An Analysis of Goubin's Refined Power Analysis Attack

Nigel P. Smart

Dept. Computer Science,
University of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol, BS8 1UB,
United Kingdom.
nigel@cs.bris.ac.uk

Abstract. Power analysis attacks on elliptic curve based systems work by analysing the point multiplication algorithm. Recently Goubin observed that if an attacker can choose the point P to enter into the point multiplication algorithm then none of the standard three randomizations can fully defend against a DPA attack. In this paper we examine Goubin's attack in more detail and completely discount its effectiveness when the attacker chooses a point of finite order, for the remaining cases we propose a defence based on using isogenies of small degree.

1 Introduction

Elliptic curves were first introduced into cryptography by Koblitz [9] and Miller [14] in 1985. Since that time, due to their perceived advantages in bandwidth and required computing resources, there has been increasing interest in using them in low-cost cryptographically enabled devices such as smart cards.

Smart cards are a particularly interesting environment due to the ability for the attacker to mount side-channel attacks based on, for example, power analysis [10] and [11]. The idea behind these attacks is to measure the power consumption of the card and use this to derive information about the underlying secret key contained in the card. Such power attacks come in two variants; Simple Power Analysis, or SPA, uses only a single observation of the power to obtain information. Differential Power Analysis, or DPA, makes many measurements and then uses a statistical technique to deduce information about the underlying secret.

In the context of elliptic curve cryptography, power analysis is applied to determine the multiplier used in a point multiplication. In other words for public $P \in E(K)$ and a private $d \in \mathbb{Z}$ one uses power analysis to determine the value of d from the power consumed in computing

$$Q = [d]P.$$

C.D. Walter et al. (Eds.): CHES 2003, LNCS 2779, pp. 281–290, 2003.

Since DPA requires multiple measurements this means one can only apply DPA to protocols in which one applies the same private multiplier d over multiple protocol runs, with possibly different values of P in each protocol run. Hence DPA can not be applied to ECDSA, two pass ECDH or two pass ECMQV. It can however be applied to ECIES, single pass ECDH or single pass ECMQV, where one of the "ephemeral" Diffie-Hellman/MQV keys is kept constant (i.e. it is a long term static public key). On the other hand, SPA can be applied to any algorithm in which one needs to keep the multiplier secret. Hence, SPA applies to all elliptic curve protocols.

A number of ways of defending against SPA have been proposed in the literature, for example the "double and add always" method of Coron [5], or the use of the Montgomery form [15] which helps prevent both SPA and timing attacks, [16], [17]. These defences try to prevent information leaking because of the different power profile of the addition and doubling formulae for the elliptic curve.

An approach attracting increasing interest is to use group formulae which are identical for both addition and doubling. This idea was introduced in the context of the Jacobi form of an elliptic curve by Liardet and Smart [12]. This was extended to cover the Hessian form of a curve, see [7] and [19],

$$x^3 + y^3 + 1 = Dxy.$$

Note that the Hessian form curves are particularly efficient in characteristic three [20], yet this advantage can only be exploited at the expense of having different routines for addition and doubling. Finally Brier and Joye have given a single formula for both the addition and doubling law for elliptic curves in standard form [4]. To recap, the standard form for a curve in characteristic two is given by

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

whilst in large prime characteristic it is given by

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

For efficiency reasons it is common to select $a = 1$ in characteristic two and $a = -3$ in large prime characteristic, see [3] for the reasons, and many curves recommended, or mandated, in standards documents satisfy these extra conditions on a.

Yet SPA defences are not enough to prevent DPA attacks. Coron [5] proposed three possible DPA defences namely; randomizing the secret exponent d, adding random points to P to randomize the base point, using a randomized projective representation. Only the third of these can be done with minimal cost, whilst the other two are not as effective and add additional computational costs into the point multiplication algorithm. In a similar vein to randomized projective coordinates Joye and Tymen introduced two other cheap randomizations, namely random curve isomorphisms and random field isomorphisms [8].

So a combined approach of using indistinguishable group laws and a randomization of (at least one of) the projective point representation, the curve representation or the field representation; would appear to offer a defence against power analysis for elliptic curve systems. However, recently Goubin [6] observed that if the attacker can choose the point P to enter into the point multiplication algorithm then none of these three randomizations can fully defend against a DPA attack.

In this paper we examine Goubin's attack in more detail and discount its effectiveness in a large number of cases, for the remaining cases we propose a defence based on using isogenies of small degree. The paper is organized as follows: In Section 2 we describe Goubin's attack and his notion of "Special Points" and examine the three anti-DPA randomizations mentioned above. We divide the special points into two types, those of small order and those of large order. Then in Section 3 we explain how careful implementation of existing standards definitions means we need not worry about special points of small order. Then in Section 4 we recap on various aspects of isogenies on elliptic curves over finite fields. We then use these isogenies to propose a defence for special points of large order in Section 5. In addition we examine whether our proposed defence works for the elliptic curves recommended or mandated in various standards. Finally we end in Section 7 with some conclusions.

2 "Special Points"

Before presenting Goubin's refined power analysis attack we present the three standard randomized DPA defences mentioned in the introduction.

Let $C(X, Y, Z)$ denote a projective representation of the affine elliptic curve we are using in our cryptosystem, whose affine form we shall assume is monic in Y. There is a map from affine coordinates to projective coordinates

$$(x, y) \longmapsto (x, y, 1)$$

and a similar reverse one

$$(X, Y, Z) \longmapsto (X/Z^s, Y/Z^t)$$

where s and t are the "weights" of the projective representation. Note: As above, we shall use lower case letters to denote variables on the affine form of the curve and capital letters for the projective form.

The three proposed randomization defences against DPA are as follows:

2.1 Randomized Projective Coordinates

Here one takes the affine point $P = (x, y)$ and before we apply d to it we first map it into a projective representation, using a random $r \in K^*$,

$$(x, y) \longmapsto (xr^s, yr^t, r).$$

One then performs the point multiplication in projective coordinates. Since multiple runs of the protocol will result in different values of r we see that each run will be uncorrelated with other runs and so a DPA attack seems impossible to mount.

2.2 Randomized Curve Isomorphism

Here we have $P \in C$ given to us and we then define $P' = (r^s x, r^t y)$ for some random $r \in K^*$. We then consider P' as a point on C' where if C is given by

$$C = \sum a_{i,j}\, x^i y^j$$

then C' is given by

$$C' = \theta^v \sum a'_{i,j}\, x^i y^j$$

with

$$a'_{i,j} = a_{i,j} \cdot r^{-(si+jt)},$$

and v chosen so as to make C' monic in the y. The curves C and C' are isomorphic. In our cryptographic operation we now compute $Q' = (X', Y') = [d]P'$ on C' and then map this back to C via $Q = (X, Y) = (X'/r^s, Y'/r^t)$.

2.3 Randomized Field Isomorphism

Here we take $P \in C$ and apply a random field isomorphism $\kappa : K \to K'$ to both P and C so as to obtain $P' = \kappa(P)$ and $C' = \kappa(C)$. We then compute $Q' = [d]P$ and then compute $Q = \kappa^{-1}(Q')$.

Goubin [6] defines a special point $P = (x, y) \in C$ to be one in which either $x = 0$ or $y = 0$. Goubin's attack works by feeding suitable multiples P', depending on ones guess for a given bit of d, of a special point into the smart card. Then when the smart cards computes $[d]P'$, the special point will occur within the computation assuming the guess is correct. The existence of the special point will be picked up with a DPA trace since the property of being a special point is preserved under the three randomizations above.

Elliptic curves in cryptography are usually chosen to have order

$$\#E(K) = h \cdot q$$

where q is a large prime and h is a small integer called the cofactor. In practice one usually has h chosen from the set $\{1, 2, 3, 4, 6\}$. The values of h correspond to the orders of the small subgroups of $E(K)$. We say that a special point has small order if it has order dividing h, otherwise we say it has large order.

In Table 1 we examine the various cases for different curves. A "?" in the Order column denotes that the point could be one of large order, whilst a "?" in the characteristic column means the curve can be used in any characteristic.

Table 1. Table of special points on Various Elliptic Curves

Curve Equation	Char	Special Point	Order
$y^2 + xy = x^3 + ax^2 + b$	2	$(0, \theta)$	2
$y^2 + xy = x^3 + ax^2 + b$	2	$(\theta, 0)$	?
$y^2 = x^3 + ax + b$	> 3	$(\theta, 0)$	2
$y^2 = x^3 + ax + b$	> 3	$(0, \theta)$	?
$x^3 + y^3 + 1 = Dxy$	?	$(\theta, 0)$	3
$x^3 + y^3 + 1 = Dxy$	?	$(0, \theta)$	3

3 "Special Points" of Small Order

Special points of small order can be dealt with by careful implementation of the protocols used in elliptic curves. Note, that since Goubin's attack is a DPA attack we need only consider protocols in which the same secret multiplier is used on multiple runs of the protocol. Hence, we only need to consider protocols such as ECIES, single-pass ECDH and single-pass ECMQV. To deal with small subgroup attacks various standards for these protocols make use of the co-factor h as a final postprocessing step before any point multiple is used in a protocol, see [1] or [2].

For example in the one-pass Diffie–Hellman protocol; if Alice has the long term key a and Bob sends her the ephemeral public key P, then Alice will compute $Q = [a]P$ followed by the (optional) postprocessing of $[h]Q$. If the cofactor is used then one calls the protocol cofactor-Diffie–Hellman. It is step of computing $Q = [a]P$ which is used by Goubin in his power analysis attack, by sending Alice a special point P of small order.

If we insist on implementors using the cofactor variant of Diffie–Hellman then we can avoid Goubin's attack by simply reversing the order of multiplication by a and h. In other words Alice first computes $Q = [h]P$ and then computes the shared secret via $[a]Q$, if and only if $Q \neq \mathcal{O}$. Goubin's attack then no longer applies since only genuine points in the subgroup of order q are passed into the point multiplication routine with the secret exponent a.

Similar arguments, involving insisting on cofactor variants of all protocols and reversing the order of multiplication by the cofactor and the secret key, can be applied to ECMQV and ECIES as defined in [1] and [2].

Recently Shoup has proposed a new variant of ECIES [18] for inclusion in a draft ISO standard. This new variant processes the cofactor in a completely different way to the old version of ECIES. A quick look at the new ECIES reveals that the new version processes the cofactor before the secret key multiplication as we recommend, hence the new version is already protected against Goubin's attack for special points of small order.

4 Recap on Isogenies

We recap, for use in the next section, some basics on isogenies between elliptic curves. All of what we require can be found in [3].

Let E_1 and E_2 denote elliptic curves over a finite field K of characteristic p. An isogeny

$$\psi : E_1 \longrightarrow E_2$$

is a non-constant rational map which respects the group structure of E_1 and E_2, i.e.

$$\psi(P+Q) = \psi(P) + \psi(Q).$$

Every isogeny has a finite kernel and the size of this kernel is called the degree of the isogeny. If E_1 and E_2 are isogenous then we have that $\#E_1(K) = \#E_2(K)$.

If j_1 and j_2 are the j-invariants of the two curves then an isogeny of prime degree l exists (over the base field) if and only if j_1 and j_2 are a solution of the modular equation of degree l, i.e.

$$\Phi_l(j_1, j_2) = 0.$$

The equation $\Phi_l(X, Y) = 0$ defines the modular curve $X_0(l)$ which parametrizes all elliptic curves for which there is a degree l isogeny between them.

These modular equations $\Phi_l(X, Y)$ grow large quite quickly as one increases l. This has led to the introduction of more suitable modular curves (and hence equations) for larger values of l (say $l > 41$). But, since in our application we are only interested in small values of l, we will not consider these generalized modular equations and so will restrict ourselves to the standard modular curves.

As a subprocedure of the Schoof-Elkies-Atkin algorithm [3][Chapter VII] one takes an elliptic curve E_1 and then determines whether there is an elliptic curve E_2 which is l-isogenous to E_1. This is done by solving the modular equation

$$\Phi_l(X, j_1) = 0$$

over the field K. One can then determine E_2 and then, via a rather involved procedure, determine the mapping ψ. See [3][Chapter VII] for the precise algorithm for determining E_2 and ψ.

The mapping ψ for a degree l isogeny is of the form

$$\psi : \begin{cases} E_1 & \longrightarrow & E_2 \\ (x, y) & \longmapsto & \left(\frac{f_1(x)}{g(x)^2}, \frac{y \cdot f_2(x)}{g(x)^3} \right) \end{cases}$$

where f_1, f_2 and g are polynomials over K of degree $2d+1$, $3d+1$ and d, for $d = (l-1)/2$ respectively.

5 "Special Points" of Large Order

In characteristic two the special points $(\theta, 0)$ of large order can easily be defended against by use of the Montgomery ladder [13], since in that case the y-coordinate

is not used. Hence, we will restrict our discussion to large prime characteristic and to curves in Weierstrass form, since these are more important for applications.

Special points of large order have been shown to exist by Goubin on a large number of the curves of large prime characteristic defined in standards. The existence of special points of large order is due to the equation

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

being such that b is a square in $\mathbb{F}_p^*$. We propose to manage the problem of special points of large order by transferring the cryptographic protocol over to an isomorphic group (but not an isomorphic curve) via an isogeny

$$\psi : E_1 \longrightarrow E_2.$$

Note, the curve E_2 and the isogeny we will use are all defined over the base field $\mathbb{F}_p$. For each curve in the standards, which exhibits a special point, we then need to determine a fixed (low degree) isogeny to an elliptic curve which does not exhibit a special point.

In Table 2 we list all recommended/mandated curves over fields of large prime characteristic in the main standards. For each curve we list the minimal degree of an isogeny to a curve which does not exhibit a special point. If the original curve does not exhibit a special point then we specify this degree as one. We also list the degree of the minimal isogeny to a curve one would prefer, i.e. a curve which has a particularly efficient model for computational purposes, by this we mean in odd characteristic a model of the form

$$y^2 = x^3 - 3x + b.$$

If the curve has minimal isogeny degree one and if the original curve was not of the above special form then we do not give a figure for the preferred minimal degree.

The data in Table 2 was computed via the Magma computer algebra system. Given a curve and the minimal isogeny degree it is relatively straightforward, see [3][Chapter VII], to compute the equation of the isogenous curve and the isogeny itself using Vélu's formulae [21]. Indeed Magma will compute this isogeny for you if required.

Hence, all that the smart card need do to protect against special points of large order is to store along with the original curve from the standard, the equation of the isogenous curve and the equation of the isogeny and its inverse. Then input points can be mapped over to the isogenous curve for computation and then mapped back again to the original curve for further processing. Clearly all the standard defences such as randomized projective representation and randomized curve isomorphisms can then be applied to the computation on the isogenous curve.

Table 2. Minimal Isogeny Degree Needed to Remove a Special Point

Curve Name	Minimal Isogeny Degree	Preferred Minimal Degree
secp112r1	1	1
secp112r2	11	11
secp128r1	7	7
secp128r2	1	-
secp160k1	1	-
secp160r1	13	13
secp160r2	19	41
secp192k1	1	-
secp192r1	23	73
secp224k1	1	-
secp224r1	1	-
secp256k1	1	-
secp256r1	3	11
secp384r1	19	19
secp521r1	5	5

6 Relative Cost of the Isogeny Defence

To apply the isogeny defence it would be better to alter the standards so that the curves are replaced with isogenous ones. However, since this is unlikely to be an option the smart card needs to convert the input point to the isogenous curve. If we assume the isogeny is of degree l this means we need to evaluate three polynomials of degree $2d+1$, $3d+1$ and d, where $d = (l-1)/2$. Using Horner's rule this implies a maximum number of field multiplications of

$$(2d+1) + (3d+1) + d = 6d + 2 \approx 3l.$$

Of course one problem is to actually store the coefficients of the polynomials defining the isogenies, which could be a problem in a device with limited memory.

In [5] Coron mentions other defences against DPA which could be used to thwart Goubin's attack. We discuss each of these in turn:

Randomization of the Private Exponent: Here one sets $d' = d + k \cdot \#E(\mathbb{F}_p)$ for some random 20-bit (say) value k. One then computes $Q = [d']P$. On average this will require an additional

$$20M_D + 10M_A$$

field multiplications, where M_D is the number of field multiplications required in an elliptic curve doubling operation and M_A is the number of field multiplications required in an elliptic curve addition operation. Typically, with projective

coordinates, we have $M_D = 8$ and $M_A = 16$. Hence, one requires on average 320 extra field multiplications, which becomes more efficient than the isogeny method as soon as $l > 106$. Whilst this method appears to be slower than the isogeny method, it should be noted however that randomizing the private exponent is easier to implement than the isogeny method.

Point Blinding: Here one first computes $S = [d]R$, for some random value of R of large order. Then at each request for the calculation of $Q = [d]P$ one computes

$$R = (-1)^b 2R,\ S = (-1)^b 2S$$

and

$$Q = [d](P + R) - S.$$

Hence, at each iteration one needs to perform two extra point additions and two extra point doublings. This corresponds to a typical cost of 48 field multiplications, which is more efficient than the isogeny method when $l > 16$.

As we have already mentioned, Coron also proposed the use of randomized projective coordinates. This does protect against other forms of DPA, but not Goubin's attack. Hence, combining randomized projective coordinates and the isogeny method one could achieve an efficient defence against all known forms of DPA against an elliptic curve implementation.

7 Conclusion

We have shown why Goubin's refined power analysis attack can be discounted for many elliptic curve systems either by use of the cofactor variant of many protocols or the use of isogenies.

The author would like to thank Marc Joye for useful comments on an earlier draft of this paper. The observation that the Montgomery ladder removes the need to consider special points of large order in characteristic two is due to him.

References

1. ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Transport Protocols. *American National Standards Institute*, Draft 2001.
2. SECG SEC 1: Elliptic Curve Cryptography. *Standards for Efficient Cryptography Group*, 1999.
3. I.F. Blake, G. Seroussi and N.P. Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, 1999.
4. E. Brier and M. Joye. Weierstrass elliptic curves and side-channel analysis. In *Public Key Cryptography – PKC 2002*, Springer-Verlag LNCS 2274, 335–345, 2002.
5. J.-S. Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In *Cryptographic Hardware and Embedded Systems – CHES '99*, Springer-Verlag LNCS 1717, 292–302, 1999.

6. L. Goubin. A refined power analysis attack on elliptic curve cryptosystems. In *Public Key Cryptography – PKC 2003*, Springer-Verlag LNCS 2567, 199–211, 2003.
7. M. Joye and J.-J. Quisquater. Hessian elliptic curves and side-channel attacks. In *Cryptographic Hardware and Embedded Systems – CHES 2001*, Springer-Verlag LNCS 2162, 412–420, 2001.
8. M. Joye and C. Tymen. Protections against differential attacks for elliptic curve cryptography – An algebraic approach. In *Cryptographic Hardware and Embedded Systems – CHES 2001*, Springer-Verlag LNCS 2162, 377–390, 2001.
9. N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, **48**, 203–209, 1987.
10. P. Kocher, J. Jaffe and B. Jun. Introduction to differential power analysis and related attacks. Technical Report, Cryptography Research Inc., 1998.
11. P. Kocher, J. Jaffe and B. Jun. Differential power analysis. In *Advances in Cryptology – CRYPTO '99*, Springer-Verlag LNCS 1666, 388–397, 1999.
12. P.-Y. Liardet and N.P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In *Cryptographic Hardware and Embedded Systems – CHES 2001*, Springer-Verlag LNCS 2162, 401–411, 2001.
13. J. López and R. Dahab. Fast Multiplication on Elliptic Curves over $GF(2^m)$ without Precomputation In *Cryptographic Hardware and Embedded Systems – CHES 1999*, Springer-Verlag LNCS 1717, 316–327, 1999.
14. V. Miller. Uses of elliptic curves in cryptography. In *Advances in Cryptology – CRYPTO '85*, Springer-Verlag LNCS 218, 417–426, 1986.
15. P.L. Montgomery. Speeding the Pollard and Elliptic Curve Methods for factorization. *Math. Comp.*, **48**, 243–264, 1987.
16. K. Okeya, H. Kurumatani and K. Sakurai. Elliptic curve with Montgomery form and their cryptographic applications. In *Public Key Cryptography – PKC 2000*, Springer-Verlag LNCS 1751, 238–257, 2000.
17. K. Okeya and K. Sakurai. Power analysis breaks elliptic cryptosystem even secure against timing attack. In *INDOCRYPT 2000*, Springer-Verlag LNCS 1977, 178-190, 2000.
18. V. Shoup. A proposal for an ISO standard for public key encryption, v2.1. Preprint, 2001.
19. N.P. Smart. The Hessian form of an elliptic curve. In *Cryptographic Hardware and Embedded Systems – CHES 2001*, Springer-Verlag LNCS 2162, 118–125, 2001.
20. N.P. Smart and E.J. Westwood. Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three *Applicable Algebra in Engineering, Communication and Computing*, **13**, 485–497, 2003.
21. J. Vélu. Isogégnies entre courbes elliptiques. *Comptes Rendus l'Acad. Sci. Paris, Ser A*, **273**, 238–241, 1971.