를 받은 후에 먼저 소비자와 판매자의 아이디(ID_C, ID_M)를 체크한다. DB에서 두 아이디와 관련된 공개키(PU_C, PU_M)를 얻는다.

Step 12 Bank: 은행은 DB에서 얻은 판매자의 공개키(PU_M)와 자신의 개인키(PR_B)를 이용해서 복호키 K_M을 계산한다.

$K_M = \hat{e}(PU_M + R, PR_B)$

복호키 K_M을 적용해서 암호 메시지를 복호화시킨다. 복호화한 메시지에서 평문($\{OI, Q, MC^+, T_s\}$)를 얻고 타임스탬프를 검증한다.

$D_{K_M}(M_{PI}) = \{OI, Q, MC^+, T_s\}$

체크: $T' - T_s < \Delta T$

Step 13 Bank: 평문($\{OI, Q, MC^+, T_s\}$)중에 $\{OI, Q\}$를 이용해서 소비자와 판매자에 대한 인증을 수행한다; $MC^+ = \hat{e}(H(OI)\cdot N\cdot PU_C, PR_B)\,\hat{e}(Q\cdot PU_M, PR_B)$. MC^+는 pairing한 결과와 일치하는지 검사함과 동시에 판매자에서 복호화한 결제 정보 OI를 해쉬해서 소비자에게 받은 $H(OI)$와 일치여부를 검사한다. Pairing증명은 다음과 같다.

$$
\begin{aligned}
MC^+ &= \hat{e}(C_{Auth} + M_{Auth}, R\cdot PU_B)^{r^{-1}} \\
&= \hat{e}((H(OI)\cdot PR_C + R)\cdot n + M_{Auth}, R\cdot PU_B)^{r^{-1}} \\
&= \hat{e}((H(OI)\cdot PR_C + R)\cdot n + q\cdot PR_M - rN, R\cdot PU_B)^{r^{-1}} \\
&= \hat{e}(H(OI)\cdot PR_C\cdot n + R\cdot n + q\cdot PR_M - rN, R\cdot PU_B)^{r^{-1}} \\
&= \hat{e}(H(OI)\cdot PR_C\cdot n + r\cdot G\cdot n + q\cdot PR_M - r\cdot nG, R\cdot PU_B)^{r^{-1}} \\
&= \hat{e}(H(OI)\cdot PR_C\cdot n + q\cdot PR_M, R\cdot PU_B)^{r^{-1}} \\
&= \hat{e}(H(OI)\cdot PR_C\cdot n\cdot r^{-1} + q\cdot PR_M\cdot r^{-1}, R\cdot PU_B) \\
&= \hat{e}(H(OI)\cdot PR_C\cdot n\cdot r^{-1}\cdot R + q\cdot PR_M\cdot r^{-1}\cdot R, PU_B) \\
&= \hat{e}(H(OI)\cdot PR_C\cdot n\cdot r^{-1}\cdot rG + q\cdot PR_M\cdot r^{-1}\cdot rG, PU_B) \\
&= \hat{e}(H(OI)\cdot PR_C\cdot n\cdot G + q\cdot PR_M\cdot G, PU_B) \\
&= \hat{e}(H(OI)\cdot PR_C\cdot N + PR_M\cdot Q, PU_B) \\
&= \hat{e}(H(OI)\cdot PR_C\cdot N + PR_M\cdot Q, PR_B\cdot G) \\
&= \hat{e}(H(OI)\cdot PR_C\cdot G\cdot N + PR_M\cdot Q\cdot G, PR_B) \\
&= \hat{e}(H(OI)\cdot PU_C\cdot N + Q\cdot PU_M, PR_B) \\
&= \hat{e}(H(OI)\cdot N\cdot PU_C, PR_B)\,\hat{e}(Q\cdot PU_M, PR_B)
\end{aligned}
$$

이에 따라,

$MC^+ = \hat{e}(H(OI)\cdot N\cdot PU_C, PR_B)\,\hat{e}(Q\cdot PU_M, PR_B)$.

Step 14 Bank: 인증을 성공하면 판매자에게 소비자 인증에 대한 성공 결과를 전송한다. 이전에 복호화했을 때 사용했던 키 K_M을 다시 이용해서 인증 성공결과 메시지(*Confirmation Msg.*)와 결제완료 시간 T_B를 함께 암호화시킨다.

$E_{K_M}\{T_B, Confirmation\ Msg.\}$

Step 15 Bank → Merchant: 자신의 아이디 ID_B 와 함께 판매자에게 보낸다.

$\{ID_B \,\|\, E_{K_M}\{T_B, Confirmation\ Msg.\}\}$

Step 16 Merchant: 은행에서 메시지를 받은 후에 이전에 만든 키 K_M을 바로 적용해서 복호화한 후 평문$\{Confirmation\ Msg., T_B\}$를 얻고 타임스탬프 T_B를 검증한다.

$D_{K_M}(E_{K_M}\{Confirmation\ Msg., T_B\})$

체크: $T' - T_B < \Delta T$

Step 17 Merchant → Consumer: 결제완료 메시지 $\{ID_M \,\|\, Notification\ Msg.\}$를 전달한다.

결과적으로 NFC 폰을 이용하는 소비자와 판매자 사이에 결제가 안전하게 이루어지면서 인증도 효율적으로 진행된다.

4. 결론 및 향후 연구

본 논문에서 공개키 알고리즘 타원곡선 암호를 사용하면서 Bilinear Pairing을 적용해서 빠른 시간에 인증과 NFC 모바일 결제를 동시에 달성함과 함께 효율성과 안전성을 고려한 NFC 모바일 결제 메커니즘을 제안하였다. 빠른 시간에 소비자와 판매자가 동시에 인증하는 장점을 가지며, 선행 연구에서 일반 공개키 기반 NFC 모바일 결제를 빠른 시간에 인증하기 어려운점과 모바일 결제시 판매자 인증없이 거래를 진행한 단점을 극복하였다. 향후 최신 NFC 기기를 이용해서 제안한 메커니즘을 적용하며 테스트를 통해 성능을 검증할 것이다.

참고문헌

[1] PopSci., "Everything You Need to Know About Near Field Communication", March 2011.

[2] G. Madlmayr and J. Langer, "Managing an NFC Ecosystem", ICMB '08 7th International Conference on Mobile Business, pp. 95-101, July 2008.

[3] 공영일, "NFC 기반 모바일 결제시장의 이해관계 분석과 시사점", 정보통신정책연구원, 제 23 권 6 호, pp. 55-63, April 2011.

[4] G. V. Damme and K. Wouters, "Practical Experiences with NFC Security on mobile Phones", Workshop on RFID Security, April 2009.

[5] H. C. Cheng, W. W. Liao, T. Y. Chi and S. Y. Wei, "A Secure and Practical Key Management Mechanism for NFC Reade/Write Mode", International Conference on Advanced Communication Technology, pp. 1095-1100, February 2011.

[6] S. Tamrakar, J. E. Ekberg and N. Asokan, "Identity Verification Schemes for Public Transport Ticketing with NFC Phones", Proceedings of the STC '11 6th ACM Workshop on Scalable Trusted Computing, pp. 37-48, October 2011.

[7] E. Husni, Kuspriyanto, N. Basjaruddin, T. Purboyo, S. Purwantoro and H. Ubaya, "Efficient Tag-to-Tag Near Field Communication (NFC) Protocol for Secure Mobile Payment", 2nd International Conference on ICICI-BME, pp. 97-101, November 2011.

[8] 임선희, 전재우, 정임진, 이옥연, "NFC 보안기술 분석 및 UICC 적용 효과 연구", 한국통신학회 논문지, 제 36 권 1 호, pp. 29-36, January 2011.

[9] Y. S. Liu, J. Li and M. Guizani, "PKC Based Broadcast Authentication using Signature Amortization for WSNs", IEEE Transactions on Wireless Communications, vol. 11, no. 6, pp. 2106-2115, June 2012.

[10] P. Lin, H. Y. Chen, Y. Fang, J. Y. Jeng and F. S. Lu, "A Secure Mobile Electronic Payment Architecture Platform for Wireless Mobile Networks", IEEE Transactions on Wireless Communications, vol. 7, no. 7, pp. 2705-2713, July 2008.

[11] C. I. Fan, W. Z. Sun, V. S. M. Huang, "Provably secure randomized blind signature scheme based on bilinear pairing", Journal of Computers and Mathematics with Applications, pp 285-293, July 2010.