

Side-Channel Angreb På Smart-Cards og Hvordan Dette Kan Håndteres

Hayati Balo, Lars G. Rasmussen

December 2003

Abstract

Dette papir beskriver hvordan en side-channel angreb på smart-cards undgås ved at bruge forskellige metoder i implementeringsfasen af ECDSA protokollen.

1 Introduktion

Sikkerheden af et kryptosystem skal ifølge NESSIE projektet[9][13], bygges op fra grunden i protokol-niveau. Når talen er om public-key(PKI) systemer, har vi både en hemmelig - og en offentlig-nøgle. De protokoller som håndterer hemmelige nøgler skal sikkerhedcheckes i implementeringsfasen, da det er muligt at angribe systemer med henblik på afsløring af hemmelig nøgle som kan have vitale konsekvenser.

Der tales om side-channel information som “afluring” af hemmelig nøgle ved at overvåge for eks. smart cards med forskelligt udstyr.

- Eksekveringstid af algoritmen eller dele heraf.
- Strømforbruget under kørsel af algoritmen eller dele heraf.
- Elektromagnetisk udstråling fra f. eks. et smart card når det er i brug.

Ud fra disse data, er det således muligt at få information om f. eks. hemmelig nøgle i forbindelse med implementering af elliptisk kurve digital signature algoritme ECDSA. Når der er tale om en

enkelt måling foretaget f.eks. på et smart card når en bestemt algoritme eksekverer, kaldes denne process en *simple side-channel analysis* eller SPA. Når der indgår flere målinger med tilhørende statistiske analyse metoder, kaldes processen en *differential side-channel analysis* eller DPA[1].

I det følgende behandles SPA hovedsageligt ud fra artiklerne [9] og [18] og der gives metoder for at undgå SPA - angreb i implementeringsfasen i f. eks. ECDSA protokollen.

2 Elliptisk Kurve Kryptografi

En generel beskrivelse af den praktiske anvendelse af elliptiske kurver og public-key systemer findes i [11] og [12]. ECDSA er en standard protokol som er beskrevet i X9.62-1998[2] og i [14] i forbindelse med project NESSIE, New European Schemes for Signatures, Integrity and Encryption. Se for eksempel <http://www.cryptonessie.org>.

Standarden IEEE P1363/D13[3] beskriver elliptiske kurve algoritmerne og detaljerne for den praktiske implementering bl.a. i projektive koordinater. Nogle kurver er standardiserede og andre er patenterede. De standardiserede kurver som også kaldes ANSI kurver er beskrevet i FIPS PUB 186-2[5]. Under generering af offentlig nøgle i ECDSA protokollen, beregnes $Q = kP$. P er en generator for den valgte gruppe og k er et tilfældigt valgt punkt som er i gruppen og som repræsenterer den hemmelige nøgle. Q bliver så den offentlige nøgle som er kendt af alle.

Gruppestrukturen på elliptiske kurver er interessante i krypto-sammenhæng da diskrete logaritme problemet er sværere her i sammenligning med andre grupper. Sikkerheden på krypto-algoritmer er baseret på nogle talteoretiske *svære* problemer[15] som for eksempel:

- Faktorisering af heltal
- Diskret logaritme problemet

Diskret logaritme problemet for elliptiske kurver over endelige legemer kan beskrives på følgende måde: Givet en generator og et punkt på kurven Q (ie. public key), beregn k således at der gælder ligningen $Q = kP$. Dette problem er behandlet indgående i [16] og vi ved at givet Q , er det *svært* at finde k i sammenligning med andre

grupper. Vi ved også at der kan eksistere *mange* kurver for et givent endeligt legeme! Disse to forhold gør anvendelsen af elliptiske kurver attraktivt i krypto- sammenhæng.

3 Gruppestrukturen

I [17] beskrives i proposition 2.2, at summen af 3 punkter på kurven (når kurven og en linie skærer hinanden) er lig \mathcal{O} . Dvs.

$$P + Q + R = \mathcal{O} \text{ og dermed } R = -(P + Q)$$

$$P + P + R = \mathcal{O} \text{ og dermed } R = -2P$$

En ikke-singulær (non-singular betyder at diskriminaten ikke er null!) elliptisk kurve over K skrives som

$$E(K) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Denne har $\dim = 6$ som vi har set vha. Riemann-Roch i forelæsning for kurver af genus = 1 og der er 7 basis elementer. Poldybden eller "vægten", $x=2$ og $y=3$ giver faktisk den balance i hvert enkelt monomial. Dette forklarer sikkert også hvorfor vi ikke har koefficienten a_5 i ligningen!

Ved at tilføje et punkt i det uendelige \mathcal{O} , fås en kommutativ gruppe ved hjælp af denne skæring mellem en linie og kurven. Man kan vise at den generelle *Weierstrass* ligning kan transformeres om til en kortere form ved hjælp af *admissible change of variables* eller "lovlig transformation" som det også kaldes i [16]. Ligningen bliver når $\text{char} \neq 2$

$$E'(K) : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \text{ hvor}$$

$$b_2 = a_1^2 + 4a_2$$

$$b_4 = a_1a_3 + 2a_4$$

$$b_6 = a_3^2 + 4a_6$$

Denne igen kan simplificeres til følgende korte eller normale form når man forudsætter at $\text{char} \neq 3$

$$E''(K) : y^2 = x^3 + ax + b$$

Additionsformlerne bliver:

$$p = (x_1, y_1) \quad Q = (x_2, y_2)$$

Algorithm 1 Double and add

Input : $P, k = (1, k_{l-2}, \dots, k_0)_2$

Output : $Q = kP$

$R_0 \leftarrow P$

for $j = l - 2$ *down to* 0 *do*

$R_0 \leftarrow 2R_0$

if $(k_j = 1)$ *then* $R_0 \leftarrow R_0 + P$

end for

return R_0

$P + Q = (x_3, y_3)$ hvor $x_3 = \lambda^2 - (x_1 + x_2)$ og $y_3 = \lambda(x_3 - x_1) + y_1$

For $\lambda = (y_2 - y_1)/(x_2 - x_1)$ hvis $P \neq Q$

Dvs. at der er isomorfi mellem $E(K)$, $E'(K)$ og $E''(K)$. Det betyder igen at vi kan bruge korte udgave af den generelle Wierstrass ligning, nemlig $E''(K)$ når vi udleder additionsformlerne som ovenfor.

4 Side-Channel Analyse

Beregning af $Q = kP$ foretages af *algoritme 1* i implementeringsfasen. Som vi så tidligere, er formlerne for doubling og addition af punkterne forskellige derfor vil denne algoritme give to forskellige tidsmålinger. Hvis $k=1$ vil det tage længere tid om at beregne punkterne. Dette bliver “*afluret*” ved et angreb på for eksempel et smart-card hvor algoritmen er implementeret og kører kun en gang! Vi kan i hvert fald gennemskue om bittet er 1 eller nul! Og dermed *afsløre* k . Det er essensen i SPA- analyse og i [20] nævnes 3 forskellige metoder til at undgå dette.

Metode 1 : Man kan tilføje en “*dummy*” instruktion til algoritmen således at der ikke er tidsmæssigt eller strømforbrugsmæssigt er forskel på om k er lig 1 eller nul. Det er klart at der bruges “*unødigt*” for meget tid når denne algoritme bruges! Algoritmen er beskrevet i [1] og [9].

Metode 2: Overveje forskellige parametriseringer af additionsformlerne således at der ikke er forskel på doubling og addition. Dvs. at man bruger kun et sæt af formler uanset om man fordobler et punkt eller lægger to forskellige punkter sammen. Dette er faktisk emnet for dette papir hvor inspirationen er fra [18]. Herom senere!

Algorithm 2 Double and add always

Input : $P, k = (1, k_{l-2}, \dots, k_0)$

Output : $Q = kP$

$R_0 \leftarrow P$

for $j = l - 2$ *down to* 0 *do*

$R_0 \leftarrow 2R_0; R_1 \leftarrow R_0 + P$

$b \leftarrow k_j; R_0 \leftarrow R_b$

end for

return R_0

Algorithm 3 Montgomery Ladder skalær multiplikation

Input : $P, k = (1, k_{l-2}, \dots, k_0)$

Output : $Q = kP$

$R_0 \leftarrow P; R_1 \leftarrow 2P$

for $j = l - 2$ *down to* 0 *do*

$b \leftarrow k_j$

$R_{1-b} \leftarrow R_0 + R_1; R_b \leftarrow 2R_b$

end for

return R_0

Metode 3: Overvej at bruge algoritmer som ikke afslører noget uanset additionsformler. I [9] kaldes disse algoritmer “*regulære*” algoritmer og et eksempel på sådan en er beskrevet som Montgomery Ladder metoden.

5 Alternative parametriseringer og Jacobi Model

Pointen her for at undgå SPA-angreb er at anvende *Jacobi* model i stedet for *Weierstrass* model. I [9] udvikler forfatterne til artiklen ud fra en *Jacobi “quartic”* som er givet ved

$$y^2 = \epsilon x^4 - 2\delta x^2 + 1$$

og siger at alle elliptiske kurver med et punkt af orden 2 kan repræsenteres af denne. Der bliver vist en isomorfi mellem denne *Jacobi quartic* og den *Weierstrass normal form* elliptisk kurve ligning for $\text{char}(K) \neq 2, 3$

$$y^2 = x^3 + ax + b$$

I projectiv form bliver isomorfien mellem *Jacobi quartics* og den projektive udgave af *normal elliptisk kurve*, nemlig

$$Y^2 = \epsilon X^4 - 2\delta X^2 Z^2 + Z^4$$

med $\varepsilon = -(3\theta^2 + 4a)/16$ og $\delta = 3\theta/4$ beskrevet med følgende transformationsformler uden bevis.

$$(\theta, 0) \mapsto (0 : -1 : 1),$$

$$(x, y) \mapsto (2(x - \theta) : (2x + \theta)(x - \theta)^2 - y^2 : y),$$

$$\mathcal{O} \mapsto (0 : 1 : 1),$$

Tilbagekonvertering foregår ved hjælp af følgende transformation.

$$(0 : 1 : 1) \mapsto \mathcal{O},$$

$$(0 : -1 : 1) \mapsto (\theta, 0),$$

$$(X : Y : Z) \mapsto \left(2\frac{(Y+Z)^2}{X^2} - \frac{\theta}{2}, Z\frac{4(Y+Z)^2 - 3\theta X^2}{X^3}\right)$$

Additionsformlerne for punkterne $(X_1 : Y_1 : Z_1)$ og $(X_2 : Y_2 : Z_2)$ er givet ved $(X_3 : Y_3 : Z_3)$ hvor

$$X_3 = X_1 Z_1 Y_2 + Y_1 X_2 Z_2,$$

$$Y_3 = [(Z_1 Z_2)^2 + \varepsilon (X_1 X_2)^2][Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2] + 2\varepsilon X_1 X_2 Z_1 Z_2 (X_1^2 Z_2^2 + Z_1^2 X_2^2)$$

$$Z_3 = (Z_1 Z_2)^2 - \varepsilon (X_1 X_2)^2$$

Vi skal også huske at tilføje at to triplets $(X_1 : Y_1 : Z_1)$ og $(x_2 : Y_2 : Z_2)$ repræsenterer samme punkt hvis og kun hvis der eksisterer et $t \in K \setminus \{0\}$ således at følgende gælder:

$$X_1 = tX_2, Y_1 = t^2Y_2 \text{ og } Z_1 = tZ_2$$

Med lidt inspiration fra *Montgomery Ladder* algoritme 3 for skalær multiplikation foreslår den ene af forfatterne (M. Joye) til artiklen [9] algoritme 4.

Hvis man bruger en kurve med 3 punkter af orden 2 opnås der ca. 1/3 forbedring med hensyn til multiplikation med konstanter i sammenligning med en kurve med kun et punkt af orden 2! Der er altså ikke meget at hente i multiplikation i F_p (de er ens i begge tilfælde!), når man bruger alternative sæt af additionsformler i artiklen [18], men teknikken der er udviklet i artiklen [18] gælder altså ikke for alle typer af kurver og derfor kan algoritme 4 med fordel bruges ud fra et effektivitets- og generaliseringshensyn i forbindelse med undgåelse af SPA-angreb i stedet for, hvis man vil undgå at anvende specielle elliptiske kurver.

Algorithm 4 Regulær double and add

Input: $P, k = (1, k_{l-2}, \dots, k_0)_2$

Output: $Q = kP$

$R_0 \leftarrow 2P; R \leftarrow P; j = l - 2$

while ($j \geq 1$) *do*

$b \leftarrow k_j; R_0 \leftarrow R_0 + R_b$

$k_j \leftarrow 0; j \leftarrow j + b - 1$

end while

$R \leftarrow R_0 + P; b \leftarrow k_0; R_0 \leftarrow R_b$

return R_0

6 Transformation til kvartisk kurve

I forbindelse med transformationsformlerne mellem de to kurver er der forskellige ting der bør checkes.

1. De transformerede punkter ligger på den kvartiske kurve

$$Y^2 = \varepsilon X^4 - 2\delta X^2 Z^2 + Z^4.$$

Dette ses umiddelbart at være tilfældet for punkterne $T(\theta, 0) = (0 : -1 : 1)$ og $T(\mathcal{O}) = (0 : 1 : 1)$. For andre punkter har vi $T(x, y) = (2(x - \theta) : (2x + \theta)(x - \theta)^2 : y)$.

Hvis vi starter med venstre side af den kvartiske ligning får vi altså

$Y^2 = ((2x + \theta)(x - \theta)^2 - y^2)^2$. Da (x, y) ligger på den elliptiske kurve $y^2 = x^3 + ax + b$ er det det samme som

$$Y^2 = ((2x + \theta)(x - \theta)^2 - (x^3 + ax + b))^2.$$

Venstre side er hermed udtrykt som et polynomium i x . Det samme kan gøres med højre side, idet y også her kun kommer til at optræde i lige potenser og dermed kan erstattes med x ved hjælp af ligningen for den elliptiske kurve.

Derefter er det i princippet let at checke om venstre og højre side er ens, men det har vi ikke gjort da vi ikke har brugt et matematikprogram.

2. $T^{-1}(T(x, y)) = (x, y)$. Dette er oplagt for $(\theta, 0)$ og \mathcal{O} . For andre punkter (x, y) bemærker vi først at $x \neq \theta$, da $(\theta, 0)$ er det eneste punkt der har θ som første koordinat. Det er altså ok. at have $X = 2(x - \theta)$ i nævneren.

$$\text{Vi checker først } x : 2 \frac{Y+Z^2}{X^2} - \frac{\theta}{2} = 2 \frac{(2x+\theta)(x-\theta)^2 - y^2 + y^2}{4(x-\theta)^2} - \frac{\theta}{2} = 2 \frac{2x+\theta}{4} - \frac{\theta}{2} = x$$

Dernæst $y : Z \frac{4(Y+Z^2)-3\theta X^2}{X^3} = y \frac{4((2x+\theta)(x-\theta)^2 - y^2 + y^2 - 3\theta(2(x-\theta))^2)}{(2(x-\theta))^3} = y \frac{2x+\theta-3\theta}{2(x-\theta)} = y$.

3. T^{-1} er uafhængig af valg af repræsentant, dvs. $T^{-1}(tX : t^2Y : tZ) = T^{-1}(X : Y : Z)$ for $t \in K^*$. Dette ses umiddelbart ved indsættelse i formelen for T^{-1} .

4. Additionsformlerne, dvs. $T^{-1}(T(P) + T(Q)) = P + Q$. Der er to tilfælde der skal checkes, nemlig $P = Q$ og $P \neq Q$, da additionsformlerne for den elliptiske kurve er forskellige som vist tidligere. Desuden skal der også tages højde for de situationer hvor \mathcal{O} og/eller $(\theta, 0)$ indgår i beregningerne. Vi har ikke forsøgt at checke dette.

7 Eksempel over \mathcal{F}_7

Vi betragter den elliptiske kurve $y^2 = x^3 + x + 4$ over F_7 . Ved at lade x gennemløbe de 7 mulige værdier og løse ligningen for y , finder man at der er 2 løsninger for $x = 0, 4, 5$ eller 6 og 1 løsning for $x = 2$.

Lægges dertil punktet \mathcal{O} i uendelig er der altså i alt 10 punkter på kurven. Disse punkter udgør en cyklisk gruppe isomorf med \mathbb{Z}_{10} , og der er et enkelt punkt af orden 2. Vi vælger en generator $P = (0, 2)$ og opskriver punkterne:

$$P = (0, 2)$$

$$2P = (4, 4)$$

$$3P = (5, 6)$$

$$4P = (6, 3)$$

$$5P = (2, 0)$$

$$6P = (6, 4)$$

$$7P = (5, 1)$$

$$8P = (4, 3)$$

$$9P = (0, 5)$$

$$10P = \mathcal{O}$$

Punktet af orden 2 er $5P = (2, 0)$, så i vores terminologi er $\theta = 2$. Fra ligningen har vi $a = 1$ og $b = 4$, så vi kan beregne $\varepsilon = -(3\theta^2 + 4a)/16 = 6$ og $\delta = 3\theta/4 = 5$.

Vi kan nu opstille ligningen for den kvartiske kurve $Y^2 = \varepsilon X^4 - 2\delta X^2 Z^2 + Z^4 = 6X^4 + 4X^2 Z^2 + Z^4$.

Ved at sætte $Z = 1$ og lade X gennemløbe de 7 mulige værdier ser man også at denne kurve indeholder præcis 10 punkter. Ved at bruge transformationsformlerne på punkterne på den elliptiske kurve, kan vi altså få dem i samme rækkefølge som før:

$$T(P) = (3 : 4 : 2) = (5 : 1 : 1)$$

$$T(2P) = (4 : 3 : 4) = (1 : 5 : 1)$$

$$T(3P) = (6 : 2 : 6) = (1 : 2 : 1)$$

$$T(4P) = (1 : 5 : 3) = (5 : 6 : 1)$$

$$T(5P) = (0 : 6 : 1)$$

$$T(6P) = (1 : 5 : 4) = (2 : 6 : 1)$$

$$T(7P) = (6 : 2 : 1)$$

$$T(8P) = (4 : 3 : 3) = (6 : 5 : 1)$$

$$T(9P) = (3 : 4 : 5) = (2 : 1 : 1)$$

$$T(0) = (0 : 1 : 1)$$

Man kan nu verificere med eksempler at man får samme resultat uanset om man bruger de sædvanlige additionsformler eller de nye.

References

- [1] J.S.Coron. Resistance Against Differential Power Analysis. Cryptographic hardware and Embedded Systems (CHES'99), volume 1717 of Lecture Notes in Computer Science, pages 292-302, Springer Verlag 1999.
- [2] ANSi X9.62-1998. Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). ANSi draft version September 1998.
- [3] IEEE P13 63/D13/Draft cversion 13. Standard Specifications for Public Key Cryptography. Annex A Number Theoretic Background. IEEE, 1999.
- [4] E. brier and M. Joye. Weierstarss Elliptic Curves and Side-Channel Attacks. D. Naccatu and P. Paillier, Eds., Public Key Cryptography vol. 2274 of Lecture Notes in Computer Science, pp. 335-345, Springer Verlag 2002.

- [5] FIPS PUB 186-2. Digital Signature Standard DSS. Technical Information Processing Standard Publication 2000. U.S. Department of Commerce. National Institute of Standards and Technology.
- [6] M.Joye and J.J.Quiquater. Hessian Elliptic Curves and Side Channel Attacks. C.Koc, D.Naccatu and C.Paar, Eds., Cryptographic Hardware and Embedded Systems. CHES 2001, vol 2162 of lecture notes in Computer Science pp. 402-410, Springer Verlag 2001.
- [7] P.Y.Liardet and N.P.Smart. Preventing SPA/DPA in ECC systems Using the Jacobi Form in C.Koc,D.Naccatu and C.Paar(Eds.) CHES 2001,CNCS 2162 pp.391-401. 2001, Springer verlag 2001.
- [8] M.Ciet,G Piret and J.J. Quisquatr. Several Optimizations for Elliptic Curves Implementation on Smart Cards. UCL Crypto group Technical Report Series 2001. <http://www.dice.ucl.ac.be/crypto>.
- [9] M.Joye. Elliptic Curve Cryptography and Side Channel Attacks. Workshop on smart cards and Site Channel Attacks, Bochum January 30-31,2003.
- [10] I. Blake, G.Seoussi,N.Smart. elliptic Curves in Cryptography. Cambridge University press 1999.
- [11] A.J.menezes. Elliptic Curve Public Key Crypto Systems. Kluver Academic Publishers, 1993.
- [12] A. Enge. Elliptic Curves and their Application to Cryptography- An Introduction. Kluver Academic Publishers, 1999.
- [13] Portfolio of Recommended Cryptographic Primitives. NESSIE Consortium. Februar 2003. <http://www.cryptonessie.org>.
- [14] R. Shipseg. ECDSA 2001. <http://www.cryptonessie.org>
- [15] G.Martinet. The Security Assumptions, March 2001. <http://www.cryptonessie.org>
- [16] S.B.Hansen. Det Diskrete Logaritme problem elliptiske kurver og kryptografi. Speciale i matematik 2002 Århus Universitet.
- [17] J.H.Silverman. The Arithmetic of elliptic Curves. Vol 106 of Graduate Texts in Mathematics, Springer 1986. 2. ed.
- [18] O.Billet and M. Joye. The Jacobi Model of an Elliptic Curve and Side Channel Analysis.
- [19] P.Y.Liardet and N.P.Smart. Preventing SPA/DPA in ECC systems Using the Jacobi Form. C.Koc, D. Naccache and C.Paar(Eds.) CHES 2001, LNCS 2162. pp. 391-401, 2001 Springer Verlag 2001.
- [20] M.Joye. Recovering Lost Efficiency of Exponentiation Algorithms on Smart Cards. Electronic Letters, 38(19):1095-1097, 2002.