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 $y = f(x) \mod p$
  - general description

  $z = f(x) \mod pr$
  $y_r = f(x) \mod r$

  $z \mod r \overset{?}{=} y_r$
  \[\begin{cases}
    \text{yes} & \Rightarrow y = z \mod p \\
    \text{no} & \Rightarrow \text{ERROR}
  \end{cases}\]

Elliptic Curves over $\mathbb{F}_p$

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

- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$
- Group law
  - $P + O = O + P = P$
  - $-P = (x_1, -y_1)$
  - $P + Q = (x_3, y_3)$ where
    \[x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = (x_1 - x_3)\lambda - y_1\]

  with $\lambda = \begin{cases}
    \frac{y_1 - y_2}{x_1 - x_2} & \text{[addition]} \\
    \frac{3x_1^2 + a}{2y_1} & \text{[doubling]}
  \end{cases}$
Elliptic Curves over $\mathbb{Z}_{pr}$

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

- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$
- Addition formulas no longer a group law (!)
  - $P + O = O + P = P$
  - $-P = (x_1, -y_1)$
  - $P + Q = (x_3, y_3)$ where
    $$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = (x_1 - x_3)\lambda - y_1$$
  with $\lambda = \begin{cases} 
    \frac{y_1 - y_2}{x_1 - x_2} & \text{[addition]} \\
    \frac{3x_2^2 + a}{2y_1} & \text{[doubling]} 
  \end{cases}$

Blömer-Otto-Seifert Countermeasure

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

**Output** $Q = [d]P$ or ⊥

**In memory** prime $r$, curve params $a_r$ and $b_r$

$P_r \in E_r(\mathbb{F}_r)$ with $\#E_r$ a prime

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

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

**Output** \( Q = [d]P \) or \( \perp \)

1. Choose a small random integer \( r \)
2. Compute \( B = y_1^2 + py_1 - x_1^3 - ax_1 \mod pr \) 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 \( Y_d^2 + pY_dZ_d^3 \not\equiv X_d^3 + aX_dZ_d^4 + BZ_d^6 \mod r \)
   and, if not, return \( \perp \) and stop
5. Return \( (X_d : Y_d : Z_d) \mod p \)

**Main Observation**

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

- Point at infinity on \( E' \) is \( O_{pr} = (\theta^2 : \theta^3 : 0) \) for any \( \theta \in \mathbb{Z}_{pr}^* \)
- Applying the formulas yields:
  - doubling
    \[
    \text{DBL-JP}(O_{pr}) = O_{pr}
    \]
  - addition
    \[
    \text{ADD-JP}(P, O_{pr}) = (0 : 0 : 0) \quad \text{ADD-JP}(O_{pr}, P) \neq P, \quad \forall P \in E'
    \]
  - also holds for \( E \)
    - \( O_{pr} \mod p = O_p \)
    - \( (0 : 0 : 0) \mod p = (0 : 0 : 0) \)
Generalization

More generally:

**Proposition**

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

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

and

$$\text{ADD-JP}(P, S) \equiv (0 : 0 : 0) \pmod{q}$$

Security Analysis

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

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

- 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 $2^{-|r/q|_2} \approx 2^{-|r|_2 + |q|_2}$
  \[ \implies \text{“effective” bit-length of } r \text{ is } |r|_2 - |q|_2 \]

- Numerical experiments

| $|r|_2$ | 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

Proportion of Undetected Faults

- Probability that $q = r$, i.e., that $(X_d : Y_d : Z_d) \equiv (0 : 0 : 0) \pmod{r}$
  \[ \implies \text{a fault will not be detected} \]

- Numerical experiments

| $|r|_2$ | 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
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.)

Summary

- Security analysis of Baek-Vasyltsov countermeasure
  - countermeasure 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