ECC 프로세서에 대한 부채널 공격 및 대응방안 동향

정영수* · 신경욱

[1]금오공과대학교

A Survey on Side-Channel Attacks and Countermeasures for ECC Processor

Young-su Jeong* · Kyung-Wook Shin

[1]Kumoh National Institute of Technology

E-mail : 20226086@kumoh.ac.kr / kwshin@kumoh.ac.kr

요 약

타원곡선 암호 (elliptic curve cryptography; ECC)는 효율적인 하드웨어 구현이 가능하면서 높은 보안 강도를 가져 오늘날 IoT 기기나 V2X 통신의 공개키 보안 하드웨어 구현에 폭넓게 사용되고 있다. 그러나 ECC 기반의 공개키 보안 시스템은 부채널 공격 (side channel attacks; SCA)에 대한 일부 보안 취약점을 갖는 것으로 알려지고 있어 ECC 프로세서 설계 시 보안공격에 대한 대응 방법의 적용이 필요하다. 본 논문에서는 부채널 공격 유형과 ECC 프로세서 설계에 적용할 수 있는 부채널 공격 대응 방안에 대해 알아본다.

ABSTRACT

Elliptic curve cryptography (ECC) is widely used in hardware implementations of public-key crypto-systems for IoT devices and V2X communication because it is suitable for efficient hardware implementation and has high security strength. However, ECC-based public-key cryptography is known to have security vulnerabilities against side-channel attacks, so it is necessary to apply countermeasures against security attacks in designing ECC processor. This paper describes a survey on the side-channel attacks and countermeasures applicable to ECC processor design.

키워드

Elliptic curves cryptography, side channel attack, simple power analysis, countermeasures

Ⅰ. 서 론

정보 통신 기술이 발전하면서 다양한 기기들이 네트워크로 연결되어 정보를 주고받고 있다. 통신 시 주고받는 데이터들은 개인 정보와 같은 민감한 정보를 담고 있어 보안의 필요성과 중요성이 증가하고 있다. 다양한 보안 암호 알고리듬들 중 타원곡선 암호 (ECC)는 적은 자원을 소모하면서 높은 보안 강도를 가져 IoT (Internet of things)와 같은 임베디드 시스템이나 V2X 통신 등 다양한 분야의 보안 시스템에 사용되고 있다. 그러나 이러한 ECC는 알고리듬 자체가 수학적으로는 안전한 것으로 입증되었지만 부채널 공격에 취약점이 있다고 알려져 있다 [1]. 특히 표준으로 구현된 ECC는 단순 전력 분석 (simple power analysis; SPA)과 차분 전력 분석 (differential power analysis; DPA) 모두에 취약한 것으로 알려져 있다 [2]. 이러한 부채널 공격에 대한 내성을 갖도록 Montgomery ladder 점 스칼라 곱셈 알고리듬을 적용한 ECC 프로세서 구현 등이 발표되고 있다 [3].

본 논문에서는 부채널 공격이 공개키 암호 시스템에 미치는 위협을 알아보고, 이에 대한 대응 방안을 사례 중심으로 조사했다. 2장에서 부채널 공격의 종류와 ECC 기반 공개키 암호에 미치는 위협을 설명하고, 3장에서는 부채널 공격 대응방안에 대한 사례들을 알아보고 4장에서 결론을 맺는다.

Ⅱ. ECC에 대한 부채널 공격 유형

부채널 공격은 공격자가 타이밍 정보나 소비 전력, 전자기파와 같은 누출된 물리적 정보를 이용해 공격하는 보안공격의 한 형태이다 [4]. 부채널 공격은 암호 알고리듬 동작 과정에서 발생하는 소비전력, 전자기파 등 부가적인 정보를 분석하는 비침입 공격 (non-invasive attacks)과 알고리듬 동작 중 레

* speaker

Table. 1 Side-channel attacks versus Countermeasures on ECC

	TA	SPA	DPA	CPA	RPA/ZPA	DA	Template attack
Double and add always [2]	O	O	-	-	-	-	-
Randomized projective coordinate [2]	-	-	O	-	-	O	O
Montgomery Powering Ladder [4]	O	O	-	-	-	-	-
Randomized Montgomery operation [1]	O	O	O	O	-	-	O
Elevated binary number system [4]	-	O	-	-	-	O	-
Randomized scalar multiplication [2]	-	-	-	-	O	-	-
Base point blinding [2]	-	-	-	-	O	-	-

TA: timing attack, SPA: simple power analysis, DPA: differential power analysis, CPA: correlation power analysis
RPA: refined power analysis, ZPA: zero power analysis, DA: doubling attack

이저나 전자파를 이용해 오류를 인위적으로 주입하여 변경된 출력과 부가적인 정보를 분석하는 준침입 공격 (semi-invasive attacks), 그리고 실제 메모리에 접근하여 정보를 획득하는 침입 공격 (invasive attacks) 등으로 구분된다. 본 논문에서는 부채널 공격 중 비침입 공격을 중점으로 조사했다.

시차 공격 (timing attack; TA)은 암호화 연산이 진행될 때 입력 값에 따라 실행 시간이 일정하지 않아 차이가 발생하면 이를 이용한 타이밍 분석을 통해 비밀키를 찾아내는 방법이다. ECC에 대한 시차 공격에는 고전적 공격 (classical attacks)과 특정 지점 공격 (particular point attacks)이 있다. 고전적 공격은 점 스칼라 곱셈 (point scalar multiplication; PSM)을 여러 번 진행하여 실행 시간을 수집하는 방법이고, 특정 지점 공격은 (2,y)점을 이용하여 감소된 PSM 연산량을 통해 비밀키를 추적한다 [5].

전력 분석 (power analysis)은 암호화가 진행될 때 발생하는 전력소모 패턴을 이용해 비밀키를 알아내는 방법이다. 전력 분석 방법에는 크게 단순 전력분석, 차분전력분석, 상관전력분석 (correlation power analysis; CPA)로 나눌 수 있다. SPA는 적은 수의 전력소모 파형을 분석하는 방법이고, DPA와 CPA는 많은 수의 전력소모 파형에 대해 평균 차와 상관계수로 분석하는 방법이다. ECC에 대한 SPA는 PSM 연산 시 점 덧셈 (point addition; PA) 연산과 점 두 배 (point doubling; PD) 연산의 전력소모 패턴이 서로 다른 경우 이를 이용해 비밀키를 획득할 수 있고, DPA는 타원곡선 위의 좌표 중 하나가 0인 좌표를 이용하는 RPA (refined power analysis)와 ZPA (zero power analysis), 점 P와 점 2P를 이용하여 비밀키를 획득하는 DA (doubling attack) 등 다양한 공격 방법들이 있다 [6].

이 외에도 덧셈 연산 시 발생하는 캐리신호의 전력 소비를 분석하는 carry-based attack (CBA) [7], 전력 소비 템플릿을 구축하여 추적하는 템플릿 공격 (template attack) [8], 내부 연산에서 상관관계를 통해 값을 추정하는 충돌 공격 (collision attack) [9], 머신러닝 기반의 전력소모 분석과 비밀키 복구 [10] 등 다양한 전력분석 방법이 있다.

III. ECC의 부채널 공격 대응방안

일반적으로, ECC는 PSM에서 부채널 공격에 취약하여 비밀키가 노출될 수 있다. PSM을 구성하는 PA 연산과 PD 연산 횟수가 달라 연산시간과 소비전력의 차이를 이용하는 부채널 공격에 취약하다[11]. 문헌에 발표된 ECC 부채널 공격 대응방안들 중 대표적인 5가지 사례를 조사했다.

첫 번째, 불필요한 연산을 추가하여 각 연산 시간을 일정하게 만들어 부채널 공격을 방지한다. 예시로 double and add always 알고리듬을 이용해 비밀키의 해당 비트가 1인지 0인지에 무관하게 PA와 PD를 수행하고 1일 때는 PA 연산결과는 버리면서 연산 시간을 일정하게 한다 [5].

두 번째, 좌표의 시작점이나 특정 비트를 쉽게 예측하지 못하도록 하는 방법이 있다. 예시로 Coron's randomized projective coordinate를 이용하여 투영 좌표로 변환할 때 $(X:Y:Z)$가 아닌 $(\lambda X:\lambda Y:\lambda Z)\,(\lambda \neq 0)$로 변환시켜 좌표를 무작위화하는 방법이 있다 [2].

세 번째, 비밀키에 의존하지 않고 PSM을 연산하는 방법이 있다. 예시로 Montgomery ladder를 이용해 PSM을 구현하면 비밀키와 상관없이 항상 PA 연산 후 PD 연산을 수행하므로 비밀키의 값을 쉽게 알 수 없다 [3].

네 번째, 연산하는 동안 값을 숨겨 소비되는 전력이 일정하지 않게 하는 방법이 있다. 한 예로 randomized Montgomery operation을 이용하여 랜덤 마스킹을 통해 중간 연산 결과를 숨겨 일정한 전력 파형을 관찰할 수 없게 한다 [1].

다섯 째, 새로운 수 체계를 이용해 연산을 정의하는 방법이 있다. 예시로 EBNS (elevated binary number system)라는 이진수 체제를 이용하여 부채널 공격에 저항성을 가지면서 연산 효율성도 유지한다 [4].

ECC의 부채널 공격 대응방법은 위의 다섯 가지 방법 이외에도 시작점 위치를 숨기는 base point blinding, PSM에서의 항등원을 이용하여 동일한 비밀키에 대해 다른 연산량을 갖는 random scalar multiplication 등 다양한 알고리듬이 제시되어 있고, 두 가지 이상의 방법을 이용하여 더 효과적인 구조를 만들어 사용하기도 한다 [12].

Ⅳ. 결론 및 의견

부채널 공격 중에서 비침입 공격의 다양한 유형에 대해 살펴보고, ECC 프로세서 설계에 적용할 수 있는 부채널 공격 대응방법에 대해 조사했다. 표 1은 ECC에 대한 부채널 공격 유형과 대응방안에 대한 비교를 보이고 있다. 부채널 공격은 점점 다양하고 고도화된 방법으로 발전하고 있으며 이에 대한 대비도 점점 진화해야 한다. 본 논문에서 조사된 사례들을 보다 면밀하게 분석하여 향후 부채널 공격에 강한 내성을 갖는 ECC 프로세서 설계에 적용할 예정이다.

Acknowledgement

This work was supported by Korea Institute for Advancement of Technology(KIAT) grant funded by the Korea Government(MOTIE) (P0017011, HRD Program for Industrial Innovation)

References

[1] K. Liao, X. Cui, N. Liao, T. Wang, D. Yu, and X. Cui, “High-Performance Noninvasive Side-Channel Attack Resistant ECC Coprocessor for GF (2m),” in *IEEE Transactions on Industrial Electronics*, vol. 64, no. 1, pp. 727-738, Jan. 2017, doi: 10.1109/TIE.2016.2610402.

[2] J.-S. Coron, “Resistance against differential power analysis for elliptic curve cryptosystems,” in *Proc. Int. Conf. on Cryptographic Hardware & Embedded Systems*. Springer, 1999, pp. 725-725

[3] Luo, Chao. “Novel Side-channel Attacks On Emerging Cryptographic Algorithms And Computing Systems.” (2018).

[4] Huang, Yue. “Efficient scalar multiplication against side channel attacks using new number representation.” (2017).

[5] Danger, Jean-Luc, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica and David Naccache. “A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards.” *Journal of Cryptographic Engineering 3* (2013): 241-265.

[6] Tawalbeh, Loai & Houssain, Hilal & Al-Somani, Turki. “Review of Side Channel Attacks and Countermeasures on ECC, RSA, and AES Cryptosystems,” *Journal of Internet Technology and Secured Transaction*. 6. (2017).

[7] Pierre-Alain Fouque, Denis Réal, Frédéric Valette, Mhamed Drissi, “The Carry Leakage on the Randomized Exponent Countermeasure,” in *Proc. 10th International Workshop*, Washington, D.C., USA, vol. 5154, pp. 198-213, August 10-13, 2008.

[8] Suresh Chari, Josyula R. Rao, Pankaj Rohatgi, “Template Attacks,” in Proc. 4th International Workshop Redwood Shores, CA, USA, vol. 2523, pp. 13-28, August 13-15, 2002.

[9] Kai Schramm, Thomas Wollinger, and Christof Paar, “A New Class of Collision Attacks and its Application to DES,” In T. Johansson, editor, *Fast Software Encryption - FSE 2003, volume 2887 of Lecture Notes in Computer Science*, pages 206-222. Springer, 2003.

[10] Mukhtar, Naila, Mohamad Ali Mehrabi, Yinan Kong, and Ashiq Anjum. “Machine-Learning-Based Side-Channel Evaluation of Elliptic-Curve Cryptographic FPGA Processor,” *Applied Sciences 9,* no. 1: 64. https://doi.org/10.3390/app9010064 (2019)

[11] Tetsuya Izu, Bodo Möller, and Tsuyoshi Takagi, “Improved Elliptic Curve Multiplication Methods Resistant against Side Channel Attacks,” *In Proceedings of the Third International Conference on Cryptology: Progress in Cryptology (INDOCRYPT '02)*. Springer-Verlag, Berlin, Heidelberg, 296-313. 2002.

[12] Fournaris, Apostolos P., Charalambos Dimopoulos, Athanassios Moschos and Odysseas G. Koufopavlou. “Design and leakage assessment of side channel attack resistant binary edwards Elliptic Curve digital signature algorithm architectures,” *Microprocess. Microsystems* 64 (2019): 73-87.