Homework 2

Due date: February 23, 2023 at 11:59PM (Gradescope)

Question 1

Consider a modified version of RSA-FDH signatures (Recall that for RSA the public key is $PK = (N, e)$ and the secret key $SK = (N, d)$ where $N = pq$ is the product of two primes p and q and e and d are selected subject to the constraint that $ed = 1 \mod \Phi(N)$). Let $H(\cdot, \cdot)$ be a random oracle outputting random values in $\mathbb{Z}_N$. We have $\mathsf{Sign}_{SK}(m) = (r, H(r, m)^d \mod N)$ where r is a random λ-bit nonce. $\mathsf{Verify}_{PK}(m, (r, s)) = 1$ if and only if $H(r, m) = s^e \mod N$. We say that the signature scheme is $(t, m, q_H, q_S, \epsilon)$-secure if any attacker running in time at most t, using space at most m, making at most q_H (resp. q_S) queries to the random oracle (resp. signing oracle) wins the signature forgery game with probability at most ϵ. Your task is to prove that modified RSA-FDH signatures are $(t, m, q_H, q_S, \epsilon)$-secure. You may assume that any attacker running in time t and space m wins the RSA-inversion game with probability at most γ. For full credit, your reduction should be as tight as possible with respect to all parameters (time, memory, q_H, and q_S).

Answer:

...

Resource and Collaborator Statement:

...

Question 2

We say that a signature scheme is $(t, s, q_H, q_S, \epsilon)$-secure if any pre-processing attacker outputting a s-bit hint, running in online time t, and making at most q_H (resp. q_S) queries to the random oracle (resp. signing oracle) in the online phase wins the signature forgery game with probability at most ϵ.

Notes: We will assume that the s-bit hint may depend on the random oracle $H(\cdot)$ but that the public/secret key (sk, pk) for our signature scheme are generated *after* the hint is fixed. The s-bit hint may depend on the random oracle $H(\cdot)$, but the primes p and q for the RSA key $N = pq$ are selected ***after*** the s-bit hint is fixed. You may assume that the RSA-key generation algorithm outputs a random public key (N, e) with $2^n \leq N \leq 2^{n+1}$ and that the random oracle outputs random $2n$-bit strings which can be interpreted as an integer between 0 and $2^{2n} - 1$. Since the RSA-inversion game generates fresh values $N, e, x, y = x^e \mod N$ (unrelated to the random oracle) you may assume that any pre-processing attacker $(\mathcal{A}_1, \mathcal{A}_2)$ wins the RSA-inversion game with probability at most γ when $\mathcal{A}_1$ gets to output an s-bit hint and $\mathcal{A}_2$ runs in time at most t.

Useful Fact: Let U_N denote the uniform distribution over $\mathbb{Z}_N$. Given $N' \geq kN$ let $D_{N,N'}$ denote a distribution over $\mathbb{Z}_N$ defined as follows 1. Sample $y \in \mathbb{Z}_{N'}$ and output

$y \mod N$. You may use the following observation without proof. The statistical distance between the two distributions is at most

$$\mathtt{SD}(U_N, D_{N,N'}) \doteq \frac{1}{2} \sum_{x \in \mathbb{Z}_N} | \Pr_{U_N}[x] - \Pr_{D_{N,N'}}[x]| \leq \frac{1}{k} .$$

Part A. Consider the regular RSA-FDH signature scheme i.e., $\mathsf{Sign}_{sk}(m) = (H(m)^d \mod N)$. Is it secure with respect to a pre-processing attacker $(\mathcal{A}_1, \mathcal{A}_2)$ where $\mathcal{A}_1$ can examine the entire random oracle and output a short s-bit hint? Either give an attack or give the tightest security bound that you can prove.

> *Answer:*
>
> ...

Part B. Suppose that RSA-key generation picks two random $n/2$-bit primes p and q (i.e., $2^{n/2}+1 < p < 2^{n/2+1}$ and $2^{n/2}+1 < q < 2^{n/2+1}$) and sets $N = pq$. Upper bound the probability that RSA-key generation outputs a particular $N = pq$. You may assume that $\pi(2^{n/2+1} - 1) - \pi(2^{n/2} + 1) > \frac{2^{n/2}}{n}$ where $\pi(x)$ counts the total number of prime numbers less than x.

> *Answer:*
>
> ...

Part C. Consider a key-prefixed version of RSA-FDH where $\mathsf{Sign}_{sk}(m) = (H(pk, m)^d \mod N)$. Is it secure with respect to a pre-processing attacker $(\mathcal{A}_1, \mathcal{A}_2)$ where $\mathcal{A}_1$ can examine the entire random oracle and output s-bit hint? Either give an attack or give the tightest security bound that you can prove.

> *Answer:*
>
> ...

> *Resource and Collaborator Statement:*
>
> ...

Question 3

Let $F : \{0,1\}^{\lambda_1} \times \{0,1\}^{\lambda_2} \rightarrow \{0,1\}^n$ be a PRF and assume that F is (t, q_F, ϵ)-secure with $\epsilon = t/2^{\lambda_1}$. Consider the encryption scheme $\mathtt{Enc}_K(m) = \langle r, F_K(r) \oplus m \rangle$ for messages of length n where r is a uniformly random λ_2-bit nonce.

Consider the Real-or-Random Security Game where an attacker gets access to an oracle $\mathbb{ENC}(\cdot)$ and tries to guess a random bit b picked by the challenger: The challenger picks a random bit b and a random λ_1 bit key K. The oracle $\mathbb{ENC}(m)$ works as follows:

$\underline{\mathbb{ENC}(m)\text{:}}$

if $b = 0$ **then**
  return $\texttt{Enc}_K(m)$.
else
  if $b = 1$ **then**
    Pick a random $n + \lambda_2$ bit string $x \in \{0,1\}^{\lambda_2+n}$
    return x.
  end if
end if

Part A. We say that an encryption scheme is (t, q, ϵ)-ROR secure if any attacker running in time t and making at most q queries to the oracle $\mathbb{ENC}(\cdot)$ wins with probability at most $\frac{1}{2} + \epsilon$ i.e., with advantage at most ϵ. Analyze the concrete security of the above encryption scheme, and discuss the dependence (if any) on the parameters λ_1, λ_2, n, and q.

> *Answer:*
>
> ...

Part B. We say that an encryption scheme is (t, s, q, ϵ)-secure if any attacker running in time at most t, using space at most s and making at most q queries to the oracle $\mathbb{ENC}(\cdot)$ wins with probability at most $\frac{1}{2} + \epsilon$. Can you improve the above analysis under the assumption that the attacker is memory bounded? Explain your answer.

> *Answer:*
>
> ...

> *Resource and Collaborator Statement:*
>
> ...

Question 4

Once again consider the encryption scheme $\texttt{Enc}_K(m) = \langle r, H(K, r) \oplus m \rangle$ for messages of length n. Here, m is an n bit message, $H(\cdot,\cdot)$ is a random oracle outputting n-bit strings, K is a λ_1 bit secret key and r is a uniformly random λ_2-bit nonce. In this problem, we will reconsider our concrete security bounds against a pre-processing attacker.

Part A. Consider a bit-fixing attacker $(\mathcal{A}_1, \mathcal{A}_2)$ where the offline attacker fixes P input/output pairs for the random oracle $H(\cdot,\cdot)$ and outputs and s-bit hint. The remaining entries for the random oracle are then picked uniformly at random. The attacker $\mathcal{A}_2$ is then given the s-bit hint and plays the Real-Or-Random-security game (Note that the challenger picks the random key K *after* $\mathcal{A}_1$ finishes). Suppose that the online $\mathcal{A}_2$ makes at most q_H (resp. q_E) queries to the random oracle (resp. encryption oracle). Upper bound the advantage of $\mathcal{A}_2$ in the ROR security game.

Answer:

...

Part B. Consider a auxiliary-input attacker $(\mathcal{A}_1, \mathcal{A}_2)$ where the attacker $\mathcal{A}_1$ examines the entire truth table for $H(\cdot,\cdot)$ and then outputs an s-bit hint. The attacker $\mathcal{A}_2$ is then given the s-bit hint and plays the Real-Or-Random-security game. Suppose that $\mathcal{A}_2$ runs in time t and makes q encryption queries. Upper bound the advantage of $\mathcal{A}_2$ in the ROR security game.

Answer:

...

Part C. Assume that the s-bit hint that is given to $\mathcal{A}_2$ is stored on a read-only tape. Suppose that the online $\mathcal{A}_2$ makes at most q_H (resp. q_E) queries to the random oracle (resp. encryption oracle) and that the attacker's memory is at most m-bits (excluding the s-bit read-only tape). Can you give a tighter upper bound on the advantage of the online attacker $\mathcal{A}_2$ in the ROR security game? We are looking for a bound in the auxiliary-input model, but it may be useful to first reconsider the upper bounds in the bit-fixing model.

Answer:

...

Resource and Collaborator Statement:

...