An Analysis of Goubin's Refined Power Analysis Attack
CHES 2003

N.P. Smart,
Dept. Computer Science,
University of Bristol

nigel@cs.bris.ac.uk

ECC

ECC is based on arithmetic on an elliptic curve.

Curves usually chosen of the form

Char p

- $Y^2 = X^3 + aX + b$
  - Usually $a = -3$ for efficiency reasons.

Char 2

- $Y^2 + XY = X^3 + aX^2 + b$
  - Usually $a = 1$ for efficiency reasons.

ECC and SPA

There have been a number of proposed methods of protecting elliptic curves against SPA in the literature:

Main problem is that the double routine and the add routine have different power profiles.

Various proposed defences:

- Double and add always
  - Coron
- Montgomery Form
- Indistinguishable Addition Formulae
  - Liardet and Smart, Joye and Quisquater, Brier and Joye

Some of these only apply to ‘special’ elliptic curves.

ECC and DPA

However SPA defences do not protect against DPA

- DPA only applies in the ECC situation where one computes

$$Q = [d]P$$

  for fixed d and many different values of P over many protocol runs.

- i.e. we only consider DPA against the ‘curve’ part of the calculation
  - May be able to apply DPA to other parts

ECC and DPA

However SPA defences do not protect against DPA

- DPA only applies in the ECC situation where one computes

$$Q = [d]P$$

  for fixed d and many different values of P over many protocol runs.
- i.e. we only consider DPA against the ‘curve’ part of the calculation
  - May be able to apply DPA to other parts

Hence

- DPA does not apply to
  - ECDSA
  - Two pass ECDH
  - Two pass ECMQV

ECC and DPA

However SPA defences do not protect against DPA

- DPA only applies in the ECC situation where one computes

$$Q = [d]P$$

  for fixed d and many different values of P over many protocol runs.
- i.e. we only consider DPA against the ‘curve’ part of the calculation
  - May be able to apply DPA to other parts

Hence

- DPA does apply to
  - ECIES
  - One pass ECDH (i.e. one static Diffie-Hellman secret)
  - One pass ECMQV

ECC and DPA Defences

Coron proposed three possible DPA defences in the ECC arena:

- 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 computational cost.

Joye and Tymen introduced two other cheap randomizations,

- Random curve isomorphisms
- Random field isomorphisms

We now recap on these defences

ECC and DPA Defences

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.

Randomized Projective Coordinates

Take the affine point $P = (x, y)$

Map it into a projective representation, using a random $r \in K^*$,

$$(x, y) \longmapsto P' = (xr^s, yr^t, r).$$

Then compute

- $Q' = [d]P'$

Map Q' back into affine the affine form Q.

Randomized Curve Isomorphism

Take the affine point $P = (x, y) \in C$

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

- $Q' = (X', Y') = [d]P' \in C'$.

Then map this back to C via $Q = (X, Y) = (X'/r^s, Y'/r^t)$.

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

- $Q' = [d]P$

Recover Q via

- $Q = \kappa^{-1}(Q')$.

Special Points

Goubin defines a special point $P = (x, y) \in C$ to be one in which

- $x = 0$

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 device.

Then when the smart cards computes $[d]P'$, the special point will occur within the computation assuming the guess is correct.

- Existence of the special point will be picked up with a DPA trace

Special points are preserved under the three randomizations above.

- Hence, attack will apply under all three DPA defences above.

Curve Orders

Elliptic curves in cryptography are usually chosen to have order

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

where

- q is a large prime
- h is a small integer called the cofactor.

In practice one usually has $h \in \{1, 2, 3, 4, 6\}$.

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.

Special Point Orders

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

“Special Points” of Small Order

Goubin’s attack can be prevented for Special Points of small order by implementors actually implementing protocols which prevent other well known attacks.

One Pass Diffie-Hellman Protocol

- Alice has the long term key a
- Bob sends her the ephemeral public key P
- 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.

- Should insist on using the cofactor variant of Diffie–Hellman
  - Avoid Goubin’s attack by swaping the order of use of a and h.

“Special Points” of Small Order

Goubin’s attack can be prevented for Special Points of small order by implementors actually implementing protocols which prevent other well known attacks.

Protected One Pass Diffie-Hellman Protocol

- Alice has the long term key a
- Bob sends her the ephemeral public key P
- Alice computes $G = [h]P$
- If $G \neq O$
  - Alice comptues $Q = [a]G$.

- The resulting key is the same as the original version
  - But we protect against Goubin’s attack.

“Special Points” of Small Order

Goubin’s attack can be prevented for Special Points of small order by implementors actually implementing protocols which prevent other well known attacks.

Other Protocols

- Similar considerations apply to other protocols which have cofactor variants
  - One pass ECMQV
  - ECIES, as defined in X9.63 and SECG
- In these cases we have to alter the order of operations from the standard
  - This is done without affecting the results
  - Hence, can be done without affecting other parties

New-ECIES

There is a newer version of ECIES, as proposed in a draft ISO standard

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.

Recap on Isogenies

To defend against Special Points of large order we propose to make use of isogenies.

Let E_1 and E_2 be curves over K of characteristic p.

An isogeny

$$\psi : E_1 \longrightarrow E_2$$

is a non-constant rational map which respects the group structure.

- Every isogeny has a finite kernel
  - Size of kernel is the degree of the isogeny
- If E_1 and E_2 are isogenous then $\#E_1(K) = \#E_2(K)$.
- If j_1 and j_2 are the j-invariants of the two curves then an isogeny of degree l exists over K if and only if

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

Recap on Isogenies

Given E_1 we can deteremine

$$\phi_l(X, j_1)$$

and if a root exists we can determine the curve E_2 and the map

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

where

- f_1 has degree $2d+1$
- f_2 has degree $3d+1$
- g has degree d

and $d = (l-1)/2$.

“Special Points” of Large Order

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 transfer 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 $\mathbb{F}_p$.

Only the isogeny and the isogenous curve itself needs to be stored.

- They can be precomputed.

Evaluating an Isogeny

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 the isogeny is of degree l 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

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

This is low in comparison to other possible defences.

Conclusion

We have shown how Goubin's attack can be prevented

- When the special point is of small order, using an implementation trick compatible with the standards.
- When the special point is of large order, using an isogenous curve.

There is a generalisation of Goubin's attack by Akishita and Takagi to appear ISC 03.

- We have not yet investigated whether our techniques will defend against this generalisation.