Amjad Alqahtani

Cryptography

Amjad.alqahtani@my.utsa.edu

Assignment 6 — Digital Signature Schemes

Contents

1 Introduction **2**

2 Deterministic vs. Randomized Sign Algorithms **2**

2.1 EUF-CMA Security Game (Definition 13.1) 2

2.2 Impact of Removing Randomness 2

2.3 Formal Proof Sketch 2

3 Is RSA-FDH Deterministic? **3**

4 RSA-FDH and the Hash-and-Sign Paradigm **3**

4.1 Construction 13.3 (Hash-and-Sign) 3

4.2 Construction 13.6 (RSA-FDH) 3

4.3 Detailed Comparison 3

4.4 Security Reduction for RSA-FDH 4

5 Why Immediate Certificate Revocation Is Correct **4**

5.1 Certificate Lifecycle 4

5.2 Analysis of All Scenarios 4

5.3 CRL vs. OCSP 5

6 Conclusion **5**

1 Introduction

Digital signature schemes provide message authenticity, integrity, and non-repudiation. This report answers four in-depth questions concerning deterministic signatures, the RSA Full-Domain Hash (FDH) scheme, the general hash-and-sign paradigm, and public-key certificate revocation policies. All citations refer to Katz & Lindell, *Introduction to Modern Cryptography*, 3rd ed., §§13.1–13.4.

2 Deterministic vs. Randomized Sign Algorithms

2.1 EUF-CMA Security Game (Definition 13.1)

A signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ is existentially unforgeable under chosen-message attack (EUF-CMA) if for every probabilistic polynomial-time (PPT) adversary A:

1. The challenger runs $(pk, sk) \to \mathsf{Gen}(1^n)$ and gives pk to A.
2. A may adaptively query a signing oracle for messages m_i of its choice and receives $\sigma_i \to \mathsf{Sign}_{sk}(m_i)$.
3. Eventually, A outputs (m^*, σ^*). A wins if $\mathsf{Vrfy}_{pk}(m^*, \sigma^*) = 1$ and $m^* \notin \{m_1, \ldots, m_q\}$.

2.2 Impact of Removing Randomness

Suppose Sign is converted from probabilistic ($\sigma \to \mathsf{Sign}_{sk}(m)$) to deterministic ($\sigma := \mathsf{Sign}_{sk}(m)$). Then:

- Resubmitting the same message m always returns the identical signature σ.
- In the EUF-CMA definition, extra oracle calls on m provide no additional data; σ was already known after the first query.
- Consequently, an optimal adversary never benefits from duplicated queries.

2.3 Formal Proof Sketch

Let A be an arbitrary EUF-CMA adversary against the deterministic scheme; assume it makes at most q signing queries. Construct A′ that simulates the signing oracle but maintains a cache:

- On query m:
  - If $m \in$ cache, then return cache[m].
  - Else, $\sigma := \mathsf{Sign}_{sk}(m)$; cache[$m$] $:= \sigma$; return σ.

A′ forwards the final forgery produced by A. Since the simulation is perfect, Pr[A wins] = Pr[A′ wins]. But A′ invokes the real signing oracle at most once per distinct message; thus, repeated queries are redundant. Therefore, determinism provides no extra advantage in the EUF-CMA game.

3 Is RSA-FDH Deterministic?

Construction 13.6 (RSA-FDH) defines the signature of a message $m \in \{0, 1\}^*$ as

$$\sigma := H(m)^d \mod N,$$

where (N, e) is the public key, d the private exponent, and $H : \{0, 1\}^* \to \mathbb{Z}^*_N$ is a deterministic full-domain hash. No fresh randomness appears, hence RSA-FDH is deterministic: identical messages yield identical signatures.

4 RSA-FDH and the Hash-and-Sign Paradigm

4.1 Construction 13.3 (Hash-and-Sign)

Given a base scheme $\Pi = (\mathsf{Gen}', \mathsf{Sign}', \mathsf{Vrfy}')$ for fixed-length $\ell(n)$ messages and a hash $H : \{0, 1\}^* \to \{0, 1\}^{\ell(n)}$, build $\Pi'' = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$: **Theorem 13.4**: If Π' is EUF-

Step	**Description**
$\mathsf{Gen}(1^n)$	Run $\mathsf{Gen}'(1^n) \to (pk', sk')$. Output $pk = (pk', s)$ where s is the description of H; secret key is $sk = (sk', s)$.
$\mathsf{Sign}_{sk}(m)$	Return $\sigma := \mathsf{Sign}'_{sk}(H(m))$.
$\mathsf{Vrfy}_{pk}(m, \sigma)$	Accept if $\mathsf{Vrfy}'_{pk}(H(m), \sigma) = 1$.

CMA-secure for $\ell(n)$-bit messages and H is collision-resistant, then Π'' is EUF-CMA-secure for arbitrary-length messages.

4.2 Construction 13.6 (RSA-FDH)

Phase	**Operation**
KeyGen	$(N, e, d) \to \mathsf{GenRSA}(1^n)$. Public key $pk = (N, e)$, secret key $sk = d$. A full-domain hash $H : \{0, 1\}^* \to \mathbb{Z}^*_N$ is fixed.
Sign	$\sigma := H(m)^d \mod N$.
Vrfy	Accept if $\sigma^e \equiv H(m) \pmod N$.

4.3 Detailed Comparison

Property	**Hash-and-Sign (General)**	**RSA-FDH (Specific)**
Base scheme Π'	Arbitrary EUF-CMA scheme on ℓ bits	Plain RSA on $\log_2 N$ bits
Hash range	$\{0, 1\}^\ell$	$\mathbb{Z}^*_N$ (full domain)
Hash requirement	Collision resistance	Modeled as random oracle; needs pseudorandom range & no multiplicative relations
Randomness in Sign	Inherited from Π'	None (deterministic)
Security proof	Holds in the standard model (if Π' secure & H CR)	Shown secure in the random-oracle model under RSA assumption

Table 1: Comparison between Hash-and-Sign and RSA-FDH

Thus, RSA-FDH is an instantiation of hash-and-sign where the base signer is plain RSA and the hash outputs span the entire RSA modulus.

4.4 Security Reduction for RSA-FDH

Model: Random-oracle model (ROM); adversary F is EUF-CMA forger.
Goal: Build RSA inverter B using F.

1. **Setup**. B receives an RSA instance (N, e, y) and must output $x = y^{1/e} \bmod N$. It sets public key (N, e) for F.

2. **Programming the oracle**. B chooses a random query index i^*. When F issues its i^*-th hash query on message m^*, B programs $H(m^*) := y$. All other queries are answered with fresh random elements of $\mathbb{Z}_N^*$.

3. **Signing queries**. Given a message m:

   - If $m = m^*$, return $\perp$ (EUF-CMA allows refusal once).
   - Else, compute $\sigma := H(m)^{1/e}$ using knowledge of $H(m)$ (thanks to oracle programming) and return it.

4. **Forge**. When F outputs (m^*, σ^*) such that $(\sigma^*)^e \equiv H(m^*) = y \pmod N$, then σ^* is exactly $y^{1/e}$. B outputs σ^* and succeeds.

Hence, an EUF-CMA forger with advantage ε yields an RSA inverter with essentially the same advantage (minus negligible terms), establishing ROM security of RSA-FDH.

5 Why Immediate Certificate Revocation Is Correct

5.1 Certificate Lifecycle

1. **Issue** — CA binds identity to public key by signing a certificate.

2. **Use** — Relying parties verify signatures using the certified public key.

3. **Revocation** — CA adds the certificate to a CRL or serves an OCSP revoked response when trust must stop.

5.2 Analysis of All Scenarios

Let the CA receive a properly-verified message "My key is stolen" under Bob's current certificate. In both cases, the cryptographic binding between Bob and pk_B is void; continued trust endangers relying parties. Thus, the CA's "revoke first, investigate later" policy is the only safe option.

Scenario	Reality	Risk if not revoked	Action
(A) Message is genuine → Key truly compromised.	Adversary can sign arbitrary messages as Bob.	Immediate revocation protects everyone.	
(B) Message is forged but passes verification → Signature scheme or key is compromised.	We already witnessed a successful forgery ⇒ further forgeries possible.	Immediate revocation again protects everyone.	

5.3 CRL vs. OCSP

- **CRL (Certificate Revocation List)**: Periodic, signed list of revoked certificate serial numbers.
  - **Pros**: Offline checking possible, no per-transaction latency.
  - **Cons**: List may be stale between updates; large downloads.
- **OCSP (Online Certificate Status Protocol)**: Client queries CA's responder for each certificate.
  - **Pros**: Near-real-time status, small responses.
  - **Cons**: Extra round-trip; privacy leak unless OCSP-stapling used.

Best practice is **OCSP-stapling**: the server fetches and caches a fresh OCSP response, embedding it in the TLS handshake so clients avoid direct contact with the CA.

6 Conclusion

- Deterministic signing yields identical signatures; duplicate oracle queries offer no EUF-CMA advantage.
- RSA-FDH is deterministic and is a concrete instantiation of the hash-and-sign paradigm with plain RSA over the full modulus domain.
- RSA-FDH's security reduction in the random-oracle model tightly relates EUF-CMA forgery to RSA inversion.
- From a PKI perspective, any credible evidence of key compromise—real or forged—mandates immediate certificate revocation to maintain systemic trust.