UFR IM^{2}AG
Université Joseph Fourier – Institut National Polytechnique

Master SCCI – Research

AC Final Exam – January 23, 2013

Exercise

1. Let E be an elliptic curve defined over $\mathbb{F}_q$ such that the Frobenius map $\Phi_q \in End(E)$ has a trace equal to zero, and let N be a positive integer.
   (a) Show that if there exists a point P in $E(\mathbb{F}_q)$ of order N, then all the N-torsion $E[N]$ is included in $E(\mathbb{F}_{q^2})$ (indication: consider the action of Φ_q^2 over $E[N]$).
   (b) What can you say about the security of the discrete logarithm problem over $E(\mathbb{F}_q)$?
2. Let E be an elliptic curve defined over $\mathbb{F}_2$ by $y^2 + y = x^3 + x$.
   (a) Show that this curve is supersingular by computing its cardinality $E(\mathbb{F}_2)$.
   (b) Give the characteristic polynomial of the Frobenius $\Phi_2 \in End(E)$. Deduce that $\Phi_2^4 = [-4]$.
   (c) Compute the cardinalities $\#E(\mathbb{F}_4)$ and $\#E(\mathbb{F}_{16})$. Does the result of 1.(a) still hold in this case?

Problem

The goal of this problem is to study some practical aspects of the implementation of a simplified version of Boneh and Franklin's scheme for identity-based encryption. In this setting, the trusted authority (TA) publishes system parameters $\{E, G_1, G_2, G_3, e, P_0, P_{pub}, n, H_1, H_3, N\}$ where

- E is an elliptic curve defined over $\mathbb{F}_q$ (of characteristic different from 2 and 3) with a distinguished point $\mathcal{O}$, with a cardinality divisible by a large prime integer n and a corresponding embedding degree $k > 1$; we suppose moreover that $k \wedge n = 1$ and that $n^3 \nmid \#E(\mathbb{F}_{q^k})$,
- $G_1 = E(\mathbb{F}_q)[n]$, $G_2 = \langle P_0 \rangle \subset E(\mathbb{F}_{q^k})[n]$ where $P_0 \in E(\mathbb{F}_{q^k}) \setminus E(\mathbb{F}_q)$ has order n, and $G_3 = \mu_n$ is the subgroup of $(\mathbb{F}_{q^k})^*$ of the n-th roots of unity,
- $e : G_1 \times G_2 \to G_3$ is a non-degenerate bilinear pairing,
- $P_{pub} = [s]P_0$ where s is the private master key,
- $H_1 : \{0;1\}^* \to G_1$ is a hash function from the set of binary strings to G_1 and $H_3 : G_3 \to \{0;1\}^N$ is a hash function from G_3 to the set of messages of size N.

To encrypt a message m of size N addressed to Alice, Bob needs to

a) obtain the public key of Alice by computing the hash value of her identity $H(id_A)$;

b) choose a random integer $r \in_R \{1; \ldots; n-1\}$;

c) compute the ciphertext $(C_1, C_2) = \big([r]P_0, m \oplus H_3(e(H_1(id_A), [r]P_{pub}))\big)$ and send it to Alice.

To decrypt (C_1, C_2), Alice computes $C_2 \oplus H_3(e(S_{id_A}, C_1))$ where $S_{id_A} = [s]H(id_A)$ is the private key she obtained from the TA.

Questions

0. Check that the scheme is correct, i.e. that Alice indeed recovers the plaintext.

1. We first consider the special case (proposed by Boneh and Franklin in their original paper) where E is given by a Weierstrass equation of the form $y^2 = x^3 + b$ with $b \in \mathbb{F}_q$ and $q = 2 \bmod 3$.

   (a) Explain why it is possible to consider in this context a "symmetric" pairing
   $$e : G_1 \times G_1 \to G_3.$$
   Indication: compute the cardinality of $E(\mathbb{F}_q)$ by showing that the cube map $x \mapsto x^3$ is a bijection over $\mathbb{F}_q$ and prove that E is supersingular.

   (b) Given a cryptographic hash function $h : \{0;1\}^* \to \{0; \ldots; q-1\}$, construct an explicit hash function H that sends any string of $\{0;1\}^*$ to a point in G_1.

In the following questions, $E : y^2 = x^3 + ax + b$ is supposed to be a pairing-friendly ordinary curve defined over $\mathbb{F}_q$ with $j(E) \neq 0, 1728$.

2. We propose the following construction for the hash function H.
   Let $Q \in E(\mathbb{F}_q)[n]$ a point of order n, i.e. such that $G_1 = \langle Q \rangle$, and let $h : \{0;1\}^* \to \{1; \ldots; n-1\}$ be any cryptographic hash function; we define the hash value of an identity *id* by $H(id) = [h(id)]Q$.
   Suppose that Eve has already asked her private key $S_{id_E} = [s]H(id_E)$ to the TA. Then, show that she is able to compute the private key of any user.

3. We propose in this question a point compression technique using the trace zero subgroup and quadratic twists.

   Let $\Phi_q \in End(E(\mathbb{F}_{q^k}))$ be the Frobenius map. The *trace map* (relative to the extension $\mathbb{F}_{q^k}/\mathbb{F}_q$) is the group morphism defined as:
   $$\begin{array}{rcl} \mathrm{tr} : E(\mathbb{F}_{q^k}) & \to & E(\mathbb{F}_q) \\ P & \mapsto & \sum_{i=0}^{k-1} \Phi_{q^i}(P) \end{array}$$

   (a) Check that the image of tr is indeed a subset of $E(\mathbb{F}_q)$ and that its restriction to the n-torsion $\mathrm{tr}_{|E(\mathbb{F}_{q^k})[n]} : E(\mathbb{F}_{q^k})[n] \to E(\mathbb{F}_q)[n]$ is well-defined.

   (b) Show that the kernel of the restricted trace map $\mathrm{tr}_{|E(\mathbb{F}_{q^k})[n]}$ is a group of order n different from G_1, called the trace zero subgroup. In particular, show that the Weil and Tate pairings from $G_1 \times G_2$ to G_3 are non degenerate when G_2 is equal to this trace zero subgroup.

   We suppose in what follows that k is even and we denote by E' the quadratic twist of E defined over $\mathbb{F}_{q^{k/2}}$, i.e. E' is such that there exists an isomorphism $\varphi : E' \to E$ defined over $\mathbb{F}_{q^k}$ but there is no isomorphism between E' and E defined over $\mathbb{F}_{q^{k/2}}$.

(c) Let t_i be the trace of the i-th Frobenius $\Phi_{q^i} = \Phi_q^i$. Show that $t_k = t_{k/2}t_{k/2} - 2q^{k/2}$ and that $\#E(\mathbb{F}_{q^k}) = \#E(\mathbb{F}_{q^{k/2}}) \times \#E'(\mathbb{F}_{q^{k/2}})$. Deduce that $E'(\mathbb{F}_{q^{k/2}})[n] \simeq \mathbb{Z}/n\mathbb{Z}$.

(d) Let $u \in \mathbb{F}_{q^{k/2}}$ be a non quadratic residue and let $v \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/2}}$ be a square root of u. Give a Weierstrass equation of the twist E' and the expression of the isomorphism φ in terms of a, b and v.

(e) Prove that $\Phi_{q^{k/2}}(\varphi(P)) = -\varphi(P)$ for any point $P \in E'(\mathbb{F}_{q^{k/2}})$. Deduce that $\varphi(E'(\mathbb{F}_{q^{k/2}})[n]) = \ker(\mathrm{tr}_{|E(\mathbb{F}_{q^k})[n]})$.

(f) Explain how this last result allows to reduce by 2 the size of the representations of elements of G_2.

4. The aim of this last question is to device a fault attack against the simplified Boneh-Franklin IBE scheme when we take for e the Weil pairing

$$\begin{array}{rcl} w_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_{q^k})[n] & \to & \mu_n \subset (\mathbb{F}_{q^k})^* \\ (P, Q) & \mapsto & w_n(P, Q) = (-1)^n \frac{f_P(Q)}{f_Q(P)}, \end{array}$$

where $f_P(Q)$ (resp. $f_Q(P)$) is computed with the following algorithm:

Algorithm 1: Miller's algorithm

```
Input  : $E$, $n = (n_l ... n_0)_2 \in \mathbb{N}^*$, $P \in E[n]$, $Q \in E$
Output: $f_P(Q)$ where $\mathrm{div} f_P = n(P) - n(O)$
$T \leftarrow P$, $f \leftarrow 1$
for $k = l - 1$ down to $0$ do
    $\ell \leftarrow$ tangent at $T$;   $v \leftarrow$ vertical line at $[2]T$;   $T \leftarrow [2]T$;   $f \leftarrow f^2 \ell(Q)/v(Q)$
    if $n_k = 1$ then
        $\ell \leftarrow$ line through $T$ and $P$;   $v \leftarrow$ vertical line at $T + P$;   $T \leftarrow T + P$;   $f \leftarrow f\ell(Q)/v(Q)$
return $f$
```

We suppose that the decryption is done on a smart card. We will assume that the attacker is able to inject a fault during the computation of the pairing $w(S_{id}, C_1)$, so that the final step in the loop of Miller's algorithm is not performed. We will also assume that the attacker is able to extract the value of the pairing during the decryption of a message of its choice.

(a) Let $\tilde{w}(S_{id}, C_1) = -\tilde{f}_{S_{id}}(C_1)/\tilde{f}_{C_1}(S_{id})$ be the result of the faulty pairing computation. Show that

$$w(S_{id}, C_1) = -\frac{\tilde{f}_{S_id}(C_1)^2 \tau_{rS_{id}}(C_1)}{\tilde{f}_{C_1}(S_{id})^2 \tau_{rC_1}(S_{id})}$$

where $\tau_P(x, y) = 0$ is the equation of the tangent of E at the point P and $r = (n-1)/2$.

(b) Show that the attacker can recover $\tau_{rS_{id}}(C_1)/\tau_{rC_1}(S_{id})$. Explain why this information allows to deduce the value of the secret key S_{id}.

(c) Why is this attack no longer possible when the Tate pairing

$$\langle P, Q \rangle_n = f_P(Q)^{\frac{q^k - 1}{n}}$$

is used instead?