2ZD-04

GLS scalar multiplication security analysis

Yue Gao[3,a)] ShuFan Wu[2,b)] Atsuko Miyaji[3,c)]

Received: January 13, 2023, Accepted: January 13, 2023

Abstract: Since the elliptic curve came up in 1985 by Miller and Koblitz, elliptic curve cryptography has become one of the most important cryptography algorithms in decades. The efficiency of its implementation attracted many researchers' attention. Scalar multiplication is one of the heaviest computations in an elliptic curve, some efficient techniques like the Gallant–Lambert– Vanstone method which adopts scalar decompositions using efficient endomorphisms have been applied broadly in practice. In this paper, we focus on the vulnerability analysis for the GLV method in GLS binary curve for corner cases, and provide a thoroughly analysis for the implementation of the GLV method in GLS curves

Keywords: Binary GLS Curves, Security, Side-channel attack

1. Introduction

The elliptic curve cryptosystem is one of the most important public key cryptosystems. Scalar Multiplication in ECC is a random scalar k multiplied by a point is the most time taken algorithm in ECC. In 2001 Gallant, Lambert, and Vanstone (GLV[1]) design a new method that uses efficiently-computable endomorphisms to replace double operation in naive double-and-add method, which has shown can accelerate point multiplication on certain ordinary elliptic curves defined over finite fields F_q. Hankerson et al.[2] implementing the GLS curves over binary field, and its been believed that binary curves are more vulnerable under attack than other curves [3].

And in [4] the author proposed λ-coordinates and associate it with GLV and GLS curves to produce a fast scalar multiplication algorithm. This algorithm has been shown to be an efficient algorithm in the security level 254-bit field. But there also have some issues related to security and integrity. In this paper, we investigate the security of the GLV method in binary GLS curves. Specifically, we focus on two sides of the security, first is the corner case which can cause the program to fail and the other is a side-channel attack called g-GHS which is an attack on a composed binary extension field. And we make a summary of the security risk of the implementation from [4] when using lambda coordinates.

2. Prelimeries

2.1 General Elliptic Curve

An ordinary binary elliptic curve in Weierstrass form is defined as:

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

With $q = 2^m$ and coefficients $a, b \in F_q, b \neq 0$ For any extension field F_{q^k}, the points $P = (x, y) \in F_{q^k} \times F_{q^k}$ that satisfy the equation from abelian group $E_{a,b}\left(F_{q^k}\right)$ together with a point at infinity ∞ .

2.2 Binary Field

The extended binary field F_{2^m} is becoming attractive because of its ”carry-free” logic which is very easy to implement.

A binary extension field can be built by taking a polynomial $f(x) \in F_2[x]$ which $f(x)$ is irreducible over F_2. This field is isomorphic to the field $F_2[x]/f(x)$. The quadratic extension of $F_2[x]/f(x)$ can be constructed by using a degree two monic polynomial and this new extension field is isomorphic to F_{q^2}. In this paper, we use $f(x) = x^{127} + x^{63} + 1$, as our base field and $g(u) = u^2 + u + 1$ the monic polynomial we used to get an extension field.

3. Lambda coordinates for GLS scalar multiplication

In [4], Oliberira et al. introduced the lambda projective system and the group law of lambda coordinates is given. Lambda projective coordinates provide an alternative formula for computing the point doubling, which replaces a general field multiplication with multiplication by the curve b parameter. For this reason, the b parameter was chosen as $b = x^{27} + 1$. And the group $E_{a,b}(F_{2^{2*127}})$ contains a subgroup of order 255 bits. The multiplication

[1] Osaka University, Graduate school of Engineering, 1-1 Yamadaoka, Suita, Osaka 565-0871,Japan
[2] National Taiwan University , No. 1, Section 4, Roosevelt Rd, Da'an District, Taipei City, Taiwan 10617
[3] Osaka University, Graduate school of Engineering, 1-1 Yamadaoka, Suita, Osaka 565-0871,Japany
[a)] gao@cy2sec.comm.eng.osaka-u.ac.jp
[b)] $w_shufan@cy2sec.comm.eng.osaka-u.ac.jp$
[c)] miyaji@cy2sec.comm.eng.osaka-u.ac.jp

in $F_{2^{2*127}}$ can be finished by shifts and xors operations. In lambda coordinates, points is represented as (x,λ) where $\lambda = x+y/x$. the λ-projective point P =(X,L,Z) corresponds to the λ affine point $(X/Z, L/Z)$ and $z\neq0$. The point at infinity is represented as $\infty = (1, 1, 0)$. The Elliptic equation in lambda projective form is:

$$(L^2 + LZ + aZ^2)X^2 = X^4 + bZ^4$$

4. Securuty Analysis under g-GHS Attack

4.1 Security analysis under Gaudry-Hess-Smart Weil descent attack

The Weil descent attack, proposed by Frey and Gangl[5], and its derivative by Hess[6], can break DLP on an algebraic curve over a composite field. For a curve defined over composite field K, using the map of scalar restriction, an algebraic curve C on a smaller field cover the curve A can be built, and by doing that the DLP on A can be reduced to DLP on C which is a smaller field that obviously easier to attack.

Menezes and Qu[7] gave an analysis of the GHS attack and showed that this attack is not applied to situations when $q = 2$ and n is prime.

But in the real world, there is still some characteristic two field like F_{2^155} is under this attack. In this section, we make a summary from [2] for the feasibility of the g-GHS attack for GLS254.

For E/F_q where q is 2^m and the quadratic twists of E, E defined over $F_{2^{2m}}$, we have isomorphic ϕ defined over F_{q^4}. Here we have Frobenius automorphism $\tau : F_{q^2} \rightarrow F_{q^2}$ defined by $x \rightarrow x^q$, for an polynomial $f = \sum_{i=0}^{d} c_i x^i$, $f \in F_2[x]$, and an element $\gamma \in F_{2^{2m}}$, $f(\tau)(\gamma) = \sum_{i=0} dc_i \gamma^{q^i}$. The Frobenius map is basically transform of the basics of a field. Let the order of be the least degree satisfying $f(\tau)(\gamma) = 0$. This order is obviously a divisor of $x^n - 1$, and the order of = order of ^{2}.

Since for GLS254 curve $E : Y^2 + XY = X^3 + aX^2 + b$ and $\#E(F_{2^{2m}}) = hr$ by definition in 2.1, the trace of a is always 1, we consider this a is fixed and denote curve by E_b.

In the field of the generally g-GHS case, when the field has a composite extension degree, we can then transform this DLP in F_{q^2} into a DLP in jacobian form hyperelliptic curve with higher-genus in which DLP problem can be expected to be solved in 2^m time.

And for the curve GLS254, even though the g-GHS attack can't be directly applied to it(faster than 2^m), we still need to pay attention to the isogenous of E where the attack may be effective. In order to avoid a g-GHS attack under this situation, first we need to choose a prime m, and then the choice of elliptic curve parameter b must be verified to not allow the attack(even though the possibility is negligible).

5. Security analysis of corner cases

5.1 Protected scalar multiplication algorithm

In [4], the author gives the definition of the protected scalar multiplication algorithm, which has shown a significant speedup compared with other scalar multiplication algorithms at the same security level.

However, there are some security issues that need to be discussed. First, the author hasn't given complete proof for the scalar multiplication algorithm. Secondly, the proof for the group law formula of *lambda*-coordinates is incomplete, so it could potentially fail some corner cases. In the implementation, k is not in the range $[1, r - 1]$, but in some cases, $k = 0$ is also a valid input for a secure constant scalar multiplication algorithm. And there is another exceptional case for this algorithm. Specifically, exceptional case happens in $P + Q$ formulas of λ-coordinates. whenever $P = \pm Q$, $P = \infty$, or $Q = \infty$. Affine point (x_P, λ_P) are represented as (X_P, L_P, Z_P) in λ coordinates where $Z \neq 0$. When the point needs to be converted back to affine coordinates, the relation $(x_P, \lambda_P) = (X_P/Z_P, L_P/Z_P)$ is used. So the point ∞ does not have a λ−coordinates representation. So the program might fail in this situation. The same situation happens for the $2Q + P$ formula, this formula breaks down when $P = \pm 2Q$ or $Q = \infty$.

6. Conclusion

We analyzed the security concerns when the GLS254 curve is used for elliptic curve cryptography. Specifically, we first analyze the feasibility of a g-GHS attack for GLS254 curves. And showed that for GLS254 curves, the g-GHS attack can apply faster than 2^m. Second, we analyzed the corner case for the implementation of the GLS curve in λ-coordinates. This implementation in [4] is not secured for corner cases. This corner case happened because the λ-coordinates can't represent the ∞ point. And it can be solved with careful implementation.

References

[1] Gallant, R. P., Lambert, R. J. and Vanstone, S. A.: Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms, Annual International Cryptology Conference (2001).

[2] Hankerson, D., Karabina, K. and Menezes, A.: Analyzing the Galbraith-Lin-Scott Point Multiplication Method for Elliptic Curves over Binary Fields, IACR Cryptology ePrint Archive, Vol. 2008, p. 334 (online), DOI: 10.1109/TC.2009.61 (2008).

[3] Arita, S., Matsuo, K., Nagao, K.-i. and Shimura, M.: A Weil descent attack against elliptic curve cryptosystems over quartic extension fields, IEICE transactions on fundamentals of electronics, communications and computer sciences, Vol. 89, No. 5, pp. 1246–1254 (2006).

[4] Oliveira, T., López-Hernández, J. C., Aranha, D. F. and Rodríguez-Henríquez, F.: Two is the fastest prime, IACR Cryptol. ePrint Arch., Vol. 2013, p. 131 (2013).

[5] FREY, G.: How to disguise an elliptic curve, Talk at the 2nd Elliptic Curve Cryptography Workshop, 1998, (online), available from ⟨https://cir.nii.ac.jp/crid/1571698600643425024⟩ (1998).

[6] Hess, F.: Generalising the GHS Attack on the Elliptic Curve Discrete Logarithm Problem, LMS Journal of Computation and Mathematics, Vol. 7, p. 167–192 (online), DOI: 10.1112/S146115700000108X (2004).

[7] Menezes, A. and Qu, M.: Analysis of the Weil Descent Attack of Gaudry, Hess and Smart, pp. 308–318 (online), DOI: 10.1007/3-540-45353-9$_2$3(2001).