On Fault-based Attacks and Countermeasures for Elliptic Curve Cryptosystems

Agustin Dominguez-Oviedo

Tecnologico de Monterrey, Campus Queretaro, Mexico

ECC 2012, Oct 31, 2012.

Outline

1. Introduction
2. Background
3. Invalid-curve Attack on Montgomery's Ladder Algorithm
4. ECSM Using Repeated and Parallel Computations
5. Algorithm-level Error Detection for ECSM
6. Conclusions and Future Work

1. Introduction

- Security of cryptosystems relies on mathematical problems that are believed to be intractable.
- In practice, cryptosystems are implemented using some programming language or hardware circuits, which run on some sort of computer.

- In real life, an adversary has a lot of possibilities to break a "provable secure" cryptosystem.

- Cryptoanalitic attacks may reveal system's vulnerabilities which then need to be fixed with countermeasures.

- Fault attacks:
  - Introduced by Boneh, DeMillo, and Lipton.
  - They take advantage of errors that occur while a cryptographic device is performing a private-key operation.
  - Such errors may be induced by a malicious adversary who has physical access to the device.
  - An erroneous output may result in leakage of secret information.

2. Background

Fault-based attacks on elliptic curve cryptosystems (ECC)

- Biehl, Meyer, and Muller introduced the first fault-based attack on ECC. They presented two variants:
  - Invalid curve attack.
  - Differential fault analysis (DFA) attack.
- Blomer, Otto, and Seifert proposed the sign change fault (SCF) attack.
  - This attack is based on changing the sign into an intermediate point during the elliptic curve scalar multiplication (ECSM).
  - This attack applies to cryptosystems that use elliptic curves over prime fields.

- SCF attack idea

Algorithm 1. Left-to-right ECSM by double-and-add

Input: $P \in E(\mathbb{F}_p)$, $k = (k_{t-1} \cdots k_1 \; k_0)_2$.
Output: $Q = kP$.

1. $Q \leftarrow \mathcal{O}$.
2. For $i = t-1$ downto 0 do
   - 2.1 $Q \leftarrow 2Q$.
   - 2.2 If $(k_i = 1)$ then
     - 2.2.1 $Q \leftarrow Q \uplus P$.
3. Return(Q).

$Q \leftarrow -Q$
Attacking
at iteration i

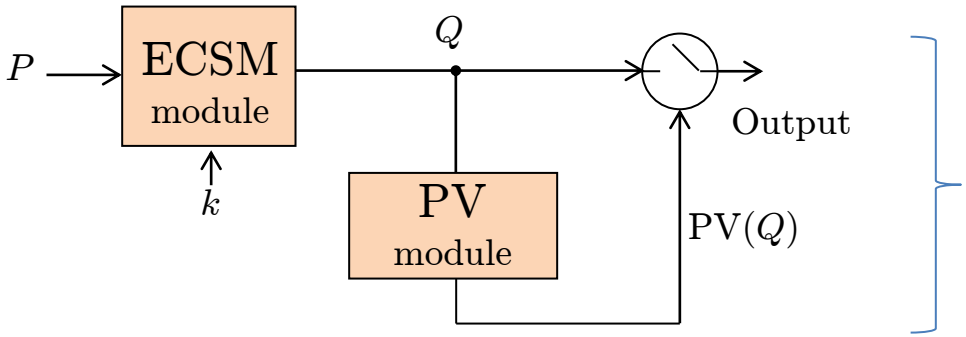
The erroneous result is: $\widetilde{Q} = \sum_{j=i+1}^{t-1} k_j 2^j P - \sum_{j=0}^{i} k_j 2^j P = 2\sum_{j=0}^{i} k_j 2^j P - kP$

- For i small enough, the $i+1$ least significant bits of k can be obtained by exhaustive search.

Error detection strategies for ECSM

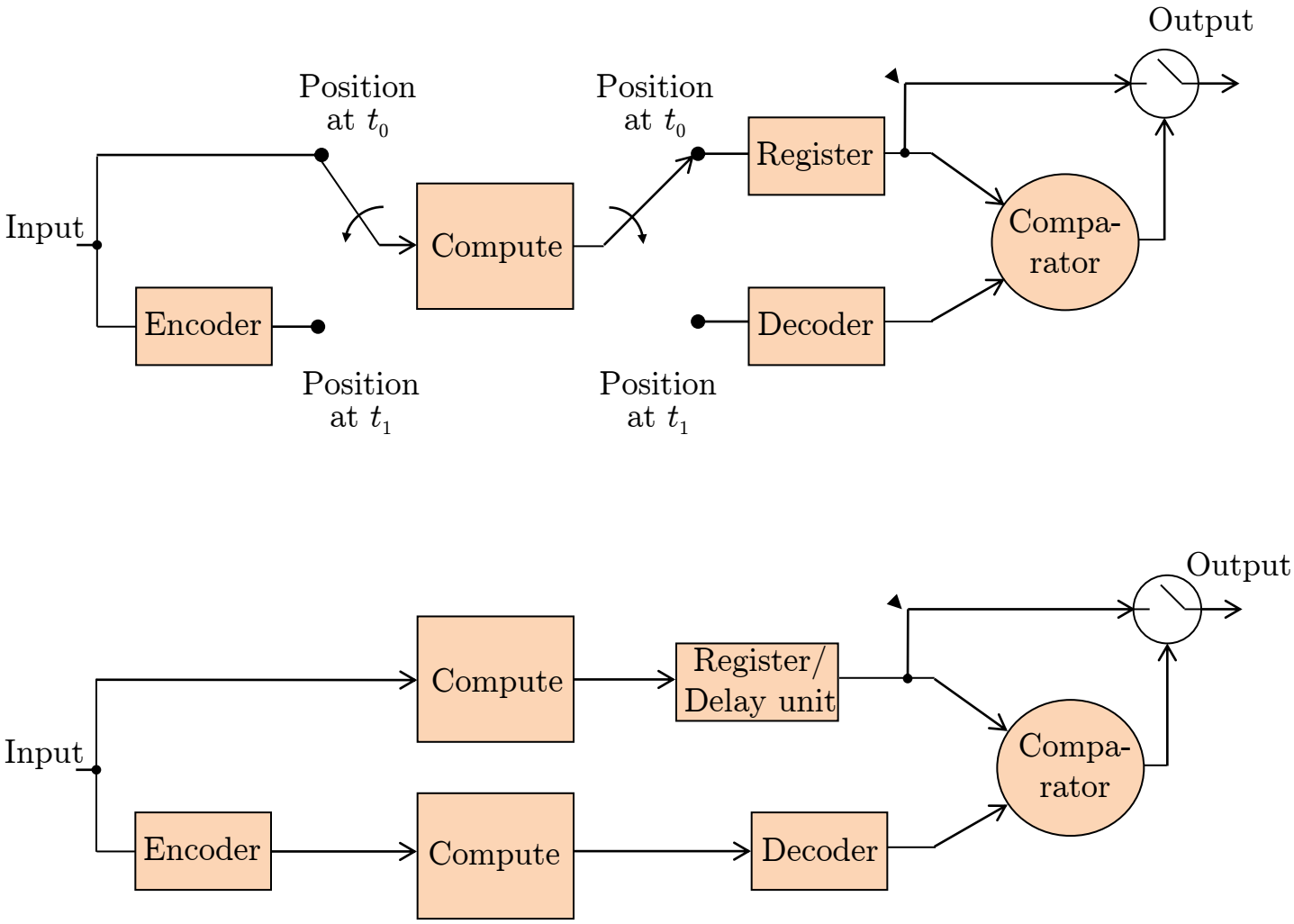
- Error detection is very important from the security point of view.
- It is a basic task in the context of fault-tolerant system design.
- Error detection using point verification (PV)

$$\mathrm{PV}(Q) = \begin{cases} \mathrm{ok} = 1 & \text{if } Q \in E(\mathbb{F}_q), \\ 0 & \text{otherwise.} \end{cases}$$



Not sufficient (e.g., the SCF attack).

- Repeated and parallel computations



- Coherency check (CC)
  - Consistency or coherency check (CC) process verifies the intermediate or final result with respect a valid pattern.
  - In the context of RSA signature generation CC has been utilized for detecting errors during the modular exponentiation.

3. Invalid-curve Attack on Montgomery's Ladder Algorithm

- An non-supersingular elliptic curve E over $\mathbb{F}_{2^m}$ is formed by the points (x, y) that satisfy the following equation:

$$E : y^2 + xy = x^3 + ax^2 + b.$$

- The invalid curve attacks reported by Biehl et. and Ciet and Joye apply for ECC applications where parameter b is not used for the group formulas.

- This is not the case for the Montgomery ladder ECSM algorithm proposed by Lopez and Dahab.
  - Parameter b is considered for point doubling.
  - But parameter a is not used.

Algorithm 1. Montgomery's ladder ECSM

Input: $P = (x, y) \in E(\mathbb{F}_{2^m})$, $k = (k_{t-1} \cdots k_1 \; k_0)_2$ with $k_{t-1} = 1$.
Output: $Q = kP$.

1. $Q_{0_x} \leftarrow x$, $Q_{1_x} \leftarrow \mathtt{x}(2P)$.
2. For $i = t - 2$ downto 0 do
   - 2.1 If $(k_i = 0)$ then
     - 2.1.1 $Q_{1_x} \leftarrow \mathtt{x}(Q_0 \uplus Q_1)$, $Q_{0_x} \leftarrow \mathtt{x}(2Q_0)$;
   - 2.2 Else
     - 2.2.1 $Q_{0_x} \leftarrow \mathtt{x}(Q_0 \uplus Q_1)$, $Q_{1_x} \leftarrow \mathtt{x}(2Q_1)$.
3. $Q_{0_y} = (Q_{0_x} + x)\left[(Q_{0_x} + x)(Q_{1_x} + x) + x^2 + y\right]/x + y$.
4. Return(Q_{0_x}, Q_{0_y}).

Group formulas utilized

- Suppose that $P = (x,y)$ is the difference between P_1 and P_0, i.e., $P_1 - P_0 = P$. If P is known, then the x-coordinate of the point addition can be obtained by the following function:

$$\mathtt{x}(P_0 \uplus P_1) = \begin{cases} x_0^2 + \dfrac{b}{x_0^2} & \text{if } P_0 = P_1, \\ x + \dfrac{x_0}{x_0 + x_1} + \left(\dfrac{x_0}{x_0 + x_1}\right)^2 & \text{if } P_0 \neq P_1. \end{cases}$$

Attack preliminaries

Theorem 1 *Let E and $\overline{E}$ be non-supersingular elliptic curves defined over $\mathbb{F}_{2^m}$. E and $\overline{E}$ given by the equations*

$$E : y^2 + xy = x^3 + ax^2 + b$$

$$\overline{E} : y^2 + xy = x^3 + \bar{a}x^2 + \bar{b}$$

are isomorphic *over $\mathbb{F}_{2^m}$ if and only if $\mathtt{Tr}(a) = \mathtt{Tr}(\bar{a})$ and $b = \bar{b}$.*

- For a fix value of parameter b there are only two isomorphic classes of curves.

- Let us define two representative elliptic curves, E_0 and E_1, one for each of there isomorphic classes:

$$E_0 : y^2 + xy = x^3 + b \qquad (a = 0),$$
$$E_1 : y^2 + xy = x^3 + x^2 + b \qquad (a = 1).$$

Lemma 1 *For E_0 and E_1:*

(i) The only points that $E_0(\mathbb{F}_{2^m})$ and $E_1(\mathbb{F}_{2^m})$ share are $\mathcal{O}$ and $(0, \sqrt{b})$.

(ii) Let $(u, v) \in E_j(\mathbb{F}_{2^m})$, where $u \in \mathbb{F}^*_{2^m}$, $v \in \mathbb{F}_{2^m}$, and $j \in \{0, 1\}$. Then, there does not exist any point in $E_{\bar{j}}(\mathbb{F}_{2^m})$ of the form (u, w) for any $w \in \mathbb{F}_{2^m}$, where $\bar{j} = 1 - j$.

Lemma 1 *(Cont.)*

(iii) *There exist two points of the form* (u, v) *and* $(u, u+v)$ *in either* $E_0(\mathbb{F}_{2^m})$ *or* $E_1(\mathbb{F}_{2^m})$ *for each* $u \in \mathbb{F}_{2^m}^*$ *and some* $v \in \mathbb{F}_{2^m}$.

(iv) *The orders of* $E_0(\mathbb{F}_{2^m})$ *and* $E_1(\mathbb{F}_{2^m})$ *satisfy the following*

$$\#E_0(\mathbb{F}_{2^m}) + \#E_1(\mathbb{F}_{2^m}) = 2^{m+1} + 2.$$

Example 1 *Let us consider* $\mathbb{F}_{2^5}$ *as represented by the irreducible polynomial* $f(z) = z^5 + z^2 + 1$. *Let us represent the elements of* $\mathbb{F}_{2^5}$ *in hexadecimal form. Let* E_0 *and* E_1 *be the curves* $y^2 + xy = x^3 + 1$ *and* $y^2 + xy = x^3 + x^2 + 1$, *respectively, defined over* $\mathbb{F}_{2^5}$. $E_0(\mathbb{F}_{2^5})$ *has an order of 44 with the following set of points:*

{(0x00,0x01),(0x01,0x00),(0x01,0x01),(0x02,0x1F),(0x02,0x1D),(0x03,0x0C),
(0x03,0x0F),(0x04,0x12),(0x04,0x16),(0x05,0x1A),(0x05,0x1F),(0x07,0x1F),
(0x07,0x18),(0x09,0x1D),(0x09,0x14),(0x0B,0x16),(0x0B,0x1D),(0x0C,0x05),
(0x0C,0x09),(0x0D,0x0B),(0x0D,0x06),(0x0F,0x19),(0x0F,0x16),(0x10,0x09),
(0x10,0x19),(0x11,0x03),(0x11,0x12),(0x12,0x14),(0x12,0x06),(0x15,0x12),
(0x15,0x07),(0x17,0x0B),(0x17,0x1C),(0x18,0x0F),(0x18,0x17),(0x1A,0x11),
(0x1A,0x0B),(0x1B,0x0F),(0x1B,0x14),(0x1C,0x09),(0x1C,0x15),(0x1F,0x06),
(0x1F,0x19),$\mathcal{O}$}.

On the other hand, $E_1(\mathbb{F}_{2^5})$ has an order of 22 with the following set of points:

{(0x00,0x01),(0x06,0x10),(0x06,0x16),(0x08,0x17),(0x08,0x1F),(0x0A,0x18),
(0x0A,0x12),(0x0E,0x07),(0x0E,0x09),(0x13,0x1C),(0x13,0x0F),(0x14,0x0D),
(0x14,0x19),(0x16,0x02),(0x16,0x14),(0x19,0x04),(0x19,0x1D),(0x1D,0x1B),
(0x1D,0x06),(0x1E,0x15),(0x1E,0x0B),$\mathcal{O}$}

Examples for NIST-recommended chosen curves (randomly chosen and Koblitz curves)

Example for $m = 163$: $f(z) = z^{163} + z^7 + z^6 + z^3 + 1$,
$b =$ 0x 00000002 0A601907 B8C953CA 1481EB10 512F7874 4A3205FD

Standard Curve B-163. $a = 1$
$\#E(\mathbb{F}_{2^{163}}) =$ 11692013098647223345629484885752781378513686403174
$=$ (2)(58460065493236116728147424428763906892568432015 87)

Weaker Curve. $\widehat{a} = 0$
$\#\widehat{E}(\mathbb{F}_{2^{163}}) =$ 11692013098647223345629472437707746935981234284444
$=$ $(2)^2$ (31)(907)(18908293)(192478327)(285644694766939633075451013 53)

Example for $m = 233$: $f(z) = z^{233} + z^{74} + 1$,
$b =$ 0x 00000066 647EDE6C 332C7F8C 0923BB58 213B333B 20E9CE42 81FE115F 7D8F90AD

Standard Curve B-233. $a = 1$
$\#E(\mathbb{F}_{2^{233}}) =$ 13803492693581127574869511724554051111679625474690027110758767268970926
$=$ (2)(69017463467905637874347558622770255558398127373450135553793836 3-4485463)

Weaker Curve. $\widehat{a} = 0$
$\#\widehat{E}(\mathbb{F}_{2^{233}}) =$ 13803492693581127574869511724554050698124810413991519109891329626226260
$=$ $(2)^2$ (5)(283)(541)(584818873)(7831953276938460946 09)(984201054369690-60152144124234193 03)

Example for $m = 283$: $f(z) = z^{283} + z^{12} + z^7 + z^5 + 1$,

$b =$ 0x 027B680A C8B8596D A5A4AF8A 19A0303F CA97FD76 45309FA2 A581485A F6263E31 3B79A2F5

Standard Curve B-283. $a = 1$

$\#E(\mathbb{F}_{2^{283}}) =$ 155413511378058325673556952545881512531392518487538097782183930535400885555747573857 42

$=$ (2)(77706755689029162836778476272940756265696259243769048891091965267700442777873786928 71)

Weaker Curve. $\widehat{a} = 0$

$\#\widehat{E}(\mathbb{F}_{2^{283}}) =$ 155413511378058325673556952545881512531392575760804225618106055022823800077085785076

$=$ $(2)^2$ (7)(19)^2(5942982169)(48758898298463720443)(45527407299960753170946983)(116544641275194419631177527)

Example for $m = 409$: $f(z) = z^{409} + z^{87} + 1$,

$b =$ 0x 0021A5C2 C8EE9FEB 5C4B9A75 3B7B476B 7FD6422E F1F3DD67 4761FA99 D6AC27C8 A9A197B2 72822F6C D57A55AA 4F50AE31 7B13545F

Standard Curve B-409. $a = 1$

$\#E(\mathbb{F}_{2^{409}}) =$ 1322111937580497197903830616065542079656809365928562438569297596608-31554965474961041628744752435822193195973457673313505354 2

$=$ (2)(661055968790248598951915308032771039828404682964281219284648798-30415777482737480520814372376217911096597986728836656752677 1)

Weaker Curve. $\widehat{a} = 0$

$\#\widehat{E}(\mathbb{F}_{2^{409}}) =$ 1322111937580497197903830616065542079656809365928562438569297584489-30761529049577288446939423450291745840511352336029816348 4

$=$ $(2)^2$ (13) (43) (599) (1867) (4201) (10711) (37882813369962759934 7) (3101704-08289997129466651228923525994078010739587674276975435706035796827 76-895114772929)

Example for $m = 571$: $f(z) = z^{571} + z^{10} + z^5 + z^2 + 1$,

$b =$ 0x 02F40E7E 2221F295 DE297117 B7F3D62F 5C6A97FF CB8CEFF1 CD6BA8CE 4A9A18AD
84FFABBD 8EFA5933 2BE7AD67 56A66E29 4AFD185A 78FF12AA 520E4DE7 39BACA0C
7FFEFF7F 2955727A

Standard Curve B-571. $a = 1$

$\#E(\mathbb{F}_{2^{571}}) =$ 772907504603451668939070378186397468859785465941286999731447050290 3-
038284579120849072287998778831546166267762243853888972493744925633 6-
261404690565766066648227863822105714 06

$=$ (2)(38645375230172583446953518909319873442989273297064349986572352 5-
145151914228956042453614399938941577308313388112192694448624687246 2-
816813070234528288303332411393191105285703)

Weaker Curve. $\widehat{a} = 0$

$\#\widehat{E}(\mathbb{F}_{2^{571}}) =$ 772907504603451668939070378186397468859785465941286999731447050290 3-
038284579120849072487067548858765683586701882154819736966569718538 3-
244825025781172616581720015410487222 92

$=$ $(2)^2$ (7)(1153)(99262049966063)(641043691173743374578683)(36502311411 -
08073953669603)(562516514411236993734142229508523209240999366989)(1 -
832372106849886832903758716153488484939785889927011316 41)

Example for $m = 163$: $f(z) = z^{163} + z^7 + z^6 + z^3 + 1$, $b = 1$

Standard Curve K-163. $a = 1$

$\#E(\mathbb{F}_{2^{163}}) = 116920130986472233456294835071968966966582371481 26$
$= (2)(58460065493236116728147417535984483483291185740 63)$

Weaker Curve. $\widehat{a} = 0$

$\#\widehat{E}(\mathbb{F}_{2^{163}}) = 116920130986472233456294738162636316178366835394 92$
$= (2)^2 (653)(6521)(341010729140266 37)(20129541232727197849723433)$

Example for $m = 233$: $f(z) = z^{233} + z^{74} + 1$, $b = 1$

Standard Curve K-233. $a = 0$

$\#E(\mathbb{F}_{2^{233}}) = 13803492693581127574869511724554051042283763955449008505312348098 96-5372$
$= (2)^2 (34508731733952818937173779311385127605709409888622521263280870-24741343)$

Weaker Curve. $\widehat{a} = 1$

$\#\widehat{E}(\mathbb{F}_{2^{233}}) = 13803492693581127574869511724554050767520671933232537715337748796 23-1814$
$= (2)(92269)(114861079)(130034039)(50621097670672361 09)(9893311373906-30128765577490907)$

Example for $m = 283$: $f(z) = z^{283} + z^{12} + z^7 + z^5 + 1$, $b = 1$

Standard Curve K-283. $a = 0$

$\#E(\mathbb{F}_{2^{283}}) =$ 155413511378058325673556952545881512531392469351722452971834999901-
9263318817690415492

$=$ (2)^2 (388533778445145814183892381364703781328481173379306132429587 49-
9752981582970442260387 3)

Other Curve. $\widehat{a} = 1$

$\#\widehat{E}(\mathbb{F}_{2^{283}}) =$ 155413511378058325673556952545881512531392624896619870428454985657 0-
3205244465645555326

$=$ (2)(777067556890291628367784762729407562656963124483099352142274928 -
2851602622232822777663)

Example for $m = 409$: $f(z) = z^{409} + z^{87} + 1$, $b = 1$

Standard Curve K-409. $a = 0$

$$\#E(\mathbb{F}_{2^{409}}) = 13221119375804971979038306160655420796568093659285624385692975800915228451569967642026930338311098320563854663624709254346844 \cdot (2)^2 \cdot (33052798439512429947595765401638551991420234148214060964232439502288071128924919105067325845777745801409636659061773135867 1)$$

Weaker Curve. $\widehat{a} = 1$

$$\#\widehat{E}(\mathbb{F}_{2^{409}}) = 13221119375804971979038306160655420796568093659285624385692976010061003197882486190980638079277513073339793817376225077823422 \cdot (2) \cdot (5616389) \cdot (90250595219) \cdot (538258252508065812423826381099759312422926717379184361670943884439581457811909443935034501042288725219735 1)$$

Example for $m = 571$: $f(z) = z^{571} + z^{10} + z^5 + z^2 + 1$, $b = 1$

Standard Curve K-571. $a = 0$

$\#E(\mathbb{F}_{2^{571}}) =$ 772907504603451668939070378186397468859785465941286999731447050290303828457912084907253591409082684733882685120330140584509469989626646924771872968646837001422293474110669 2

$=$ (2)^2 (193226876150862917234767594546599367214946366485321749932861762572575957114478021226813397852270671183470671280082535146127367497406661731192968242161709250355573368527667 3)

Weaker Curve. $\widehat{a} = 1$

$\#\widehat{E}(\mathbb{F}_{2^{571}}) =$ 772907504603451668939070378186397468859785465941286999731447050290303828457912084907223915223686346451102761292270730286436561474790548137525290500739995298056498851818700 6

$=$ (2)(835205577201087993065806 99)(596201686362718542354710701)(776087954036971417157963313951798343506780344407592335678148510064755548342323544940279982843984107558240344658148264 97)

Case	m	Curve		Size of each prime factor of $\#E(\mathbb{F}_{2^m})$ (in bits)
Randomly chosen curves	163	NIST B-163	E	2,163
		Weaker curve	$\widehat{E}$	$2, 5, 10, 25, 28, 95$
	233	NIST B-233	E	$2, 233$
		Weaker curve	$\widehat{E}$	$2, 3, 9, 10, 30, 70, 113$
	283	NIST B-283	E	$2, 283$
		Weaker curve	$\widehat{E}$	$2, 3, 5, 33, 66, 86, 87$
	409	NIST B-409	E	$2, 409$
		Weaker curve	$\widehat{E}$	$2, 4, 6, 10, 11, 13, 14, 69, 284$
	571	NIST B-571	E	$2, 570$
		Weaker curve	$\widehat{E}$	$2, 3, 11, 47, 80, 82, 159, 191$
Koblitz curves	163	NIST K-163	E	$2, 163$
		Weaker curve	$\widehat{E}$	$2, 10, 13, 55, 85$
	233	NIST K-233	E	$2, 232$
		Weaker curve	$\widehat{E}$	$2, 17, 27, 27, 63, 100$
	283	NIST K-283	E	$2, 281$
		Other curve	$\widehat{E}$	$2, 284$
	409	NIST K-409	E	$2, 407$
		Weaker curve	$\widehat{E}$	$2, 23, 37, 116, 234$
	571	NIST K-571	E	$2, 569$
		Weaker curve	$\widehat{E}$	$2, 87, 89, 395$

Attack preliminaries

- The idea is to perform the ECSM computation in a curve that does not belong the "original" isomorphic class.
- The "other" isomorphic class may include only weaker curves.
  - 9 of the 10 NIST-recommended elliptic curves.

Attack assumptions

- Consider a cryptosystem that uses a *strong* elliptic curve $E_s(a_s, b_s)$ defined over $\mathbb{F}_{2^m}$ with curve parameters a_s and b_s (e.g., a NIST-recommended elliptic curve).
- Assume that there exists a weaker curve $E_{\overline{s}}(a_{\overline{s}}, b_{\overline{s}})$ defined over $\mathbb{F}_{2^m}$ with curve parameters $a_{\overline{s}}$ and $b_{\overline{s}}$, such that $\mathtt{Tr}(a_{\overline{s}}) = \overline{\mathtt{Tr}(a_s)}$ and $b_{\overline{s}} = b_s$.

Fault model

- Fault into the x-coordinate of the input point:

$$P = (P_x, P_y) \in E_s(\mathbb{F}_{2^m}) \xrightarrow{\text{fault}} \widetilde{P} = (\widetilde{P}_x, P_y)$$

- Suppose that $\widetilde{P}$ is known.*
- Consider that the result $\widetilde{Q} = k\widetilde{P} = (\widetilde{Q}_x, \widetilde{Q}_y)$ is released.

* Similar results are obtained when these value is not known.

Attack procedure

- For a given $\widetilde{P} = (\widetilde{P}_x, P_y)$ we can verify if exists $\widehat{P} = (\widetilde{P}_x, \widehat{P}_y) \in E_{\overline{s}}(\mathbb{F}_{2^m})$ for some $\widehat{P}_y \in \mathbb{F}_{2^m}$.
- From $\widetilde{Q} = (\widetilde{Q}_x, \widetilde{Q}_y)$ we can obtain $\widehat{Q} = (\widetilde{Q}_x, \widehat{Q}_y) \in E_{\overline{s}}(\mathbb{F}_{2^m})$ for some $\widehat{Q}_y \in \mathbb{F}_{2^m}$.
- With $\widehat{P}, \widehat{Q} \in E_{\overline{s}}(\mathbb{F}_{2^m})$ we can obtain $k \bmod n$ using the Silver-Pohlig-Hellman's algorithm, where $n = \mathtt{ord}(\widehat{P})$.
- The attacker with only one pair $(\widehat{P}, \widehat{Q})$ and some acceptable amount of exhaustive search would be able to retrieve the secret scalar k with a probability of success ρ.

Probability of success

Case	m	ρ				
		$e = 0$	$e = 1$	$e = 2$	$e = 5$	$e = 10$
Randomly chosen curves	163	0.48333745	0.48333745	0.96667491	0.98278616	0.99943089
	233	0.39784981	0.39784981	0.79569963	0.99462453	0.99677211
	283	0.40601504	0.40601504	0.81203008	0.94736842	0.96992481
	409	0.44966230	0.44966230	0.89932460	0.93679646	0.99732494
	571	0.42819973	0.42819973	0.85639945	0.99913270	0.99913270
Koblitz curves	163	0.49915775	0.49915775	0.99831549	0.99831549	0.99908107
	233	0.49999457	0.99998915	0.99998915	0.99998915	0.99998915
	409	0.49999991	0.99999982	0.99999982	0.99999982	0.99999982
	571	0.49999999	0.99999999	0.99999999	0.99999999	0.99999999

Table 3.4: Probability of success ρ of obtaining k with the attack for $E_{\overline{s}}(\mathbb{F}_{2^m})$ from the NIST-recommended curves for a given parameter e

Countermeasures for this attack

- Group formulas change
  - Use both EC parameters a and b.
  - More computations required.
- Curve selection
  - Use only $E_s(\mathbb{F}_{2^m})$ for which does not exist $E_{\overline{s}}(\mathbb{F}_{2^m})$.
  - e.g., NIST K-283 curve.
- Point verification (PV)
  - PV of input.
  - PV of output.
- Coherency check (CC)
  - CC among the involved variables (i.e. $Q_0 \uplus P = Q_1$).

4. ECSM Using Repeated and Parallel Computations

Assumptions

- High-level design ➡ the ECSM module is the main block.
- ECSM module implemented in hardware.
- ECSM may become faulty:
  - Natural causes.
  - Attack from an adversary.
- Other modules are much less complex:
  - Implemented in a secure environment.
  - Software or hardware.
- Input/output of the ECSM are given in projective coordinates.

Encoding/decoding for ECSM

- Encoding for input point P:
  - Point randomization

$$(X, Y, Z) \mapsto (\gamma^c X, \gamma^d Y, \gamma Z),\ \gamma \in \mathbb{F}_q^*.$$

  - $c = 1$, $d = 2$ for $\mathcal{LD}$; and $c = 2$, $d = 3$ for $\mathcal{J}$.
  - Since $k(X, Y, Z) \sim k(\gamma^c X, \gamma^d Y, \gamma Z)$ the decoder is not needed.

Encoding/decoding for ECSM

- Encoding for scalar k :
  - Scalar randomization

$$k \mapsto k'' = k + j\#E(\mathbb{F}_q).$$

- j is a positive integer.

- No decoder needed:

$$k''P = (k + j\#E(\mathbb{F}_q))P \equiv kP.$$

Error detecting structures for ECSM

- ECSM using full re-computation (RC)

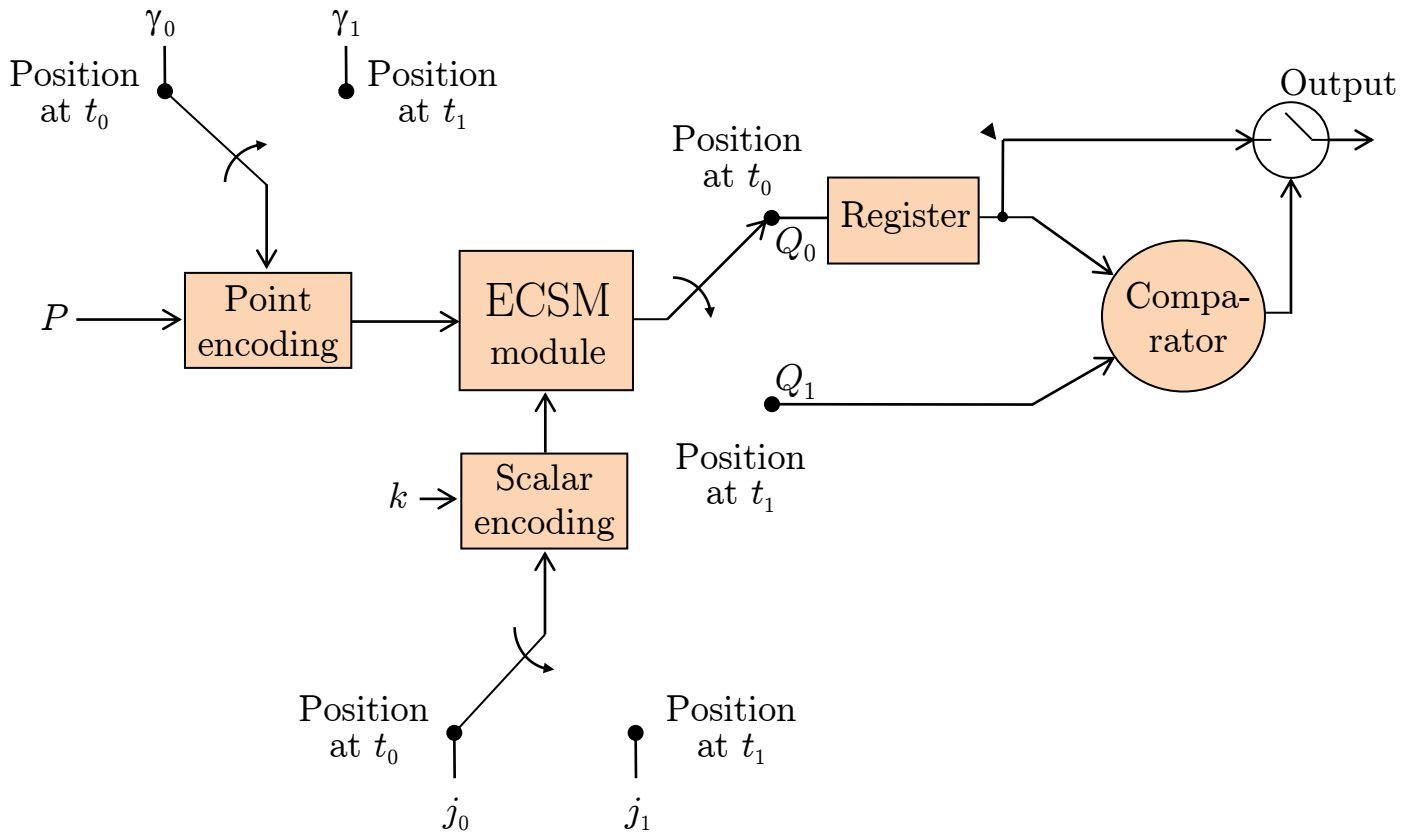


Figure 4.1: ECSM using full re-computation with point and scalar randomization (RC)

- ECSM using parallel computation (PC)

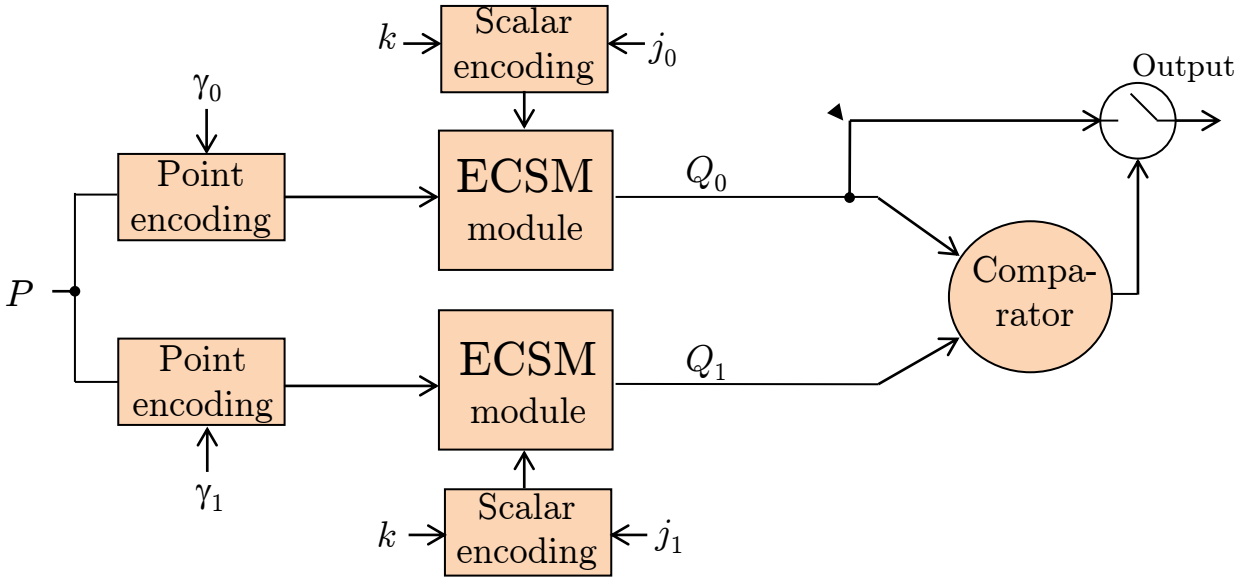
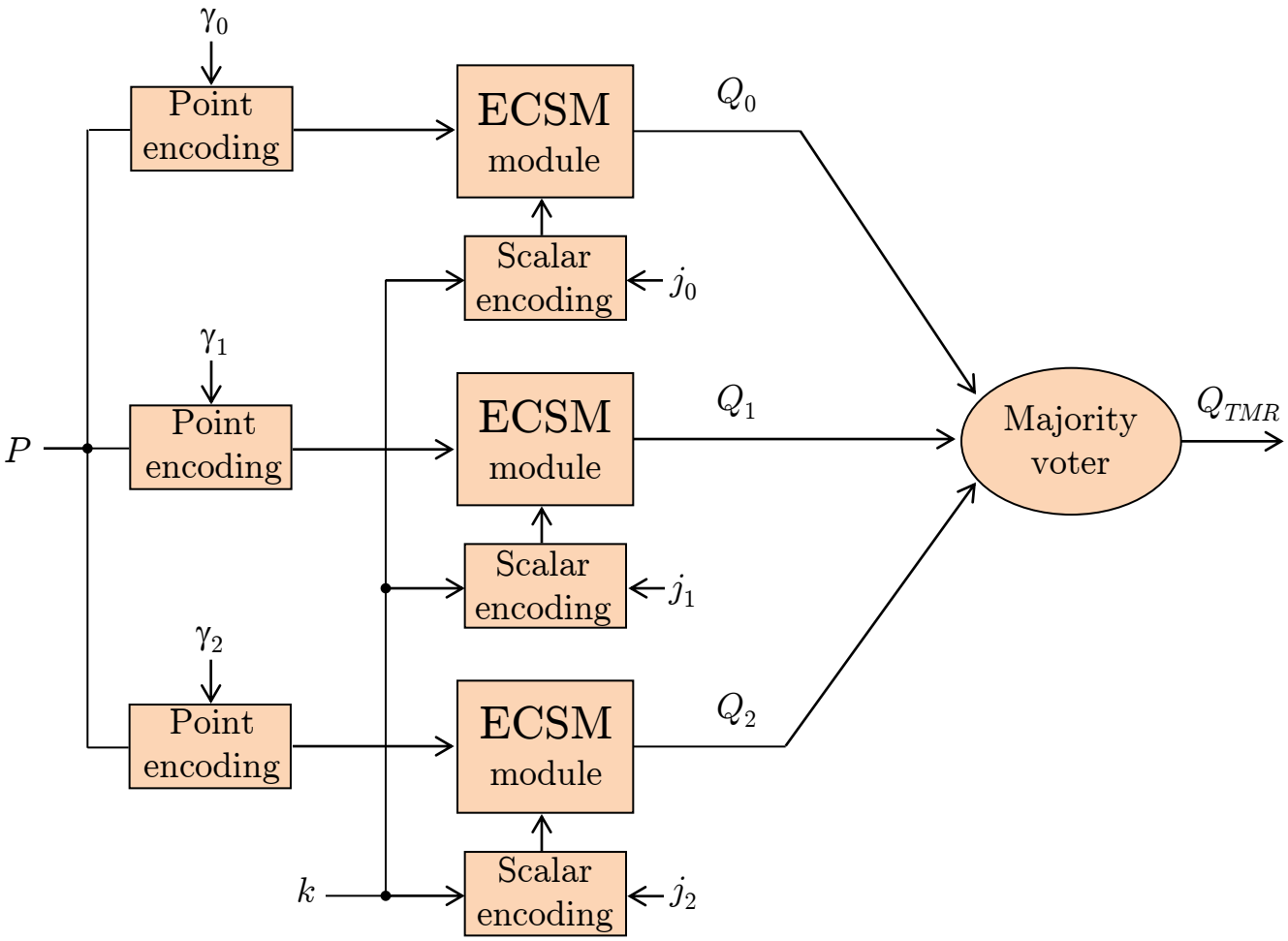
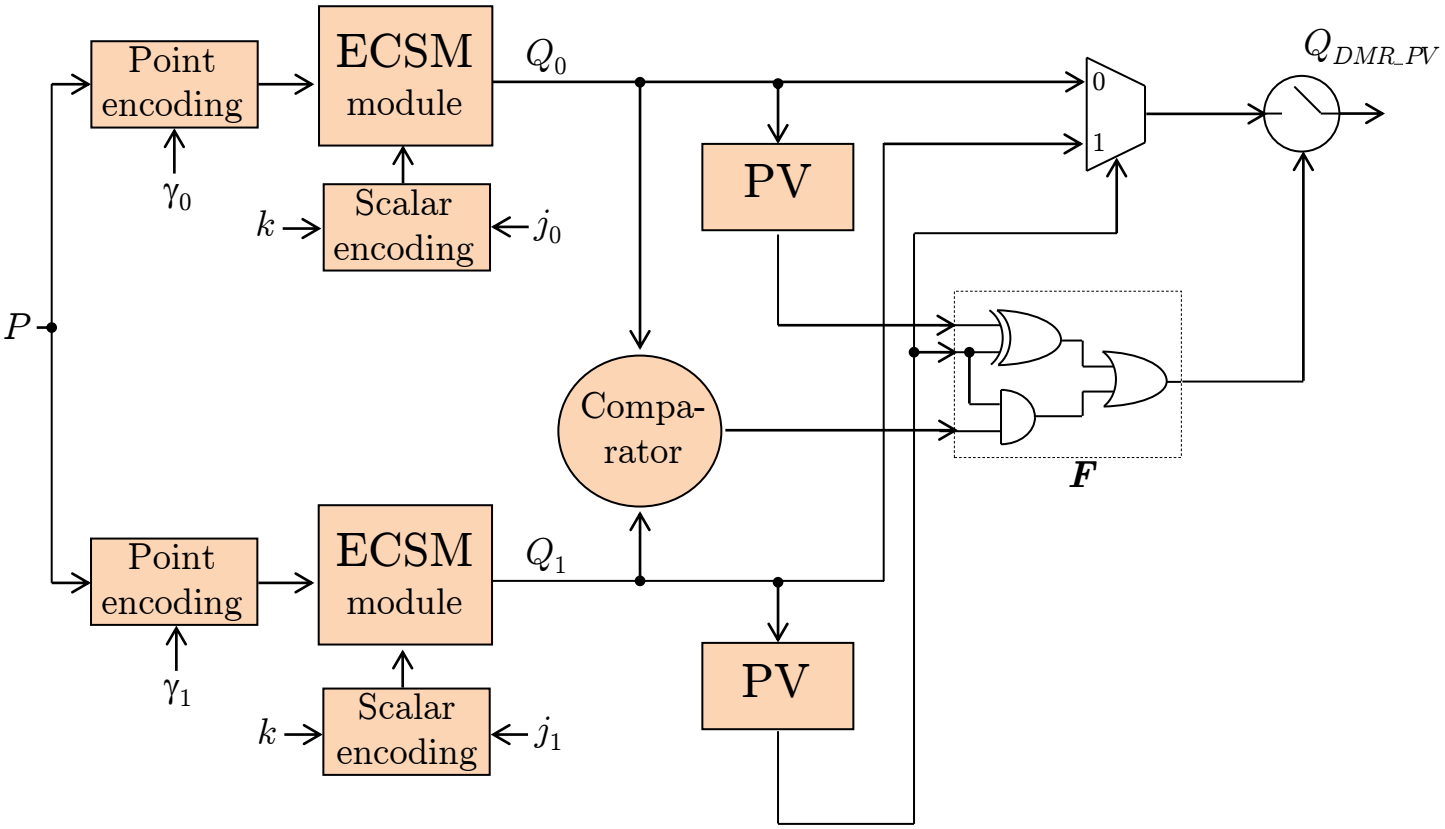


Figure 4.2: Parallel computation based ECSM with point and scalar randomization (PC)

- Triple Modular Redundancy ECSM



- Dual Modular Redundancy with Point Verification ECSM



5. Algorithm-level Error Detection for ECSM

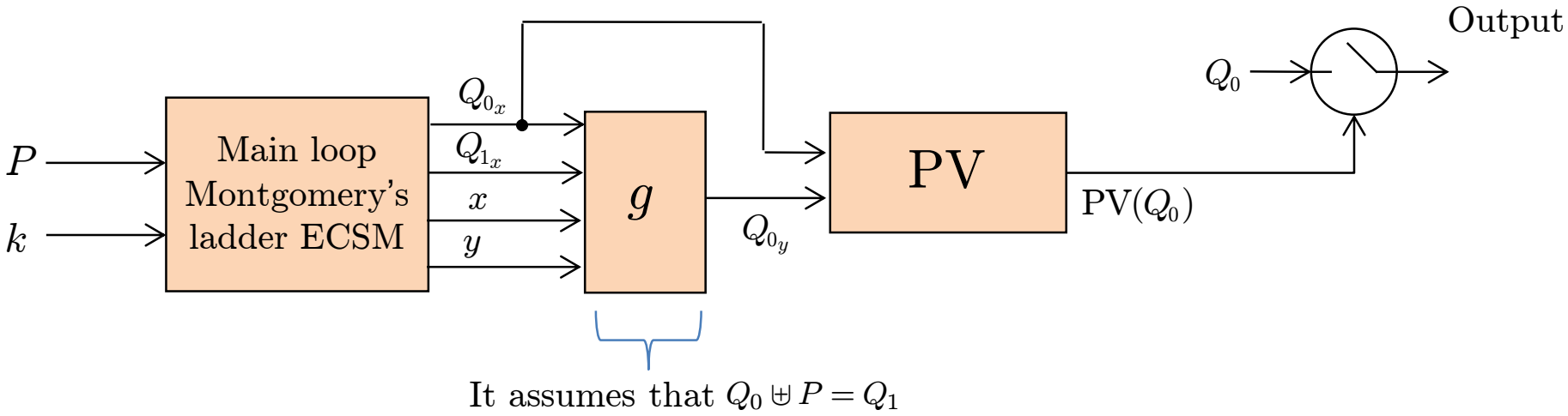
Definitions and assumptions

- Algorithm-level protections:
  - PV
  - Algorithm specific functions for CC labelled as CCi (i.e., CC1-CC4).
- Any variable utilized in ECSM can be a target of faults.

$$(V_0, V_1, \ldots V_{j-1}) \xrightarrow{\text{fault}} (\widetilde{V}_0, \widetilde{V}_1, \ldots \widetilde{V}_{j-1})$$

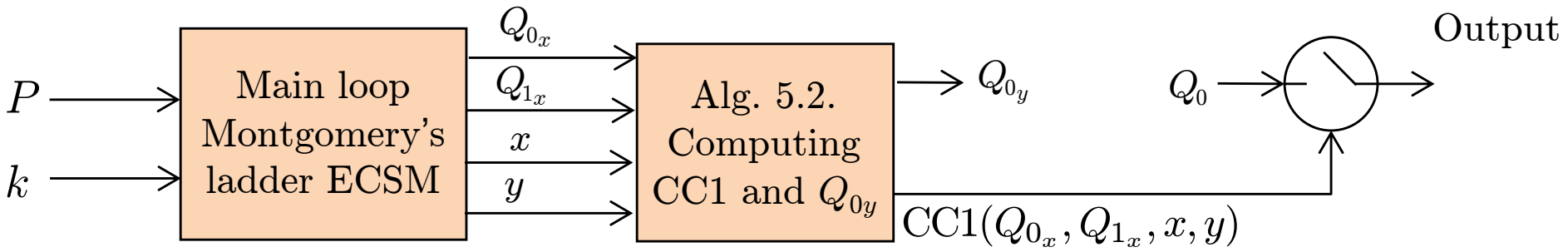
Error detection in the Montgomery ladder ECSM

- For error detection we consider:
  - PV process at the end of the ECSM: $\mathrm{PV}(Q_0)$.



Error detection in the Montgomery ladder ECSM

- CC among the involved variables: $\mathrm{CC1}(Q_{0_x}, Q_{1_x}, x, y)$.



$$\mathrm{CC1}(Q_{0_x}, Q_{1_x}, x, y) = \begin{cases} \mathrm{ok} = 1 & \text{if } \mathtt{x}(\widehat{Q}_0 \uplus P) = Q_{1_x} \text{ or } \mathtt{x}(-\widehat{Q}_0 \uplus P) = Q_{1_x}, \\ 0 & \text{otherwise.} \end{cases}$$

Error detection comparison between PV and CC1

- We have proved that the error detection coverage between PV and CC1 is equivalent if an integrity check of the input point P is performed

Error detection in ECSM by double-and-add-always

- Protections to the left-to-right and right-to-left versions.
  - PV process helps to prevent the DFA attack.
  - CC functions (CC3 and CC4) help to prevent the safe error attack proposed by Yen and Joye.
- For applications using curves over $\mathbb{F}_p$.
  - The left-to-right version is insecure against the SCF attack.
  - The right-to-left version resists the SCF attack.

Algorithm 5.5. Right-to-left double-and-add-always ECSM with PV and CC

Input: $P = (x, y) \in E(\mathbb{F}_{2^m})$ of order n, where n is an odd prime. A positive integer $k = (k_{t-1} \cdots k_1 k_0)_2$.
Output: $Q = kP$.

1. $Q_0 \leftarrow \mathcal{O}$, $Q_1 \leftarrow \mathcal{O}$, $Q_2 \leftarrow P$.
2. For $i = 0$ to $t - 1$ do
   2.1 $Q_{\overline{k_i}} \leftarrow Q_{\overline{k_i}} \uplus Q_2$.
   2.2 $Q_2 \leftarrow 2Q_2$.
3. If $((\mathrm{PV}(Q_0) = 1)$ and $(\mathrm{PV}(Q_1) = 1)$ and $(\mathrm{CC4}(Q_0, Q_1, Q_2, P) = 1)$ and $(\mathrm{IC}(P) = 1))$ then
   3.1 Return(Q_0);
4. Else return("Error detected").

- At the end of the loop:

$$Q_0 = kP,$$
$$Q_1 = \overline{k}P,$$
$$Q_2 = 2^t P, \quad \text{where } \overline{k} = 2^t - k - 1.$$

- Note that if we add Q_0, Q_1, and P we obtain

$$Q_0 \uplus Q_1 \uplus P = kP \uplus (2^t - k - 1)P \uplus P = 2^t P = Q_2.$$

- For verifying the coherency among these points:

$$\mathrm{CC4}(Q_0, Q_1, Q_2, P) = \begin{cases} \mathrm{ok} = 1 & \text{if } Q_2 = Q_0 \uplus Q_1 \uplus P, \\ 0 & \text{otherwise.} \end{cases}$$

- Example of an SCF attack on Algorithm 5.5
  - Error-free computation $k = (1110001101)_2 = 909$, $\overline{k} = (0001110010)_2 = 114$

i	0	1	2	3	4	5	6	7	8	9
Q_0	P	P	$5P$	$13P$	$13P$	$13P$	$13P$	$141P$	$397P$	$909P$
Q_1	$\mathcal{O}$	$2P$	$2P$	$2P$	$18P$	$50P$	$114P$	$114P$	$114P$	$114P$
Q_2	$2P$	$4P$	$8P$	$16P$	$32P$	$64P$	$128P$	$256P$	$512P$	$1024P$

  - SCF in Q_2 at $i = 4$

i	0	1	2	3	4	5	6	7	8	9
Q_0	P	P	$5P$	$13P$	$13P$	$13P$	$13P$	**-115P**	**-371P**	**-883P**
Q_1	$\mathcal{O}$	$2P$	$2P$	$2P$	$18P$	**-14P**	**-78P**	**-78P**	**-78P**	**-78P**
Q_2	$2P$	$4P$	$8P$	$16P$	**-32P**	**-64P**	**-128P**	**-256P**	**-512P**	**-1024P**

$$\widetilde{Q}_0 \uplus \widetilde{Q}_1 \uplus P = (-883 - 78 + 1)P = -960P \neq -1024P$$

SCF countermeasures

- Affine coordinates
  - Montgomery's ladder without using y-coordinates.
  - Algorithm 5.5.
- Projective coordinates
  - Montgomery's ladder without using Y-coordinates.
  - Combined curve
  - RC (and PC)
  - Algorithm 5.5.
- Overhead Algorithm 5.5 (# of finite field operations $t = 192$)
  - Affine $\approx 0.8\%$
  - Projective $\approx 28\%$

6. Conclusions

We have presented:

- An invalid-curve attack on the Montgomery ladder ECSM algorithm over the binary field.
- Error detection and fault tolerance in ECSM using repeated and parallel computations.
- Algorithm-level error detection in ECSM utilizing PV, CC, and IC.

More information

- A. Dominguez-Oviedo, M A. Hasan, and B. Ansari, "Fault-Based Attack on Montgomery's Ladder Algorithm", Journal of Cryptology, vol. 24, pp. 346-374, 2011.
- A. Dominguez-Oviedo and M. A. Hasan, ""Algorithm-level error detection for Montgomery ladder-based ECSM," Journal of Cryptographic Engineering, vol. 1, no. 1, pp. 57–69, 2011.
- A. Dominguez-Oviedo and M. A. Hasan, "Error detection and fault tolerance in ECSM using input randomization," IEEE Transactions on Dependable and Secure Computing, vol. 6, pp. 175–187, 2009.

Thank you!