

한국정보보호학회 충청지부

제 23회 정기총회 및 정보보호학술논문발표회

2019년 10월 18일 – 19일
대전, 한남대학교(공과대학-9호관)

Organized by

한국정보보호학회 충청지부



대신정보통신(주)



- 안세희, 김규동, 박상돈, 김소정
- 4. 취약점 공개 제도 및 버그 바운티의 활성화 저해 요인 분석 및 해결 방안 제시
- 정다운, 서정택 (순천향대학교)
- 5. EC-KCDSA에서 보수 관계의 난수를 사용하는 개인키 복구**
- 고주성, 곽진 (아주대학교)
- 6. Time Bomb 악성코드 분석을 위한 시간 가속 방법
- 이상록

14:45-15:45 Session F 정보보호관리, 정보보호표준, 콘텐츠보안, 클라우드보안
(공과대학 9호관-90518)

(좌장: 조규상 교수(동양대학교))

1. Chainlink에서 다양한 프로토콜을 지원하기 위한 스마트 컨트랙트 라이브러리 개발*
- 김근영, 박준후, 김혁진, 류재철 (충남대학교)
2. Meltdown 취약점을 이용한 Docker 컨테이너 공격 방법
- 김문선, 윤한재, 이만희 (한남대학교)
3. Intel SGX 환경에서의 Spectre 부 채널 공격 연구
- 한찬희, 이만희 (한남대학교)
4. Spectre variant-4 취약점 및 대응 패치 연구
- 성태호, 이만희 (한남대학교)
5. 검색 가능 암호와 속성기반 암호를 활용한 데이터 접근제어에 관한 연구
- 황용운, 이임영 (순천향대학교)
6. 데이터 공동소유 환경을 위한 Threshold Proxy Re-encryption
- 김원빈, 이임영 (순천향대학교)

14:45-15:45 Poster B KIISC-CC 2019
(공과대학 9호관-디자인씽킹 스튜디오(90524))

(좌장: 이만희 교수(한남대학교))

1. 대항적 예제를 이용한 악성코드 탐지모델 안전성 검증 연구
- 전동호, 윤한준

EC-KCDSA에서 보수 관계의 난수를 사용하는 개인키 복구

고주성*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

Recovery of Private Key that Uses Complementary Nonces on EC-KCDSA

Ju-Seong Ko*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요약

최근 블록체인 응용 기술의 주요 구성요소로 무결성 및 사용자 인증을 보장하는 전자 서명 알고리즘이 사용되고 있다. 전자 서명 알고리즘은 난수 생성 알고리즘 등의 암호학적 요소들과 함께 사용되기 때문에 전자 서명 알고리즘의 안전성은 암호학적 요소들에 기반한다. 하지만 해당 알고리즘들에서 보안 문제가 발생하지 않더라도 타원 곡선과의 결합으로 인해 새로운 문제가 발생할 수 있다. 따라서 본 논문에서는 타원 곡선의 특성으로 인해 EC-KCDSA에서 보수 관계의 난수를 사용한 사용자의 개인키 복구가 가능함을 분석한다.

I. 서론

최근 블록체인을 응용한 다양한 서비스가 제공되고 있으며, 블록체인 기술의 주요 구성요소로 타원 곡선 기반 전자 서명 알고리즘이 사용되고 있다. 한국에서 발표된 타원 곡선 기반 전자 서명인 EC-KCDSA(Korean Certificate based Digital Signature Algorithm using Elliptic Curves)의 서명 생성 과정을 살펴보면 서로 보수 관계의 난수 사용 시 동일한 서명 값을 생성한다[1]. 이는 EC-KCDSA에서 함께 사용하는 난수 생성 및 해시 알고리즘의 안전성과 관계 없이 사용자의 개인키를 유출시킬 수 있다.

따라서 본 논문에서는 EC-KCDSA에서 보수 관계의 난수를 사용한 사용자의 개인키 복구가 가능함을 분석한다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터 지원사업의 연구 결과로 수행되었음(IITP-2019-2016-0-00304)

II. 관련 연구

2.1 EC-KCDSA

EC-KCDSA는 ElGamal 서명 방식의 변형인 전자 서명 알고리즘으로 이산대수 문제에 안전성을 두고 있다. 난수 생성 알고리즘 및 해시 함수를 이용하여 서명을 생성한다[1]. (표 1)은 EC-KCDSA의 서명 생성 과정이다.

(표 1) EC-KCDSA 서명 생성 과정

순서	과정
입력	도메인 변수, 메시지 M , 서명키(d, Q)
출력	서명 값 (r, s)
1	난수 k 를 임의로 선택 ($k < n-1$)
2	$kG = (x_1, y_1)$
3	$r = Hash(x_1)$
4	$c_Q = MSB(x_Q y_Q, L)$
5	$v = Hash(C_Q M)$
6	$e = (r \oplus v) \bmod n$
7	$s = d(k - e) \bmod n, (s \neq 0)$
MSB(A, n) : A의 상위 n-bits 반환	

III. 개인키 복구 과정 분석

3.1 보수 관계의 난수로 동일한 서명 값 생성

동일한 개인키로 두 서명을 생성할 때, 서로 보수 관계인 난수를 사용하면 (표 1)의 3번째 과정에서 동일한 서명 값 r 이 생성된다. 이는 ECC 특성 상 난수 k 와 생성원 G 에 대해 kG 와 $-kG$ 는 동일한 x 좌표를 생성하기 때문이다.

동일한 개인키로 생성한 두 서명이 동일한 서명 값 r 을 가지면 (표 1)의 7번째 식을 변형하여 개인키를 복구할 수 있다. 다음은 동일한 개인키와 보수 관계의 난수를 이용해 두 개의 서명 값을 생성하고, 다시 서명 값을 복구하는 과정이다.

$$\bullet \quad s_1 = d(k - e_1) \bmod n, \quad s_2 = d(-k - e_2) \bmod n$$

두 식을 더한 후 다음과 같이 나타낼 수 있다.

$$\bullet \quad d = -(s_1 + s_2)(e_1 + e_2)^{-1} \bmod n$$

3.2 동일한 서명 값으로부터 개인키 복구

(표 2)는 secp283k1 파라미터를 사용하는 EC-KCDSA에서 동일한 개인키와 보수 관계의 난수를 이용해 두 서명을 생성한 것이다.

(표 2) EC-KCDSA의 두 서명 정보

과정	파라미터	16진수 값
사용된 개인키		014930E66B51F09FEEBBAFFC 9111C5CF8AE406C935AC9618 F0A613B96D97F7DB8F6EBA74
첫 번째 서명	메시지 M_1	5468697320697320612073616D70 6C65206D65737361676520666F7 22045432D4B4344534120696D70 6C656D656E746174696F6E20766 16C69646174696F6E2E
	공개키 X_q	078A6ACDD5F779F25E8AB413 965E217FE6B1B63D4717EEF50 DC8C59DF7B1A095BC3027AE
정보	공개키 Y_q	07B6D9625F2D9DDF516B5037E 1E7B11526E12AC4E65AD498C D85D65A9E915D58976C00F
	서명 값 r	E214F3CF8BBB6E92F779E6C8 A3424BA8647340025EB49EEDC 601674681B14AFD
	서명 값 s_1	0014CC0BB9245B7A8BC3C6E03 92AAACEDCED8A619D9676E9 73D5244D7F45E01DB425A93E

두 번째 서명	메시지 M_2	5468697320697320612073616D70 6C65206D65737361676520666F7 22045432D4B43445341205072697 6407433204B33792033787472406 37469304E21
정보	공개키 X_q	첫 번째와 동일
	공개키 Y_q	
	서명 값 r	
정보	서명 값 s_2	00C64D8E255B0C89CEBA7227 ECE4FA9E13031353BB21C985C B98E034D89B4AF05AC9B904

(표 3)은 (표 2)의 정보를 통해 3.1절에서 제시한 복구 과정을 수행한 것이다. 복구 과정을 통해 생성한 개인키는 (표 2)의 개인키와 일치한다.

(표 3) EC-KCDSA 개인키 복구 및 검증 과정

과정	파라미터	16진수 값
개인키 복구 과정	모듈러 n	01FFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFE9AE2ED075 77265DFF7F94451E061E163C61
	$s_1' + s_2'$	0114DE2A98A7CA5B7E4BD74B 8F46FFE85542F936C265ABB40 AE060971170160E6771F896
	$\text{inv}(e_1' + e_2')$	5172812908FD14A380BED9A8F0 0FE4AAF0E09DCE0E066A8A7 A5960B4BEFEF805662B27
	d'	014930E66B51F09FEEBBAFFC 9111C5CF8AE406C935AC9618F 0A613B96D97F7DB8F6EBA74

IV. 결론

본 논문에서는 EC-KCDSA에서 동일한 개인키와 서로 보수 관계인 난수를 이용해 두 개의 서명을 생성했을 때 서명 생성에 이용된 개인키가 복구될 수 있음을 분석하였다. 이는 EC-KCDSA에서 함께 사용하는 난수 생성 및 해시 알고리즘의 설계 목적 상 보수 관계의 난수 생성을 방지하지 않으므로 실제로 발생할 수 있다.

[참고문헌]

- [1] 한국정보통신기술협회, “부가형 전자 서명 방식 표준 - 제3부: 한국형 인증서 기반 타원 곡선 전자 서명 알고리즘(EC-KCDSA), TTAK.KO-12.0015/R3, 2016.12.