On the Non-repudiation of Isogeny Based Signature Scheme

Sookyung Eom[1](✉), Hyang-Sook Lee[2], and Seongan Lim[1]

[1] Institute of Mathematical Sciences, Ewha Womans University, Seoul, Korea
[2] Department of Mathematics, Ewha Womans University, Seoul, Korea
{esk9030,hsl,seongannym}@ewha.ac.kr

Abstract. For a digital signature scheme, unforgeability and non-repudiation are two main security requirements. In 2017, Galbraith, Petit and Silva presented GPS signature, an efficient isogeny based signature with a proven unforgeability. In this paper, we present a successful key substitution attack on GPS signature which threaten the non-repudiation of GPS signature. We also suggest how to prevent key substitution attack in general as well as our attack in this paper. We also present an example of our attack using Sage to illustrate isogenies of elliptic curves and our attack.

Keywords: Isogeny-based signature · Non-repudiation · Post-quantum cryptography

1 Introduction

The essential security goals of digital signatures include integrity of the signed data, authenticity of the signed data and the signer, and non-repudiation of the origin of the signature. The unforgeability of a signature scheme guarantees the integrity and authenticity of the signature scheme. Therefore, unforgeability and non-repudiation are two main security requirements for signature schemes. The forgeability of a signature can be an evidence of the failure of non-repudiation of the signature scheme, and thus, the issue of non-repudiation of a signature can be addressed only for unforgeable signatures. However, the unforgeability of a signature may not guarantee the non-repudiation of the signature [1,6].

It suggests that further analysis on the non-repudiation of unforgeable signature schemes is necessary, especially for the newly presented signature schemes

S. Eom was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (No. 2016R1C1B2013851). H.-S. Lee was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (No. 2018R1A2A1A05079095). S. Lim was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (No. 2016R1D1A1B01008562).

Published by Springer Nature Switzerland AG 2019
O. Blazy and C. Y. Yeun (Eds.): WISTP 2018, LNCS 11469, pp. 63–77, 2019.
https://doi.org/10.1007/978-3-030-20074-9_6

such as post-quantum signatures (secure signatures in the presence of quantum computers). The isogeny-based public key cryptography is widely studied as a candidates of post-quantum signatures due to short key sizes and compatibility with the current elliptic curve primitives [3,4,10,15]. In [12], Galbraith, Petit and Silva presented an efficient isogeny based signature, which we call it as GPS signature, by applying the Fiat-Shamir transformation [2] to the De Feo-Jao-Plût identification [10]. GPS signature scheme is proven unforgeable under the hardness assumptions of some isogeny problems in the random oracle model [12].

In this paper, we study the non-repudiation of GPS signature scheme. We present a successful key substitution attack, one of the most basic attack which threaten the non-repudiation of a digital signature scheme. Our attack on GPS signature implies that the non-repudiation fails for the current version of GPS signature. Our result is the first key substitution attack on isogeny based signature schemes under the consideration of the non-repudiation of the signature. Since the non-repudiation has not been considered in the current design of isogeny based signatures even though it is one of the main security issues of digital signature schemes, we believe that our result would put forward further studies on secure design of isogeny based signatures. Our attack on GPS signature uses isomorphisms on the underlying elliptic curves and the fact that isomorphic elliptic curves have the same j-invariants. We recommend to restrict different j-invariants for each public key to prevent our key substitution attack in this paper. Moreover, we suggest to format the message as specific to each public key, such as $pk||message$, prior to signing according to the analysis of Menezes and Smart [1].

The paper is organized as follows. In Sect. 2, we give preliminaries on isogeny, non-repudiation of signature and key substitution attack. Section 3 describes our key substitution attack on GPS signature scheme using isomorphism and explain why the non-repudiation fails for GPS signature with an example of our key substitution attack. We also discuss countermeasures of our attack on GPS signature. Section 4 concludes the paper.

2 Preliminaries

In this section, we review some concepts and properties of isogenies of elliptic curves and isogeny problems related to GPS signature. We also recall the definition of key substitution attack for digital signature schemes and its impacts on the non-repudiation of signatures.

2.1 Elliptic Curves and j-invariants

Definition 2.1 *(Elliptic curve [9]). An elliptic curve over a field $\mathbb{K}$ is a smooth projective plane curve of genus one having a specified distinguished point. Projective Weierstrass equation of an elliptic curve over a field $\mathbb{K}$ is*

$$E(\mathbb{K}) \ : \ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3;$$

Affine Weierstrass equation of an elliptic curve over a field $\mathbb{K}$ *is*

$$E(\mathbb{K}) \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \textit{ with } \infty;$$

When char $K \neq 2, 3$*, we can write*

$$E(\mathbb{K}) \ : \ y^2 = x^3 + ax + b;$$

with $a, b \in \mathbb{K}$ *such that* $\triangle = -16(4a^2 + 27b^2) \neq 0$ *for smoothness condition.*

Standard projective coordinates are used to represent the points of elliptic curve $y^2 = x^3 + ax + b$. In standard projective coordinates, the triple (X, Y, Z) represents the affine point $(x = X/Z, y = Y/Z)$ of the curve. We use the standard projective coordinates in our example in Sect. 3.2.

Definition 2.2 *(j-invariant [9]). Let E be the elliptic curve given by* $y^2 = x^3 + ax + b$*, where* a, b *are elements of a field* $\mathbb{K}$ *of characteristic not 2 or 3. Define the j-invariant of E to be*

$$j = j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Given an elliptic curve E, its j-invariant can be found in polynomial-time; moreover, given a j-invariant $j^* \in \mathbb{K}$, one can find a curve E with $j(E) = j^*$ in polynomial time. As the name suggests, the j-invariant is invariant under $\overline{\mathbb{K}}$-isomorphisms of algebraic sets, and so a j-invariant uniquely identifies a $\overline{\mathbb{K}}$-isomorphism class of elliptic curves over $\mathbb{K}$.

Theorem 2.3 [9]**.** *Let* $E_1(\mathbb{K}) = \{(x_1, y_1)|y_1^2 = x_1^3 + a_1x_1 + b_1\}$ *and* $E_2(\mathbb{K}) = \{(x_2, y_2)|y_2^2 = x_2^3 + a_1x_2 + b_1\}$ *be two elliptic curves over the field* $\mathbb{K}$ *with the j-invariants* j_1 *and* j_2*, respectively. If* $j_1 = j_2$*, then there exists* $\mu \neq 0$ *in the algebraic closure* $\overline{\mathbb{K}}$ *such that* $a_2 = \mu^4 a_1$*,* $b_2 = \mu^6 b_1$*. The transformation* $x_2 = \mu^2 x_1$*,* $y_2 = \mu^3 y_1$ *takes one equation to the other.*

2.2 Isogeny

Definition 2.4 *(Isogeny [9]). Let E and* $E^{'}$ *be elliptic curves defined over a field* $\mathbb{K}$*. An isogeny from E to* $E^{'}$ *is a non constant morphism* $\phi : E \rightarrow E^{'}$ *that maps the neutral element into the neutral element.*

An isogeny $\phi : E \rightarrow E^{'}$ over a finite field $\mathbb{F}_q$ can be represented as a rational map whose coefficients belong to $\mathbb{F}_q$. An isogeny of degree m, when it is considered as a rational map, is called an m-isogeny. If ϕ is a separable isogeny, then $deg\phi = |ker\phi|$ [10]. If there is a separable isogeny between two curves, we say that they are isogenous. A theorem of Tate in [7] says that if E and E' are defined over a finite field $\mathbb{F}_q$, then E and E' are isogenous over $\mathbb{F}_q$ if and only if $|E(\mathbb{F}_q^{'}) = |E'(\mathbb{F}_q^{'})|$ for every finite extension $\mathbb{F}_q^{'}$ of $\mathbb{F}_q$. In [8], it has been shown that E' is isogenous to E over $\mathbb{F}_q$ if and only if E is isogenous to E' over $\mathbb{F}_q$.

The isogeny class of a curve E over $\mathbb{F}_q$ is defined to be the set of all curves E' which are isogenous to E, up to $\overline{\mathbb{F}_q}$-isomorphism. Since any algebraic morphism of curves is either constant or surjective [11], if $\phi : E \to E'$ is a nontrivial isogeny, then $\phi(E) = E'$.

An isogeny $\phi : E \to E^{'}$ such that $E = E'$ is called an endomorphism. The set of endomorphisms of an elliptic curve E denote $End(E)$. For a finite field $\mathbb{F}$, this set $End(E)$ is a $\mathbb{Z}$ module of rank 2 or 4. We say that E is supersingular if the rank of $End(E)$ as a $\mathbb{Z}$ module is 4, and ordinary otherwise. Any supersingular elliptic curve E is defined over $\mathbb{F}_{p^2}$ for some prime p, and for each prime $m \neq p$ there are $m + 1$ isogenies of degree m with domain E (though not all of them are defined over $\mathbb{F}_{p^2}$, in general) [10]. These isogenies of degree m are in one-to-one correspondence with the subgroups of E of order m; moreover, each such subgroup $\Phi \subset E$ is the kernel of a unique isogeny ϕ, and we write $\phi(E) = E/\Phi$ [8]. That is, an isogeny can be identified with its kernel [14]. Hence to specify an isogeny it suffices to specify its kernel, and conversely given a subgroup Φ of E we can construct the isogeny ϕ whose kernel is Φ, using Velu's formulae [13].

If we have two isogenies $\phi : E \to E^{'}$ and $\hat{\phi} : E' \to E$ such that $\phi \cdot \hat{\phi}$ and $\hat{\phi} \cdot \phi$ are the identity maps, we say that $\phi, \hat{\phi}$ are isomorphisms and E and E' are isomorphic. The isomorphic elliptic curves over finite field can be named with their j-invariant.

2.3 Computational Isogeny Problems Relating to GPS Signature

There are several hard problem candidates related to supersingular elliptic curves, we present the problems related to the security of GPS signature scheme. The GPS signature scheme is based on De Feo-Jao-Plût identification protocol [10] which uses *isogeny smooth prime* defined as follows.

Definition 2.5 *(isogeny smooth prime* [10]*).* *A prime p is called isogeny smooth prime if $p = \ell_1^{e_1}\ell_2^{e_2} f \pm 1$ where ℓ_1 and ℓ_2 are two distinct small primes, and e_1, e_2 and f are positive integers.*

The security of GPS signature scheme relies on Computational Supersingular Isogeny (CSSI) and Decisional Supersingular Product (DSSP) problems from [10]. Let E_0 and E_1 be supersingular elliptic curves over $\mathbb{F}_{p^2}$ for an isogeny smooth prime p, that is, $p = \ell_1^{e_1}\ell_2^{e_2} f \pm 1$. Let $\{R_1, S_1\}$ and $\{R_2, S_2\}$ be bases for $E_0[\ell_1^{e_1}]$ and $E_0[\ell_2^{e_2}]$, respectively.

Problem 2.6 *(Computational Supersingular Isogeny - CSSI).* *Let $\phi_1 : E_0 \to E'$ be an isogeny with kernel $\langle [m_1]R_1 + [n_1]S_1 \rangle$, where m_1, n_1 are chosen uniformly at random from $\mathbb{Z}/\ell_1^{e_1}\mathbb{Z}$, and not both divisible by ℓ_1. The problem is, given $(E', (\phi_1(R_2), \phi_1(S_2))$, to find a generator of $\langle [m_1]R_1 + [n_1]S_1 \rangle$.*

Problem 2.7 *(Decisional Supersingular Product - DSSP).* *Let $\phi : E_0 \to E_1$ be an isogeny of degree $\ell_1^{e_1}$. The problem is, given*

$$((E_0, E_1), (R_2, S_2, \phi(R_2), \phi(S_2)), (E_2, E_3)),$$

to determine from which distribution the pair (E_2, E_3) is sampled;

- (E_2, E_3) *such that there is a cyclic group* $G \subseteq E_0[\ell_2^{e_2}]$ *of order* $\ell_2^{e_2}$ *and* $E_2 \cong E_0/G$ *and* $E_3 \cong E_1/\phi(G)$.
- (E_2, E_3) *where* E_2 *is chosen at random among the curves having the same cardinality as* E_0, *and* $\phi' : E_2 \to E_3$ *is a random* $\ell_1^{e_1}$*-isogeny.*

As discussed in [10] and [12], the problems CSSI and DSSP are non-standard isogeny problems since they use special primes as *isogeny smooth prime*, use somewhat small isogeny degrees, and reveal auxiliary points. In general, the problems CSSI and DSSP are proven to be exponentially hard even under quantum attack [10], but it is known that revealing auxiliary points may be dangerous in certain context. Even with such concern on the underlying computational problems CSSI and DSSP, GPS signature is simple to describe and easy to implement which could be very important advantages in practice.

2.4 Non-repudiation of Signature Scheme and Key Substitution Attack

A digital signature scheme consists of three polynomial time algorithms

$$(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$$

which are defined as follows:

$\mathsf{KeyGen}(1^\lambda)$: On a given security parameter λ, the algorithm KeyGen outputs a pair (pk, sk) of keys, where pk is a public key for signature verification and sk is a private key for signature generation. The private key sk is kept secret by the owner of the public key pk.

$\mathsf{Sign}(sk, m \in \{0,1\}^*)$: On a given message $m \in \{0,1\}^*$ and a private key sk, the algorithm Sign outputs a signature σ_m.

$\mathsf{Verify}(m, \sigma_m, pk)$: On a given input $((m, \sigma_m), pk)$, the algorithm Verify outputs $1(=\mathsf{valid})$ or $0(=\mathsf{invalid})$.

We say that a digital signature is correct if

$$\mathsf{Verify}(m, \mathsf{Sign}(sk, m \in \{0,1\}^*), pk) = 1$$

for any $(pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$ and message m. The existential unforgeability (EUF) of a signature requires that it is infeasible for anyone to compute a valid signature under a public key pk without knowing the private key sk. Generally, a secure signature scheme means EUF-CMA (existential unforgeable against chosen message attack) secure which is defined as follows.

Definition 2.8 *(EUF-CMA). A digital signature scheme* $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ *is EUF-CMA secure if for all probabilistic polynomial-time algorithm* $\mathcal{A}$ *with access to a signing oracle* $\mathsf{Sign}(\cdot, sk)$, *there is a negligible function* $\epsilon(\cdot)$ *such that:*

$$\Pr\left[\begin{cases}(pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\cdot, sk)}(pk)\end{cases} : (m^* \notin Q) \wedge (\mathsf{Verify}(m^*, \sigma^*, pk) = 1)\right] \leq \epsilon(\lambda),$$

where Q *is the set of queries which* $\mathcal{A}$ *has accessed to the signing oracle.*

The non-repudiation of a signature requires that it is infeasible for the signer to repudiate his/her signing on a valid signature under the public key pk of the signer. For a digital signature scheme, unforgeability and non-repudiation are two main security requirements which seem to be closely related. The existence of a forged signature of a signature scheme lets the signer to claim his/her signed signature as a forged signature. Therefore, issue of non-repudiation of a signature is to be considered only for EUF-CMA secure signatures. It is known that unforgeability of signature may not guarantee the non-repudiation of the signature [1,6].

We focus on the non-repudiation of digital signatures in this paper. The most basic attack for the non-repudiation is the public key substitution attack. The goal of public key substitution attack is to compute a new public key pk' where a valid signature σ on a message m under a public key pk can be also validated under pk'. Therefore, any signer can repudiate his/her signing on a signature σ on a message by using the existence of a successful key substitution attack. More precisely, the signer, the owner of public key pk, computes pk' by using a key substitution attack and claims that the signature σ is signed by the owner of pk', not himself/herself. The key substitution attack has been formalized as follows.

Definition 2.9 ***(Key Substitution Attack)*** [6]**.** *Given a signature scheme* $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$*, a key substitution attack is a probabilistic polynomial-time algorithm* $\mathcal{A}$ *which on input of valid domain parameters outputs two valid public keys* pk *and* pk' *and a message/signature pair* (m, σ) *where* $\mathsf{Verify}(m, \sigma, pk)$ *and* $\mathsf{Verify}(m, \sigma, pk')$ *each return* $1 (= \mathsf{valid})$*. A digital signature scheme is key substitution secure if it is secure against key substitution attacks.*

Since the potential attacker for the non-repudiation of a signature scheme is the original signer, one can assume that the key substitution attacker for the non-repudiation of a signature knows the private key of the original signature and the private information, such as nonce, used during signing process. And this contrasts the potential attackers against the unforgeability of a signature scheme.

3 Results

3.1 GPS Signature Scheme

This section recalls a signature scheme in [12], which we call it as GPS signature. Let p be a large isogeny smooth prime, that is, $p = \ell_1^{e_1}\ell_2^{e_2} \cdot f \pm 1$, where ℓ_1, ℓ_2 are small primes (typically $\ell_1 = 2$ and $\ell_2 = 3$). We define a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$ with $|E_0(\mathbb{F}_{p^2})| = \ell_1^{e_1}\ell_2^{e_2} \cdot f$ and a primitive $\ell_1^{e_1}$-torsion point $P_1 \in E_0$. Define $E_1 = E_0/\langle P_1 \rangle$ and denote the corresponding $\ell_1^{e_1}$-isogeny by $\phi : E_0 \to E_1$. In [12], Galbraith, Petit and Silva apply the Fiat-Shamir transform [2] to the De Feo-Jao-Plût identification scheme, and construct GPS signature which is described as follows.

$\mathsf{KeyGen}(1^\lambda)$: On input a security parameter λ, the algorithm proceeds the following steps:

- generate a prime $p = \ell_A^{e_1}\ell_B^{e_2} \cdot f \pm 1$ with at least 4λ bits for small $\ell_1,\ \ell_2,\ f$ (ideally $f = 1, \ell_1 = 2, \ell_2 = 3$) and $\ell_1^{e_1} \approx \ell_2^{e_2}$.
- choose a supersingular elliptic curve E_0 with j-invariant j_0.
- compute points $R_2, S_2 \in E_0(\mathbb{F}_{p^2})[\ell_2^{e_2}]$ and a random primitive $\ell_1^{e_1}$-torsion point $P_1 \in E_0[\ell_1^{e_1}]$.
- compute an isogeny $\phi : E_0 \to E_1$ with kernel generated by P_1, and let j_1 be the j-invariant of the image curve.
- set $R_2^{'} = \phi(R_2), S_2^{'} = \phi(S_2)$.
- choose a hash function H with $t = t(\lambda)$ bits of output.
- output

$$pk = (p, j_0, j_1, R_2, S_2, R_2^{'}, S_2^{'}, H),\ sk = P_1.$$

$\mathsf{Sign}(sk = P_1, m \in \{0,1\}^*)$: On the given input, the algorithm proceeds the following steps:

- for $i = 1, \ldots, t$,
  - choose random integers $0 \le \alpha_i < \ell_2^{e_2}$.
  - compute an isogeny $\psi_i : E_0 \to E_{2,i}$ with the kernel generated by $R_2 + [\alpha_i]S_2$ and let $j_{2,i} = j(E_{2,i})$.
  - compute an isogeny $\psi_i^{'} : E_1 \to E_{3,i}$ with the kernel generated by $R_2^{'} + [\alpha_i]S_2^{'}$ and let $j_{3,i} = j(E_{3,i})$.
  - compute

$$h = H(m, j_{2,1}, \ldots, j_{2,t}, j_{3,1}, \ldots, j_{3,t}) = b_1 b_2 \cdots b_t \in \{0,1\}^t.$$

- for $i = 1, \ldots, t$,
  - if $b_i = 0$ then set $z_i = \alpha_i$.
  - if $b_i = 1$ then compute $\psi_i(P_1)$ and set $z_i = (j_{2,i}, \psi_i'')$ where $\psi_i'' : E_{2,i} \to E_{3,i}'$ is an isogeny with the kernel generated by $\psi_i(P_1)$.
- output

$$\sigma_m = (h = b_1 b_2 \cdots b_t, z_1, \ldots, z_t)$$

$\mathsf{Verify}(m, \sigma_m, pk)$: On the given input,

- from pk, recover the parameters p, E_0, E_1.
- for each $1 \le i \le t$, using the information provided by z_i, one recompute the j-invariants $j_{2,i}'$ and $j_{3,i}'$.
  - in the case $b_i = 0$ this is done by using $z_i = \alpha_i$ and computing $j_{2,i}'$ from the isogeny with kernel generated by $R_2 + [\alpha_i]S_2 \in E_0$ and $j_{3,i}'$ from the isogeny with the kernel generated by $R_2^{'} + [\alpha_i]S_2^{'} \in E_1$.
  - when $b_i = 1$ then the value $j_{2,i}$ and a description of the isogeny $\psi_i'' : E_{2,i} \to E_{3,i}'$ is provided in z_i. The verifier computes $j_{2,i}' = j_{2,i}$ and $j_{3,i}'$ as the j-invariant of the image curve of ψ_i'' which means that $j_{3,i}' = j(E_{2,i}/Ker(\psi_i'')) = j(E_{3,i}')$.
- compute $h^{'} = H(m, j_{2,1}', \ldots, j_{2,t}', j_{3,1}', \ldots, j_{3,t}')$.
- output $1(= \mathsf{valid})$ if and only if $h^{'} = h$.

Theorem 3.1 ([12]). *If the problems CSSI (Computational Supersingular Isogeny) and DSSP (Decisional Supersingular Product) are computationally hard then the signature above, GPS signature, is secure in the random oracle model under a chosen message attack.*

3.2 Our Attack on the Non-repudiation of GPS Signature

Now we show that GPS signature fails to provide non-repudiation of the signature. In particular, we present a key substitution attack on GPS signature for a signer to repudiate his/her signature. We describe our attack in general and present an example.

3.2.1 A Description of Our Key Substitution Attack

Our attack uses isomorphism of elliptic curves. A legal but malicious user U creates two public keys

$$pk = (p, j_0, j_1, R_2, S_2, R_2^{'}, S_2^{'}, H), \quad \text{and } pk' = (p, j_0, j_1, \widetilde{R_2}, \widetilde{S_2}, \widetilde{R_2}^{'}, \widetilde{S_2}^{'}, H) \qquad (1)$$

- $\eta_0(\widetilde{P_1}) = P_1, \eta_0(\widetilde{R_2}) = R_2, \eta_0(\widetilde{S_2}) = S_2$ and
- $\eta_1^{-1} \cdot \phi \cdot \eta_0(\widetilde{R_2}) = \widetilde{R_2}^{'}, \eta_1^{-1} \cdot \phi \cdot \eta_0(\widetilde{S_2}) = \widetilde{S_2}^{'}$

for some isomorphisms $\eta_0 : E_0' \to E_0$ and $\eta_1 : E_1' \to E_1$ with the inverses $\eta_0^{-1} : E_0 \to E_0'$ and $\eta_1^{-1} : E_1 \to E_1'$, respectively.

The public key pk' is correctly formulated by using the isogeny $\eta_1^{-1} \cdot \phi \cdot \eta_0 : E_0^{'} \to E_1^{'}$ with kernel generated by $\widetilde{P_1}$. We set $\widetilde{\phi} = \eta_1^{-1} \cdot \phi \cdot \eta_0$.

The following commutative diagram explains the relations between pk and pk'.

$$\begin{tikzcd}
E_0' \arrow[r, "\widetilde{\phi} = \eta_1^{-1} \cdot \phi \cdot \eta_0"] \arrow[d, "\eta_0"'] & E_1' \arrow[d, "\eta_1"] \\
E_0 \arrow[r, "\phi"] \arrow[d, "\psi_i"'] & E_1 \arrow[d, "\psi_i'"] \\
E_{2,i} \arrow[r, "\psi_i''"] & E_{3,i}
\end{tikzcd}$$

Now we prove that the user with the public key $pk^{'}$ succeed a key substitution attack on GPS signature scheme.

Theorem 3.2. *Let the public keys* $pk = (p, j_0, j_1, R_2, S_2, R_2^{'}, S_2^{'}, H)$ *and* $pk' = (p, j_0, j_1, \widetilde{R_2}, \widetilde{S_2}, \widetilde{R_2}^{'}, \widetilde{S_2}^{'}, H)$ *of GPS signature be given as in Eq. 1. For any valid signature* $\sigma_m = (h = b_1 b_2 \cdots b_t, z_1, \ldots, z_t)$ *on a message* $m \in \{0,1\}^*$ *under the public key* pk*,* σ_m *is a valid signature on the message* $m \in \{0,1\}^*$ *under the public key* pk'*.*

Proof. From the validity of $\sigma_m = (h = b_1 b_2 \cdots b_t, z_1, \ldots, z_t)$ as a signature on the message $m \in \{0,1\}^*$ under the public key pk, the followings hold,

- for the $i = 1, ..., t$ with $b_i = 0$, which implies that $z_i = \alpha_i$,
  - $j_{2,i} = j(E_0/\langle R_2 + [\alpha_i]S_2\rangle)$ and $j_{3,i} = j(E_0/\langle R'_2 + [\alpha_i]S'_2\rangle)$.
- for the $i = 1, ..., t$ with $b_i = 1$, which implies that $z_i = (j_{2,i}, \psi^{''}_i : E_{2,i} \to E'_{3,i})$, $j_{3,i} = j(E_{2,i}/\langle Ker(\psi^{''}_i)\rangle) = j(E'_{3,i})$.
- $h = b_1 b_2 \cdots b_t = H(m, j_{2,1}, \ldots, j_{2,t}, j_{3,1}, \ldots, j_{3,t})$.

Now we show that σ_m is also a valid signature on m under pk'. From (m, σ_m), anyone can verify the validity of σ_m as a signature on m under pk' as follows:

- If $b_i = 0$, that is, $z_i = \alpha_i$, any verifier computes $(j^{'}_{2,i}, j^{'}_{3,i})$ as follows by using pk' which turns out $(j^{'}_{2,i}, j^{'}_{3,i}) = (j_{2,i}, j_{3,i})$:
  - The verifier computes $j'_{2,i} = j(E'_0/\langle \widetilde{R_2} + [\alpha_i]\widetilde{S_2}\rangle)$ from an isogeny $\widetilde{\psi}_i : E'_0 \to E'_{2,i}$ whose kernel is generated by $\widetilde{R_2} + [\alpha_i]\widetilde{S_2}$. We want to show that $j'_{2,i} = j_{2,i}$. Since $\eta_0 : E_0 \to E'_0$ is an isomorphism, we have

    $$j'_{2,i} = j(E'_0/\langle Ker(\widetilde{\psi}_i)\rangle) = j(E_0/\langle Ker(\widetilde{\psi}_i \cdot \eta_0^{-1})\rangle).$$

    We also have that $Ker(\widetilde{\psi}_i \cdot \eta_0^{-1}) = \langle R_2 + [\alpha_i]S_2\rangle$ from the fact

    $$\eta_0^{-1}(R_2 + [\alpha_i]S_2) = \eta_0^{-1}(R_2) + [\alpha_i]\eta_0^{-1}(S_2) = \widetilde{R_2} + [\alpha_i]\widetilde{S_2}.$$

    Therefore, $j'_{2,i} = j(E_0/Ker(\widetilde{\psi}_i \cdot \eta_0^{-1})) = j(E_0/\langle R_2 + [\alpha_i]S_2\rangle) = j_{2,i}$
  - The verifier computes $j'_{3,i} = j(E'_1/\langle \widetilde{R_2}' + [\alpha_i]\widetilde{S_2}'\rangle)$ from an isogeny $\widetilde{\psi}_i{}' : E'_1 \to E'_{3,i}$ whose kernel is generated by $\widetilde{R_2}' + [\alpha_i]\widetilde{S_2}'$. We want to show that $j'_{3,i} = j_{3,i}$. Since $\eta_1 : E_1 \to E'_1$ is an isomorphism, we have

    $$j'_{3,i} = j(E'_1/\langle Ker(\widetilde{\psi}_i{}')\rangle) = j(E_1/\langle Ker(\widetilde{\psi}_i{}' \cdot \eta_1^{-1})\rangle).$$

    We also have that $Ker(\widetilde{\psi}_i \cdot \eta_1^{-1}) = \langle R'_2 + [\alpha_i]S'_2\rangle$ from the fact

    $$\eta_1^{-1}(R'_2 + [\alpha_i]S'_2) = \eta_1^{-1}(R'_2) + [\alpha_i]\eta_1^{-1}(S'_2) = \widetilde{R_2}' + [\alpha_i]\widetilde{S_2}'.$$

    Therefore, $j'_{3,i} = j(E_1/\langle Ker(\widetilde{\psi}_i{}' \cdot \eta_1^{-1})\rangle) = j(E_1/\langle R'_2 + [\alpha_i]S'_2\rangle) = j_{3,i}$.
- If $b_i = 1$, that is, $z_i = (j_{2,i}, \psi^{''}_i : E_{2,i} \to E'_{3,i})$, then any verifier computes $j^{'}_{3,i}$ as follows

  $$j'_{3,i} = j(E_{2,i}/\langle Ker(\psi^{''}_i)\rangle) = j_{3,i}.$$

- Since the verifier computes $(j^{'}_{2,i}, j^{'}_{3,i})$ such that $(j^{'}_{2,i}, j^{'}_{3,i}) = (j_{2,i}, j_{3,i})$ for all i, it is clear to see that

  $$H(m, j'_{2,1}, \ldots, j'_{2,t}, j'_{3,1}, \ldots, j'_{3,t}) = H(m, j_{2,1}, \ldots, j_{2,t}, j_{3,1}, \ldots, j_{3,t}) = h.$$

Therefore, $\sigma_m = (h, z_1, \ldots, z_t)$ is a valid signature on $m \in \{0,1\}^*$ under the public key $pk' = (p, j_0, j_1, \widetilde{R_2}, \widetilde{S_2}, \widetilde{R_2}', \widetilde{S_2}', H)$. □

Theorem 3.2 implies that the signer U whose public key is pk can repudiate his/her signing of σ_m on m whenever he/she wants by submitting pk' as another public key that validates the signature σ_m on m. Moreover, we note that the public key pk' can be computed independently to any valid pair $(message, signature)$ under pk, the owner U of pk can register pk' as another legal user in the system a priori to prepare his/her future malicious actions. This concludes that GPS signature scheme does not provide the non-repudiation property.

Remark 3.3. *Unruh* [5] *has given a transform that converts a secure interactive identification scheme into a signature scheme that is secure against a quantum adversary. In* [12] *the authors presented a post-quantum version of GPS signature using the Unruh transform and prove that it is existentially unforgeable in the quantum random oracle model if CSSI and DSSP are computationally hard for a quantum computer. It is easy to see that our key substitution attack on the (classic) GPS signature scheme works exactly the same for the post-quantum version of GPS signature scheme, too. Therefore, we see that the post-quantum version of GPS signature scheme does not provide the non-repudiation property, too.*

3.2.2 An Example

In this section, we present a simple example of our key substitution attack on GPS signature for a clear view of isogenies and our attack. We compute our example using Sage with a small prime p for simplicity. We also use the hash function $MD5$ in our example, but our attack succeeds independently the underlying hash function.

(A Valid Key Generation)

- $p = 2^4 \cdot 3^3 \cdot 2 - 1 = 863$;
- $E_0 : y^2 = x^3 + x$, an elliptic curve over a finite field $\mathbb{F}_{p^2}$;
- a is generator of finite field $\mathbb{F}_{p^2}$;
- Choose points $P_1, R_2, S_2 \in E_0$ as follows:

$$P_1 = (197a + 648 : 758a + 405 : 1),$$
$$R_2 = (422a + 27 : 548a + 682 : 1),\ S_2 = (164a + 7 : 478a + 586 : 1)$$

- Compute an isogeny $\phi : E_0 \to E_1$ of degree 16 with the kernel $\langle P_1 \rangle$ where $E_1 : y^2 = x^3 + (155a + 756)x + (18a + 470)$ and the isogeny ϕ is defined as follows:

$$\begin{aligned}
\phi &= (\frac{q_1(x)}{q_2(x)}, \frac{r_1(x,y)}{r_2(x)}) \\
q_1(x) &= x^{16} + (-36a - 343)x^{15} + (169a + 373)x^{14} + (312a + 388)x^{13} \\
&\quad + (284a + 400)x^{12} + (-398a + 78)x^{11} + (330a - 125)x^{10}(-41a - 139)x^9 \\
&\quad + (-295a - 193)x^8 + (249a - 353)x^7 + (-321a - 224)x^6 + (-199a + 165)x^5 \\
&\quad + (-182a + 265)x^4 + (352a + 127)x^3 + (-31a + 257)x^2 + (-239a + 77)x \\
&\quad + (174a + 150) \\
q_2(x) &= x^{15} + (-36a - 343)x^{14} + (200a - 339)x^{13} + (143a + 351)x^{12} \\
&\quad + (-65a - 311)x^{11} + (195a - 81)x^{10} + (23a + 395)x^9 + (-25a + 252)x^8 \\
&\quad + (340a - 422)x^7 + (329a - 325)x^6 + (-24a + 201)x^5 + 307a - 158)x^4 \\
&\quad + (242a - 368)x^3 + (-118a - 163)x^2 + (147a - 20)x + (48a + 133) \\
r_1(x,y) &= x^{23}y + (-286a + 33)x^{22}y + (215a + 131)x^{21}y + (203a - 75)x^{20}y \\
&\quad + (202a - 238)x^{19}y + (203a + 273)x^{18}y + (-348a - 351)x^{17}y \\
&\quad + (-31a - 269)x^{16}y + (412a + 373)x^{15}y + (117a + 414)x^{14}y \\
&\quad + (204a + 157)x^{13}y + (-203a - 363)x^{12}y + (290a - 250)x^{11}y \\
&\quad + (-59a - 49)x^{10}y + (-189a + 349)x^9y + (-391a - 360)x^8y \\
&\quad + (385a - 231)x^7y + (328a - 189)x^6y + (-142a - 283)x^5y \\
&\quad + (76a + 398)x^4y + (-303a + 129)x^3y + (352a + 62)x^2y \\
&\quad + (-16a - 397)xy + (366a + 237)y \\
r_2(x) &= x^{23} + (-286a + 33)x^{22} + (184a - 20)x^{21} + (-60a - 208)x^{20} \\
&\quad + (-235a + 431)x^{19} + (428a - 178)x^{18} + (-a + 378)x^{17} + (327a + 338)x^{16} \\
&\quad + (-27a - 356)x^{15} + (77a + 351)x^{14} + (-385a - 137)x^{13} + (425a - 63)x^{12} \\
&\quad + (226a + 372)x^{11} + (95a + 156)x^{10} + (118a - 425)x^9 + (-128a + 248)x^8 \\
&\quad + (344a + 299)x^7 + (310a - 417)x^6 + (184a + 337)x^5 + (371a - 154)x^4 \\
&\quad + (-105a + 307)x^3 + (11a + 243)x^2 + (79a + 327)x + (409a - 149)
\end{aligned}$$

- Compute j-invariants $j_0 = j(E_0) = 2$, $j_1 = j(E_1) = 465a + 831$.
- Compute $R_2', S_2' \in E_1$ as follows:

$$\begin{aligned}
R_2^{'} &= \phi(R_2) = (347a + 480 : 357a + 737 : 1), \\
S_2^{'} &= \phi(S_2) = (712a + 662 : 268a + 204 : 1)
\end{aligned}$$

- Hash function $H = MD5 : \{0,1\}^* \to \{0,1\}^{128}$
- Output

$$pk = (p, j_0, j_1, R_2, S_2, R_2^{'}, S_2^{'}, H),\ sk = P_1.$$

(A Key Generation for Key Substitution Attack)

- For the given E_0 from the valid key generation, compute an isomorphism $\zeta_0 : E_0 \to E_0^{'}$ defined by $\zeta_0(x,y) = (557x, (842a+442)y)$ for the elliptic curve $E_0' : y^2 = x^3 + 2x$. Compute $\eta_0 = \zeta_0^{-1} : E_0' \to E_0$, then $\eta_0^{-1} = \zeta_0$. Note that $\eta_0(x,y) = (251x, (677a + 93)y)$ and $j(E_0') = j(E_0) = j_0$.
- For the given E_1 from the valid key generation, compute an isomorphism $\zeta_1 : E_1 \to E_1^{'}$ defined by $\zeta_1(x,y) = (406x, (385a + 239)y)$ for $E_1^{'} : y^2 = x^3 + (465a + 542)x + (349a + 291)$. Compute $\eta_1 = \zeta_1^{-1} : E_1' \to E_1$, then $\eta_1^{-1} = \zeta_1$. Note that $\eta_1(x,y) = (423x, (779a + 42)y)$ and $j(E_1') = j(E_1) = j_1$.

- Compute
  - $\widetilde{P_1} = \eta_0^{-1}(P_1) = (256a + 404 : 23a + 425 : 1)$
  - $\widetilde{S_2} = \eta_0^{-1}(S_2) = (603a + 31 : 164a + 224 : 1)$
  - $\widetilde{R_2} = \eta_0^{-1}(R_2) = (636a + 736 : 825a + 34 : 1)$
- Compute the isogeny $\widetilde{\phi} = \eta_1^{-1} \cdot \phi \cdot \eta_0 : E_0' \to E_1'$. Note that the kernel of $\widetilde{\phi}$ is $\langle \widetilde{P_1} \rangle$. Set
  - $\widetilde{S_2}' = \widetilde{\phi}(\widetilde{S_2}) = (830a + 379 : 680a + 602 : 1)$
  - $\widetilde{R_2}' = \widetilde{\phi}(\widetilde{R_2}) = (213a + 705 : 795a + 677 : 1)$
- Output

$$pk' = (p, j_0, j_1, \widetilde{R_2}, \widetilde{S_2}, \widetilde{R_2}', \widetilde{S_2}', H),\ sk = \widetilde{P_1}$$

(A Signature Generation using sk on a message $m = message$)

A signature σ_m on the message $m = \mathsf{message}$ is computed as follows: First we compute the first part h of the signature as follows: For a randomly chosen $[\alpha_i]_{1 \le i \le t} = [15, 5, 6, 18, 2, \ldots]$, compute the following isogenies and j-invariants for each i:

- $\psi_i : E_0 \to E_{2,i}$ with the kernel $\langle R_2 + [\alpha_i]S_2 \rangle$ and $j_{2,i} = j(E_0/\langle R_2 + [\alpha_i]S_2 \rangle)$:

$$j_2 = [j_{2,1}, j_{2,2}, j_{2,3}, j_{2,4}, \ldots] = [515a + 716, 473a + 144, 473a + 144, 451a + 551, \ldots]$$

- $\psi_i' : E_1 \to E_{3,i}$ with the kernel $\langle R_2' + [\alpha_i]S_2' \rangle$ and $j_{3,i} = j(E_1/\langle R_2' + [\alpha_i]S_2' \rangle)$:

$$j_3 = [j_{3,1}, j_{3,2}, j_{3,3}, j_{3,4} \ldots] = [232a+541, 657a+665, 657a+665, 590a+114 \ldots]$$

For the two sequences j_2 and j_3 of j-invariants, compute the hash value

$$h = b_1 b_2 b_3 \cdots = H(\mathsf{message}, j_2, j_3) = 10111011 \ldots.$$

Now we compute the second part (z_i's) of the signature as follows:

- From the fact $b_1 = 1$, set $z_1 = (j_{2,1} = 515a + 716, \psi_1'')$, where
  - $\psi_1'' : E_{2,1} \to E_{3,1}'$ is an isogeny with the kernel generated by $\psi_1(P_1)$ for the elliptic curves $E_{2,1} : y^2 = x^3 + (285a + 129)x + (507a + 262)$ and $E_{3,1}' : y^2 = x^3 + (713a + 733)x + (70a + 235)$.
- $b_2 = 0$, and set $z_2 = \alpha_2 = 5$.

$$\vdots$$

Finally, we have a sequence $z = [z_1, z_2, z_3 \ldots] = [(515a + 716, \psi_1''), 5, (473a + 144, \psi_3''), \ldots]$, and the computed signature is $\sigma = ((h, z), \mathsf{message})$. This signature $\sigma_m = ((h, z), \mathsf{message})$ can be verified as a valid signature on $\mathsf{message}$ under the public key pk.

(Key Substitution Attack on σ_m using the public key pk')

Note that $pk' = (p, j_0, j_1, \widetilde{R_2}, \widetilde{S_2}, \widetilde{R_2}', \widetilde{S_2}', H)$. Suppose that a valid signature $\sigma = ((h, z), \mathsf{message})$ under pk is given as follows:

- $h = H(\mathsf{message}, j_2, j_3) = 10111011\cdots$
- $z = [z_1, z_2, z_3, \ldots] = [(515a + 716, \psi_1^{''}), 5, (473a + 144, \psi_3^{''}), \ldots] = [(j_{2,1}, \psi_1^{''} : E_{2,1} \rightarrow E_{3,1}'), \alpha_2, (j_{2,3}, \psi_3^{''} : E_{2,3} \rightarrow E_{3,3}'), \ldots]$

For the verification, anyone compute the values of j-invariants ($j_2' = [j_{2,1}', j_{2,2}', \ldots], j_3' = [j_{3,1}', j_{3,2}', \ldots]$) for the pk' as follows:

From $b_1 = 1$ and $z_1 = (j_{2,1}, \psi_1^{''}) = (515a + 716, \psi_1^{''} : E_{2,1} \rightarrow E_{3,1}')$:

- set $j_{2,1}' = j_{2,1}$ and
- compute the j-invariant $j_{3,1}' = j(E_{3,1}') = 232a + 541$, which turns out $j_{3,1}' = j_{3,1}$.

From $b_2 = 0$, that is, $z_2 = \alpha_2 = 5$:

- The verifier computes an isogeny $\widetilde{\psi_2} : E_0' \longrightarrow E_{2,2}'$ with the kernel $\widetilde{R_2} + 5\widetilde{S_2}$ and the j-invariant $j_{2,2}' = j(E_0'/\langle \widetilde{R_2} + 5\widetilde{S_2} \rangle) = 473a + 144$, which turns out $j_{2,2}' = j_{2,2}$.
- The verifier computes an isogeny $\widetilde{\psi_2'} : E_1' \longrightarrow E_{3,2}'$ with the kernel $\widetilde{R_2}' + 5\widetilde{S_2}'$ and the j-invariant $j_{3,2}' = j(E_1'/\langle \widetilde{R_2}' + 5\widetilde{S_2}' \rangle) = 657a + 665$, which turns out $j_{3,2}' = j_{3,2}$.

Similarly, the values of j-invariants j_2', j_3' for the pk' such that $j_2 = j_2^{'}, j_3 = j_3^{'}$ are computed. Clearly, $h = H(\mathsf{message}, j_2, j_3) = H(\mathsf{message}, j_2', j_3')$, therefore, the signature $\sigma = ((h, z), \mathsf{message})$ is valid under pk'.

3.3 How to Prevent Our Attack

Our attack on GPS signature uses isomorphisms of the underlying elliptic curves and isomorphic elliptic curves have the same j-invariants. Therefore, if one restricts distinct j-invariants (j_0, j_1) for each public key, our key substitution attack can be prevented. However, our result is the first key substitution attack on isogeny based signature schemes under the consideration of the non-repudiation of the signature and one could expect a more advanced key substitution attack on isogeny based signature.

In general, there are two ways to prevent key substitution attacks on digital signature schemes. One is that the certificate authority (CA) for public keys requires that users to prove possession of user's private key before issuing certificates. This prevents the adversary mounts key substitution attacks without knowing the corresponding private key. However, this counter-measure is not suitable to prevent key substitution attack under consideration of non-repudiation, since the original signer is considered as a potential attacker and the original signer knows the related private keys. Another way to prevent key substitution attack is proposed by Menezes and Smart. They formalize the key substitution security as a security of signature schemes in multi-user setting and formatting messages specific to each public key, such as including the signer's public key to the message in some unambiguous way prior to signing (e.g., $pk||message$) guarantees the key substitution security if the original signature scheme is proven unforgeable [1].

4 Conclusion

GPS signature [12] is an efficient isogeny based signature scheme which is proven EUF-CMA secure in the random oracle model under the assumption that the problems CSSI (Computational Supersingular Isogeny) and DSSP(Decisional Supersingular Product) are infeasible. In this paper, we show that the current version of GPS signature fails to provided non-repudiation by presenting a public key substitution attack on GPS signature. In [12], they also presented a post-quantum version of GPS signature which is proven EUF-CMA secure in the quantum random oracle model based on the hardness of CSSI and DSSP. It is easy to see that our key substitution attack on the (classic) GPS signature scheme works exactly the same against the post-quantum version of GPS signature scheme, too. We recommend to use distinct j-invariants (j_0, j_1) for each public key of GPS signature scheme to prevent our key substitution attack. Moreover, we suggest to format messages as specific to each public key, such as $pk||message$, prior to signing according to the analysis of Menezes and Smart [1].

References

1. Alfred, M., Nigel, S.: Security of signature schemes in a multiuser setting. Des. Codes Cryptogr. **23**, 261–274 (2004)
2. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12
3. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.-Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 19–34. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25405-5_2
4. Jao, D., Soukharev, V.: Isogeny-based quantum-resistant undeniable signatures. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 160–179. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11659-4_10
5. Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 755–784. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_25
6. Jens-Matthias, B., Stefan, R., Rainer, S.: Key substitution attacks revisited: taking into account malicious signers. Int. J. Inf. Secur. **5**, 30–36 (2006)
7. John, T.: Endomorphisms of abelian varieties over finite fields. Inven. Math **2**, 134–144 (1966)
8. Joseph, H.S.: The Arithmetic Elliptic Curves. Graduate Texts in Mathematics. Springer, New York (2009). ISBN 9780387962030
9. Lawrence, C.W.: Elliptic Curves: Number Theory and Cryptography, 2nd edn. CRC Press, London (2008). ISBN 978-1420071467
10. De Feo, L., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Math. Cryptol. **8**, 209–247 (2014)
11. Robin, H.: Algebraic Geometry. Graduate Texts in Mathematics, vol. 52. Springer, New York (1977). https://doi.org/10.1007/978-1-4757-3849-0

12. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10624, pp. 3–33. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70694-8_1
13. Velu, J.: Isogenies Entre Courbes Elliptiques. Communications de Academie royale des Sciences de Paris, pp. 305–347 (1971)
14. William, C.W.: Abelian varieties over finite fields. Annales scientifiques de l'$\acute{E}$.N.S., pp. 521–560 (1969)
15. Xi, S., Haibo, T., Wang, Y.: Toward quantum-resistant strong designated verifier signature from isogenies. Int. J. Grid Util. Comput. **5**, 80–86 (2014)