

SIGNATURE SCHEME 1. Gennaro-Halevi-Rabin signature scheme GHR.

Key generation.

Input: Security parameter n , and ℓ and $h: \mathbb{B}^\ell \rightarrow P$ as above.

Output: N , public key pk , secret key sk , and $t \in \mathbb{Z}_N^\times$.

1. Choose uniformly random r -safe primes p and q with $2^{(n-1)/2} \leq p, q < 2^{n/2}$, where r is the largest prime in P .
2. RSA modulus $N \leftarrow p \cdot q$.
3. $t \xleftarrow{\$} \mathbb{Z}_N^\times$.
4. $\text{sk} \leftarrow (N, \phi(N))$, $\text{pk} \leftarrow (N, t)$.

SIGNATURE SCHEME 2. Gennaro-Halevi-Rabin signature scheme GHR.

Signing.

Input: $m \in \mathbb{B}^\ell$.

Output: $s = \text{sig}_{\text{sk}}(m)$.

1. Compute the inverse v of h_m in $\mathbb{Z}_{\phi(N)}^\times$.
2. Compute $s \leftarrow t^v$ in \mathbb{Z}_N^\times .

Verifying.

Input: $m \in \mathbb{B}^\ell$ and $u \in \mathbb{Z}_N^\times$.

Output: “true” or “false”.

3. If $u^{h_m} = t$ in \mathbb{Z}_N^\times then return “true” else return “false”.

Theorem

In the Gennaro-Halevi-Rabin signature scheme, the verification step works correctly. If 2^ℓ is polynomial in n , then the operations can be executed in time polynomial in n .

PROBLEM 3. Weak RSA problem.

Input: an RSA modulus $N = pq$ and $y \in \mathbb{Z}_N^\times$.

Output: $x \in \mathbb{Z}_N^\times$ and an integer $c \geq 2$ with $y = x^c$ in \mathbb{Z}_N^\times .

Theorem

Let N be an RSA modulus, and \mathcal{F} be an existential (τ, σ) -forger of GHR signatures with modulus N , making at most q signature queries with chosen messages. Then using \mathcal{F} one can solve the weak RSA problem for an n -bit key $y \xleftarrow{\text{RSA}} \mathbb{Z}_N^\times$ in polynomial time $\tau + (q + 1) \cdot O(n^3 + \ell 2^\ell)$ with success probability at least $2^{-\ell} \sigma$.

ALGORITHM 4. Reduction \mathcal{A} from weak RSA to breaking GHR.

Input: RSA modulus N , $y \in \mathbb{Z}_N^\times$.

Output: x, c with $x^c = y$ in \mathbb{Z}_N^\times and $c \geq 2$, or “failure”.

1. Choose $i \xleftarrow{\$} \mathbb{B}^\ell$.
2. For each $m \in \mathbb{B}^\ell$, compute h_m . Compute the integer

$$u = \prod_{\substack{m \in \mathbb{B}^\ell \\ m \neq i}} h_m.$$

3. Choose $r \xleftarrow{\$} \mathbb{Z}_N^\times$. Compute $t = (r^{h_i} y)^u$ in \mathbb{Z}_N^\times , and send the GHR pk = (N, t) to \mathcal{F} .
4. When \mathcal{F} requests a signature for some message $m \in \mathbb{B}^\ell$, \mathcal{A} replies with $s = (r^{h_i} y)^{u/h_m}$ if $m \neq i$; note that u/h_m is an integer. If $m = i$, \mathcal{A} reports “failure”.
5. \mathcal{F} returns some (m, s) at the end to \mathcal{A} , which is a validly signed message with probability at least σ . If $m \neq i$, \mathcal{A} reports “failure”. If $m = i$, \mathcal{A} checks $\text{ver}_{N,t}(m, s)$. If the signature is valid, it computes integers v and w so that $v \cdot h_i + w \cdot u = 1$. Then \mathcal{A} returns $x = s^w r^{-uw} y^v$ and $c = h_i$.

We will show the following properties of this algorithm \mathcal{A} :

- ▶ \mathcal{A} can be executed in time polynomial in n ,
- ▶ \mathcal{A} satisfies \mathcal{F} 's key and signature requests properly, or fails,
- ▶ \mathcal{A} returns a solution to the weak RSA problem with probability at least $\sigma \cdot 2^{-\ell}$.

Corollary

We have $\text{weak RSA}(N) \leq_p$ existentially forging GHR signatures with modulus N using chosen messages.

Strong RSA assumption

The weak RSA problem is hard, that is, there is no random polynomial-time algorithm that solves it with nonnegligible success rate.