On the Security of a Unified Countermeasure

Marc Joye

Thomson R&D, Security Labs
marc.joye@thomson.net

FDTC 2008
Washington DC ▪ August 10, 2008

This Talk

If not properly implemented, cryptosystems are susceptible to implementation attacks, including

- fault attacks, and
- side-channel attacks (SPA, DPA, . . .)

Countermeasures

For elliptic curve cryptosystems:

- Blömer, Otto and Seifert (FDTC 2005)
- Baek and Vasyltsov (ISPEC 2007)
  - fault coverage less than what was anticipated
  - further security weaknesses

Shamir's Method

- Secure evaluation of $y = f(x) \bmod p$
  - general description

$$
\begin{tikzcd}
z = f(x) \bmod pr \arrow[dr] & & y_r = f(x) \bmod r \arrow[dl] & \\
& z \bmod r \stackrel{?}{=} y_r \arrow[rr, "no"] \arrow[d, "yes"] & & \text{ERROR} \\
& y = z \bmod p & &
\end{tikzcd}
$$

Elliptic Curves over $\mathbb{F}_p$

$$E(\mathbb{F}_p) = \{y^2 = x^3 + ax + b\} \cup \{\boldsymbol{O}\}$$

- Let $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = (x_2, y_2)$
- Group law
  - $\boldsymbol{P} + \boldsymbol{O} = \boldsymbol{O} + \boldsymbol{P} = \boldsymbol{P}$
  - $-\boldsymbol{P} = (x_1, -y_1)$
  - $\boldsymbol{P} + \boldsymbol{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = (x_1 - x_3)\lambda - y_1$$

$$\text{with } \lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{[addition]} \\ \dfrac{3x_1^2 + a}{2y_1} & \text{[doubling]} \end{cases}$$

Elliptic Curves over $\mathbb{Z}_{pr}$

$$E(\mathbb{Z}_{pr}) = \{y^2 = x^3 + ax + b\} \cup \{\boldsymbol{O}\}$$

- Let $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = (x_2, y_2)$
- Addition formulas no longer a group law (!)
  - $\boldsymbol{P} + \boldsymbol{O} = \boldsymbol{O} + \boldsymbol{P} = \boldsymbol{P}$
  - $-\boldsymbol{P} = (x_1, -y_1)$
  - $\boldsymbol{P} + \boldsymbol{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = (x_1 - x_3)\lambda - y_1$$

$$\text{with } \lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{[addition]} \\ \dfrac{3x_1^2 + a}{2y_1} & \text{[doubling]} \end{cases}$$

THOMSON images & beyond

Blömer-Otto-Seifert Countermeasure

Input d, $\boldsymbol{P} = (x_1 : y_1 : 1) \in E(\mathbb{F}_p)$

Output $\boldsymbol{Q} = [d]\boldsymbol{P}$ or $\perp$

In memory prime r, curve params a_r and b_r
$\boldsymbol{P_r} \in E_r(\mathbb{F}_r)$ with $\#E_r$ a prime

1. Let $E'_{/\mathbb{Z}_{pr}} : Y^2 = X^3 + \mathrm{CRT}(a, a_r)X\,Z^4 + \mathrm{CRT}(b, b_r)\,Z^6$ and compute $\boldsymbol{P'} = \mathrm{CRT}(\boldsymbol{P}, \boldsymbol{P_r})$
2. Compute $\boldsymbol{Q'} = [d]\boldsymbol{P'}$ on E'
3. Compute $\boldsymbol{R'} = [d \pmod{\#E_r}]\boldsymbol{P_r}$ on E_r
4. Check whether
$$\boldsymbol{Q'} \overset{?}{\equiv} \boldsymbol{R'} \pmod{r}$$
and, if not, return $\perp$ and stop
5. Return $\boldsymbol{Q'}$ mod p

Baek-Vasyltsov Countermeasure

Input d, $\boldsymbol{P} = (x_1 : y_1 : 1) \in E(\mathbb{F}_p)$

Output $\boldsymbol{Q} = [d]\boldsymbol{P}$ or $\perp$

1. Choose a small random integer r
2. Compute $B = {y_1}^2 + py_1 - {x_1}^3 - ax_1 \bmod pr$ and let $E'_{/\mathbb{Z}_{pr}} : Y^2 + pYZ^3 = X^3 + aXZ^4 + BZ^6$
3. Compute $(X_d : Y_d : Z_d) = [d](x_1 : y_1 : 1)$ on E' (using an SPA-resistant point multiplication algorithm)
4. Check whether $$ {Y_d}^2 + pY_d{Z_d}^3 \stackrel{?}{\equiv} {X_d}^3 + aX_d{Z_d}^4 + B{Z_d}^6 \pmod r $$ and, if not, return $\perp$ and stop
5. Return $(X_d : Y_d : Z_d) \bmod p$

THOMSON images & beyond

Main Observation

$$ E'_{/\mathbb{Z}_{pr}} : Y^2 + pYZ^3 = X^3 + aXZ^4 + BZ^6 $$

- Point at infinity on E' is $\boldsymbol{O}_{pr} = (\theta^2 : \theta^3 : 0)$ for any $\theta \in \mathbb{Z}^*_{pr}$
- Applying the formulas yields:
  - doubling
    $$ \text{DBL-JP}(\boldsymbol{O}_{pr}) = \boldsymbol{O}_{pr} $$
  - addition
    $$ \left.\begin{array}{l} \text{ADD-JP}(\boldsymbol{P}, \boldsymbol{O}_{pr}) \\ \text{ADD-JP}(\boldsymbol{O}_{pr}, \boldsymbol{P}) \end{array}\right\} \begin{array}{l} = (0 : 0 : 0) \\ \neq \boldsymbol{P}, \quad \forall \boldsymbol{P} \in E' \end{array} $$
  - also holds for E
    - $\boldsymbol{O}_{pr} \bmod p = \boldsymbol{O}_p$
    - $(0 : 0 : 0) \bmod p = (0 : 0 : 0)$

THOMSON images & beyond

Generalization

More generally:

Proposition

Let $q \mid r$. For any $\boldsymbol{P}$ and $\boldsymbol{S}$ satisfying extended curve equation E' such that the Z-coordinate of $\boldsymbol{S}$ mod q is zero, we have:

$$\text{DBL-JP}(\boldsymbol{S}) \equiv \boldsymbol{S} \pmod{q}$$

and

$$\left.\begin{array}{l}\text{ADD-JP}(\boldsymbol{P}, \boldsymbol{S}) \\ \text{ADD-JP}(\boldsymbol{S}, \boldsymbol{P})\end{array}\right\} \equiv (0 : 0 : 0) \pmod{q}$$

Security Analysis

- Let $(X_d : Y_d : Z_d) = [d]\boldsymbol{P}$
- Verification step

$$Y_d{}^2 + pY_dZ_d{}^3 \stackrel{?}{\equiv} X_d{}^3 + aX_dZ_d{}^4 + BZ_d{}^6 \pmod{r}$$

- Expected probability of fault detection
  - about, *at best*, $2^{-|r|_2}$
  - countermeasure is not perfect
    - it checks whether $(X_d : Y_d : Z_d)$ belongs to the curve E' mod r; or
    - that it is triplet $(0 : 0 : 0)$

Effective Randomization Bit-Length

- Let q denote the largest factor of r such that $(X_d : Y_d : Z_d) \equiv (0 : 0 : 0) \pmod{q}$
- A random fault will go through verification step with probability of about $2^{-|r/q|_2} \approx 2^{-|r|_2 + |q|_2}$

  $\Longrightarrow$ "effective" bit-length of r is $|r|_2 - |q|_2$

- Numerical experiments

$\lvert r\rvert_2$	P-192	P-224	P-256	P-384	P-521
20	10.7	10.3	10.1	9.6	9.2
32	22.7	22.3	22.1	21.6	21.2
40	30.7	30.3	30.1	29.6	29.2

  - loss in effectiveness: approximately 10 bits
    - (slightly) increases with field size

THOMSON images & beyond

Proportion of Undetected Faults

- Probability that $q = r$, i.e., that $(X_d : Y_d : Z_d) \equiv (0 : 0 : 0) \pmod{r}$

  $\Longrightarrow$ a fault will not be detected

- Numerical experiments

$\lvert r\rvert_2$	P-192	P-224	P-256	P-384	P-521
20	23.2%	27.3%	28.9%	33.8%	37.3%
32	2.4%	3.1%	3.6%	5.0%	6.2%
40	0.4%	0.6%	0.7%	1.0%	1.4%

  - for 20-bit r, average proportion of undetected faults is more than 23.2%
  - for larger values, proportion is smaller but not non-negligible

THOMSON images & beyond

Further Results

- Suppose last intermediate values are no longer be randomized
  - i.e., as soon as $(X_d : Y_d : Z_d) \equiv (0:0:0) \pmod{r}$
- DPA-type attack applies on the output of the algorithm by reversing the computations
  - can be combined with Naccache-Smart-Stern attack
    - "projective coordinates leak"
    - can be prevented (affine- or randomized projective coord.)

THOMSON images & beyond

Summary

- Security analysis of Baek-Vasyltsov countermeasure
  - contermeasure leads to a larger overhead
    - 10 additional bits are required for the randomizer
    - (addition formulæ are also more costly)
  - non-negligible proportion of faults is undetected when the randomizer is in the range $2^{20} \sim 2^{40}$
- Extensive experiments on NIST-recommended curves

Conclusion

- Countermeasure should be used with care!
- Importance of using larger randomizers
  - at the cost of performance losses

THOMSON images & beyond