Def (Trapdoor hash function) \( \text{Gen, Hash, Patch} \) st.

* \( \text{Gen}(1^k) \rightarrow K, \text{trapdoor} \)
* \( \text{Hash}_K(m, r) \) is a \( \text{CRHF} \)
* \( \text{Patch}_K(m, m', r, \text{trapdoor}) \rightarrow r' \) st.
  \[ \text{Hash}_K(m, r) = \text{Hash}_K(m', r') \]

A's Goals

* to forge a sig on any msg
* to forge a sig on a specific msg

A's Abilities

* A knows just \( \text{vk} \)
* A obtains sigs on random msgs \( \rightarrow \) msg attack (RMA)
* A can adaptively obtain sigs \( \rightarrow \) chosen on msgs of its choosing \( \rightarrow \) msg attack (CMA)

Existential Unforgeability

* EUF-CMA, the standard (strongest) notion of security for digital sigs

Today: EUF-RMA + TDHF \( \Rightarrow \) EUF-CMA

Informally, security of TDHF: Given \( \tilde{m}, \tilde{r} \), can't tell if it was the original \( m, r \) or the "patched" \( m', r' \)
Example of a TDHF.

* $\text{Gen} (1^k) \rightarrow (K, \text{generator } g, \text{ order } q)$

\[ \text{let } h = g^t, \quad t \in \mathbb{Z}_q \]

$K = (G, g, q, h)$ trapdoor = t

* $\text{Hash}_K (m, r) = g^{m+tr} = q^{m+tr}$

want to patch s.t.

$\text{msg} \in \mathbb{Z}_q$ random value

$\in \mathbb{Z}_q$

* $\text{Patch}_K (m, m', r, t)$:

uniformly

if $r$ is random, so is $r'$

Suppose $(\text{KeyGen, Sign, Verify})$ is a EUF-RMA sig scheme

Let $\text{KeyGen}^* (1^k)$: Run $\text{KeyGen} (1^k) \rightarrow (vk, sk)$

$\text{Gen} (1^k) \rightarrow (K, \text{trapdoor})$

output $\{ vk^* = (vk, K) \}

\quad \{ sk^* = sk \}$

$\text{Sign}^* (sk^*, m)$: Pick $r$ according to the sampling alg in $\text{Hash}_K$

for choosing $r$

Compute $msg = H_K (m, r)$

$\sigma = \text{Sign} (sk, msg)$

Output $\sigma^* = (\sigma, r)$

$(vk, K)$

$\text{Verify}^* (vk^*, m, \sigma^*)$: Compute $msg$ & then verify $(vk, msg, \sigma)$
Proof of security

Reduction: input is \( vk \)

\[ \text{access to a signer that signs random messages} \]

Goal: issue one more sig

\[ \begin{array}{c}
\text{Reduction} \\
K, \text{trapdoor} \\
\vdots \\
vk^* \\
\text{Signer for random msgs} \\
\end{array} \]

\[ \begin{array}{c}
m \\
r \leftarrow \$ \\
\sigma \leftarrow \text{Sign}(m) \\
\text{Hash}_{K}(mF, vk) \\
\text{msg}^*, \sigma \\
\end{array} \]

\[ \begin{array}{c}
m_{F, \sigma_{F}} \\
\text{(r, o)} \\
\text{msg}^*, \sigma \\
m_{F, \sigma_{F}} \\
\end{array} \]

\[ \text{A adaptively queries msg's to be signed} \]

\& finally forges a sig \((m_{F, \sigma_{F}})\)

Tying loose ends

& Security under RMA \quad \text{let } M \text{ be the message space}

\[ \begin{array}{c}
\text{Challenger} \\
\vdots \\
\text{Adversary} \\
\text{def } (\text{EUF-RMA}) \\
\end{array} \]

\[ \begin{array}{c}
vk \\
m_{F, \sigma_{F}} \\
\text{msg} \leftarrow M, \text{sk,} \\
\sigma \leftarrow \text{Sign}(msg) \\
\text{msg}^*, \sigma \\
\text{READY} \\
\text{msg}^*, \sigma^* \\
\end{array} \]

\[ \text{Pr [Verify} (vk, msg^*, \sigma^*) = \text{accept}] \]

is negl.

In RMA, msgs are chosen uniformly @ random, so Challenger can do this
§ Security for trapdoor hashing

want: \( \forall m, \text{ if } r \text{ is RANDOM, then msg is UNIFORMLY RANDOM element of } M \)

§ RMA-like secure signature scheme under strong RSA assumption

**DEF** (Strong RSA assumption)

On input \((N, x)\)

\(^\uparrow \text{RSA modulus } \in \mathbb{Z}_N^* \)

it is hard to find \(y, e > 1\) s.t. \(y^e \equiv x \mod N\)

**The Scheme**

\{*

\* Key Gen \((1^k)\): \(vk \leftarrow (N, x)\)

\(sk = \text{factorization of } N\)

\(m \leftarrow \{0, 1\}^{l \text{ bits}}\)

\* Sign \((sk, m)\): Interpret \(m\) as a prime #

Output \(\sigma = y\) s.t. \(y^m \equiv x \mod N\)

\* Verify \((vk, m, \sigma)\): \(\sigma^* = x\)

In what sense is this secure? Secure under RMA-like security game

RMA-like in that msgs are chosen independent of \(vk\). but may not be iid UNIFORM

\[
C_h \xleftarrow{} m_0, \ldots, m_r \xrightarrow{A} \xrightarrow{\text{vk, } \sigma_1, \ldots, \sigma_r} m^*, \sigma^*
\]
Strong RSA signature scheme is secure against the RMA-like attack (under the strong RSA assumption)

**Proof**

If $A$ can break RMA-like game, $B$ can break strong RSA thanks to meaning produces $(m^*, \sigma^*)$ meaning given $(N, x)$ can Liz for $s.t. (\sigma^*) m^* = x^*$ find $y, e$ s.t. $y^e \equiv x \mod N$

this cleaned up reduction

\[ (N, x) \rightarrow \rightarrow (N, x) \]

$B$ forms $x^* = \prod_{i} m_i^*$

\[ = x^2 \]

and $\sigma_i^* = x \prod_{j \neq i} m_j$

so that $(\sigma_i^*) m_i = (x \prod_{j \neq i} m_j) m_i = x \prod_{i} m_i = x^2 = x^*$

$m^*$ relatively prime to all $m_i$'s so $\exists a, b \in \mathbb{Z}$ s.t. $am^* + bz = 1$

$(\sigma^*) m^* = x^* = x^2$ by defn of $A$'s success

$\Rightarrow (\sigma^*) m^* b = x^2 b$

$\Rightarrow (\sigma^*) m^* b x m^* a = x^2 b + m^* a = x^2 = x$

$\Rightarrow ( (\sigma^*)^b (x^*) ) m^* = x$

$\Rightarrow (\sigma^*) m^* = y^e$
§ GHR '98 \( H_k \) trapdoor hash function

\[
\begin{align*}
\text{same as} & \quad \{  \\
\text{before but} & \quad h = H_k(m, r) \text{ interpret as prime}  \\
\text{w/ these} & \quad \text{Verify } (vk, m, \sigma, r)  \\
\text{changes} & \quad ^\uparrow \text{need this as well}
\end{align*}
\]

\[\text{THM}\] The GHR sig scheme is secure under the strong RSA assumption & if Hash is a secure trapdoor hash function