CS 259C/Math 250: Elliptic Curves in Cryptography
Homework #4

Due November 30, 2011

Solutions must be handed in in class, handed to Mark (494 Gates), or emailed to Mark (zhandry at cs.stanford.edu) by 4pm on the due date.

Use of SAGE is allowed on any problem. If you use SAGE you must show your work by attaching your computations to the solutions you turn in. Use of LaTeX is encouraged but not required.

1. (8 points) **Multi-user encryption.** In this problem we will convert Joux's three-way key exchange protocol into a "multi-user" encryption scheme.

   Let $E/\mathbb{F}_p$ be a supersingular elliptic curve with $P \in E(\mathbb{F}_p)$ a point of (prime) order n. Let $\mathbb{G} = \langle P \rangle$ and define the modified Weil pairing $\hat{e}\colon \mathbb{G} \times \mathbb{G} \to \mu_n \subset \mathbb{F}_{p^2}^{\times}$ as in class. (In particular, $\hat{e}(P,P)$ is a generator of μ_n.) We assume that $\mathsf{pp} = (E, \hat{e}, P)$ are public parameters known to everyone in the system.

   Suppose Alice and Bob execute their parts of the three-way key exchange protocol. Specifically, Alice chooses $a \stackrel{\text{R}}{\leftarrow} [1,n]$ and publishes $Q_A = [a]P$, while Bob chooses $b \stackrel{\text{R}}{\leftarrow} [1,n]$ and publishes $Q_B = [b]P$.

   (a) Show how a third party can encrypt a message $M \in \mu_n$ to Alice and Bob simultaneously. Specifically, give an encryption algorithm $\mathsf{Enc}(\mathsf{pp}, Q_A, Q_B, M)$ and a decryption algorithm $\mathsf{Dec}(\mathsf{pp}, \mathsf{sk}, C)$ that satisfy the following correctness property

   $$\mathsf{Dec}(\mathsf{pp},\ a,\ \mathsf{Enc}(\mathsf{pp}, Q_A, Q_B, M)) = \mathsf{Dec}(\mathsf{pp},\ b,\ \mathsf{Enc}(\mathsf{pp}, Q_A, Q_B, M)) = M.$$

   (*Hint:* Construct a variant of Boneh-Franklin IBE that doesn't use any hash functions.)

   (b) Prove that if the BDDH assumption holds for $\mathbb{G}$, then the system in (1a) is semantically secure against any attacker not knowing a or b. Specifically, suppose you are given a BDDH challenge P, aP, bP, cP, γ and an adversary $\mathcal{A}$ that can distinguish the encryption of a chosen message M from the encryption of a random message M'. Design an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine and decides whether $\gamma = \hat{e}(P,P)^{abc}$.

   If we had a more powerful map, we could extend this functionality to more than two receivers. Specifically, suppose that we had a nondegenerate, symmetric, ℓ-*linear* map $\tilde{e}\colon \mathbb{G}^\ell \to \mu_n$. In particular, $\tilde{e}$ satisfies

   $$\tilde{e}([c_1]P, \ldots, [c_\ell]P) = \tilde{e}(P, \ldots, P)^{c_1 \cdots c_\ell}.$$

(c) Suppose that ℓ parties each choose some $a_i \xleftarrow{R} [1, n]$ and publish $Q_i = [a_i]P$. Let $M \in \mu_n$ be a message. Generalize your system from above: give Enc and Dec algorithms such that any party can use her secret key and the public information to decrypt the ciphertext. (You do not need to give a security proof.)

(d) (Bonus, 2 points.) Modify the ℓ-party system to allow encrypting to *subsets* of users. Specifically, describe a modified set of public parameters and give an Enc algorithm that takes the public information, a subset $S \subset \{1, \ldots, \ell\}$, and a message M, and outputs a ciphertext C. Give a Dec algorithm that takes the public information and a user's secret key a_i and outputs a message. The correctness condition is that for any $S \subset \{1, \ldots, \ell\}$, if $i \in S$ then

$$\mathsf{Dec}(\mathsf{pp},\ a_i,\ \mathsf{Enc}(\mathsf{pp}, \{Q_i\}, S, M)) = M.$$

You do not need to provide a security proof, but you should make sure there is no obvious way for the users outside of S to combine their secret keys to decrypt the message. (*Hint:* consider adding random points R_i to the public parameters.)

The ℓ-party construction requires an efficiently computable ℓ-linear map between groups where the discrete logarithm problem is hard. Unfortunately, the largest ℓ for which we know how to construct such a map is $\ell = 2$!

2. (6 points) **Signatures from IBE.** Moni Naor observed that any IBE scheme can be converted to a signature scheme: the signature σ on a message m is the IBE secret key corresponding to $\mathsf{id} = m$, and to verify a signature we test whether the given key σ can decrypt the IBE encryption of a random message.

Specifically, suppose that $\mathcal{E} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ is an IBE scheme. We construct a signature scheme $\mathcal{S}$ as follows:

- $\mathsf{Gen}()$: Run the IBE Setup algorithm to obtain public parameters pp and a master key mk. Output $\mathsf{pk}_\mathcal{S} = \mathsf{pp}$ and $\mathsf{sk}_\mathcal{S} = (\mathsf{pp}, \mathsf{mk})$.
- $\mathsf{Sign}(\mathsf{sk}_\mathcal{S}, m)$: Interpret $\mathsf{sk}_\mathcal{S}$ as an IBE master key mk and public parameters pp, and interpret the message m as an identity id. Output $\sigma \leftarrow \mathsf{Extract}(\mathsf{pp}, \mathsf{mk}, \mathsf{id})$.
- $\mathsf{Verify}(\mathsf{pk}_\mathcal{S}, m, \sigma)$: Interpret $\mathsf{pk}_\mathcal{S}$ as IBE public parameters pp, interpret m as an identity id, and interpret σ as an IBE secret key sk_id. Choose a random message $\tilde{m}$ in the IBE message space. Output "accept" if

$$\mathsf{Dec}(\mathsf{pp},\ \mathsf{Enc}(\mathsf{pp}, \mathsf{id}, \tilde{m}),\ \mathsf{sk}_\mathsf{id}) = \tilde{m}.$$

  Output "reject" otherwise.

Show that if $\mathcal{E}$ is a semantically secure IBE scheme, then $\mathcal{S}$ is a secure signature scheme. Specifically, assume that there is a signature adversary $\mathcal{A}$ that outputs a valid forgery for $\mathcal{S}$ with probability ϵ. Construct an IBE adversary $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine and breaks $\mathcal{E}$ with advantage $\epsilon - 1/r$, where r is the size of the message space for $\mathcal{E}$. You will need to show:

- how $\mathcal{B}$ responds to $\mathcal{A}$'s signature queries;
- how $\mathcal{B}$ uses $\mathcal{A}$'s forgery to distinguish the encryption of a chosen message M from that of a random message M';

- that the advantage of $\mathcal{B}$ in the IBE security game is $\epsilon - 1/r$.

Note that you don't need to worry about any hash function or "random oracles" — you just need to work with the definitions of security. You may assume that Dec is a deterministic algorithm that always outputs a message in the IBE message space.

(Bonus, 2 points.) Why must Verify be randomized? Specifically, say where your security proof fails if we use the following Verify' algorithm: output "accept" if and only if

$$\mathsf{Dec}(\mathsf{pp},\ \mathsf{Enc}(\mathsf{pp}, \mathsf{id}, 0),\ \mathsf{sk}_{\mathsf{id}}) = 0.$$

3. (8 points) **Asymmetric BLS signatures.** The asymmetric version of Boneh-Lynn-Shacham signatures uses an elliptic curve E, two order-n subgroups $\mathbb{G}_1, \mathbb{G}_2 \subset E[n]$, and a nondegenerate, efficiently computable, bilinear map $e \colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_n$. The proof of security in this setting requires an efficiently computable isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$. When E is supersingular we can take $\mathbb{G}_1 = \mathbb{G}_2 = E[n] \cap E(\mathbb{F}_p)$, e to be the modified Weil pairing $\hat{e}$, and ψ to be the identity map. In this problem we will investigate a candidate for the map ψ on more general curves.

   Let ϕ be the p-Frobenius endomorphism. For a fixed $k \geq 1$, define the *trace map* Tr by

   $$\mathrm{Tr}(P) = \sum_{i=0}^{k-1} \phi^i(P).$$

   (a) Show that Tr maps points defined over $\mathbb{F}_{p^k}$ to points defined over $\mathbb{F}_p$. Specifically, show that if $P \in E(\mathbb{F}_{p^k})$, then $\mathrm{Tr}(P) \in E(\mathbb{F}_p)$.

   Suppose that $E(\mathbb{F}_p)$ has a point of prime order n and E has embedding degree $k \geq 2$ with respect to n (i.e., $E[n] \subset E(\mathbb{F}_{p^k})$). Assume $n \nmid kp$. Recall from Homework 3 that ϕ has eigenvalues 1 and p on $E[n]$.

   (b) Show that if $P \in E[n]$ is an eigenvalue of ϕ with eigenvalue p, then $\mathrm{Tr}(P) = \infty$. (*Hint:* factor $p^k - 1$.)

   (c) Show that for any $P \in E[n]$ with $P \neq \infty$, the point $[k]P - \mathrm{Tr}(P)$ is an eigenvector of ϕ with eigenvalue p.

   (d) Let P be a point in $E(\mathbb{F}_p)$ of order n, and let $\mathbb{G}_1 = \langle P \rangle$. For any $R \in E[n]$, let $\mathbb{G}_R = \langle R \rangle$. Show that if R is chosen at random from $E[n]$, then with probability $(1 - 1/n)^2$ it holds that:

      - $e_n(P, R)$ is a generator of $\mu_n \subset \mathbb{F}_{q^k}$, and
      - $\mathrm{Tr} \colon \mathbb{G}_R \to \mathbb{G}_1$ is an isomorphism.

      (Here e_n is the usual Weil pairing.)

4. (10 points) **BGN encryption in prime-order groups.** In this exercise we show how to achieve the functionality of the Boneh-Goh-Nissim encryption scheme without using composite-order groups. Let $E/\mathbb{F}_p$ be an elliptic curve and $P \in E(\mathbb{F}_p)$ a point of *prime* order n. Define the following algorithms:

- $\mathsf{Setup}()$: Choose random $a, b, c \xleftarrow{\text{R}} [1, n]$ such that $c \neq ab \bmod n$. Define $Q = [a]P$, $R = [b]P$, $S = [c]P$. Output the public key $\mathsf{pk} = (P, Q, R, S)$ and the secret key $\mathsf{sk} = (a, b, c)$.
- $\mathsf{Enc}(\mathsf{pk}, m)$: Given a message $m \in [0, t]$ for some small t, choose random $r \xleftarrow{\text{R}} [1, n]$ and output $([m]P + [r]Q, [m]R + [r]S)$.

(a) Give a Dec algorithm that takes a ciphertext (A, B) and outputs m. (*Hint:* first recover $[m]P$, then do a brute-force discrete log calculation.)

(b) Show that if the DDH assumption holds in $\mathbb{G}_1 = \langle P \rangle$, then $\mathcal{E} = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ is semantically secure. (*Hint:* use the "real-or-zero" definition of semantic security from Homework 2, and emulate the BGN security proof from class.)

(c) Let (A_1, B_1) and (A_2, B_2) be encryptions of messages m_1, m_2 respectively. Give an algorithm Add that takes the public key pk and the two ciphertexts as input, and outputs a random encryption of $m_1 + m_2$. The output ciphertext should be distributed as if the message $m_1 + m_2$ was encrypted with fresh randomness. Note that Add does not know either m_1 or m_2.

(d) Now suppose that $P' \in E(\mathbb{F}_{p^k})$ is a point of order n such that $e_n(P, P') \neq 1$. Let $\mathbb{G}_2 = \langle P' \rangle$, and let $\mathsf{pk}' = (P', Q', R', S')$ and $\mathsf{sk}' = (a', b', c')$ be public and secret keys obtained by running $\mathsf{Setup}()$ using the group $\mathbb{G}_2$. Suppose we have

$$(A, B) = \mathsf{Enc}(\mathsf{pk}, m) \qquad \text{and} \qquad (C, D) = \mathsf{Enc}(\mathsf{pk}', m').$$

(Here $A, B \in \mathbb{G}_1$ and $C, D \in \mathbb{G}_2$.) Let Mult be an algorithm that takes as input the two public keys and the two ciphertexts and outputs the tuple $(w, x, y, z) \in \mu_n^4$, where

$$w = e_n(A, C), \quad x = e_n(A, D), \quad y = e_n(B, C), \quad z = e_n(B, D).$$

Show how to recover $e_n(P, P')^{m \cdot m'}$ from (w, x, y, z) and the two secret keys $\mathsf{sk}, \mathsf{sk}'$.

We conclude that if the DDH assumption holds in $\mathbb{G}_1$ *and* $\mathbb{G}_2$, then we have a semantically secure cryptosystem that encrypts small messages, supports arbitrarily many additions of encrypted messages, and allows one multiplication of encrypted messages — exactly the functionality of the BGN cryptosystem. (Technically we also need to show how to rerandomize the tuple (w, x, y, z), but we ignore this for now.)

It is believed that if E is an ordinary (i.e., non-supersingular) elliptic curve, then the DDH assumption holds in the subgroups $\mathbb{G}_1$ and $\mathbb{G}_2$ where $\mathbb{G}_1$ is the 1-eigenspace of Frobenius (i.e., points of order n in $E(\mathbb{F}_p)$) and $\mathbb{G}_2$ is the p-eigenspace of Frobenius (i.e., points of order n with trace zero).

5. (6 points) **Pairing-friendly curves.** For this problem you will want to consult problem #9 of Homework 3.

(a) Find a field $\mathbb{F}_{2^d}$ and a supersingular elliptic curve $E/\mathbb{F}_{2^d}$ of the form $y^2 + y = x^3 + Ax$ (with $A \in \mathbb{F}_{2^d}$) such that

- $E(\mathbb{F}_{2^d})$ has a subgroup of prime order $r > 2^{160}$.

- E has embedding degree 4 with respect to r.
- The Weil pairing on $E[r]$ takes values in a field of size at least 2^{1000}.

(*Hint:* You should find d and r before starting your search for E.)

(b) Find a field $\mathbb{F}_{3^d}$ and a supersingular elliptic curve $E/\mathbb{F}_{3^d}$ of the form $y^2 = x^3 + Ax + 1$ (with $A \in \mathbb{F}_{3^d}$) such that

- $E(\mathbb{F}_{3^d})$ has a subgroup of prime order $r > 2^{160}$.
- E has embedding degree 6 with respect to r.
- The Weil pairing on $E[r]$ takes values in a field of size at least 2^{1000}.

(c) Define

$$\begin{aligned} p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1 \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1 \end{aligned}$$

Find an integer $\alpha > 2^{63}$ such that $p(\alpha)$ and $r(\alpha)$ are both prime. Construct an elliptic curve $E/\mathbb{F}_{p(\alpha)}$ of the form $y^2 = x^3 + B$ such that $\#E(\mathbb{F}_{p(\alpha)}) = r(\alpha)$. Show that E has embedding degree 12 with respect to $r(\alpha)$.

This curve is a *Barreto-Naehrig curve* and is the curve of choice for pairing applications at the 128-bit security level.