Hash-and-Sign with Weak Hashing Made Secure

Sylvain Pasini
and
Serge Vaudenay

LASEC EPFL

ACISP '07, Townsville, Australia

July the 4^{th} 2007


Signatures Schemes

Digital Signature Definition

A Digital Signature scheme is defined by three algorithms:

setup: $(K_p, K_s) \leftarrow \text{setup}()$

sign: $\sigma \leftarrow \text{sign}(K_s, m)$

verify: $b \leftarrow \text{verify}(K_p, m, \sigma)$
outputs 1 when (m, σ) is valid and 0 otherwise

Two categories:

- Fixed message-length digital signature, e.g. $m \in \{0,1\}^n$
- Arbitrary message-length digital signature, e.g. $m \in \{0,1\}^*$

Adversarial Models

We consider

- an adversary $\mathcal{A}$ playing a game with a challenger $\mathcal{C}$
- the goal of $\mathcal{A}$ is to output a valid pair $(\widehat{m}, \widehat{\sigma})$

We distinguish

UF: Universal forgeries, i.e. $\widehat{m}$ is imposed to $\mathcal{A}$

EF: Existential forgeries, i.e. $\widehat{m}$ is chosen by $\mathcal{A}$

KMA: $\mathcal{A}$ receives samples pairs (m_i, σ_i)

CMA: $\mathcal{A}$ has access to a signing oracle

In the following, we use

	KMA	CMA
UF	weak security	
EF		strong security

Example: plain RSA is weakly secure

Plain RSA:

setup: Let $n = pq$ where p, q are huge prime numbers.
Pick e and let $d = e^{-1} \bmod \varphi(n)$.
$K_p = (e, n)$ and $K_s = (d, n)$.

sign: $\sigma = m^d \bmod n$.

verify: If $\sigma^e = m \pmod n$ output 1,
otherwise output 0.

A trivial existential forgery:

- Pick σ
- Let $\widehat{m} = \sigma^e \bmod n$
- The pair $(\widehat{m}, \sigma)$ is always valid

So, plain RSA is weakly secure.


The Hash-and-Sign Paradigm and its Variations

Motivation

Usually, plain signature schemes

- have a limited domain
- are weakly secure

Consider S_0 a weakly secure scheme on domain $\{0,1\}^n$.

We would build a signature scheme S' which is able to

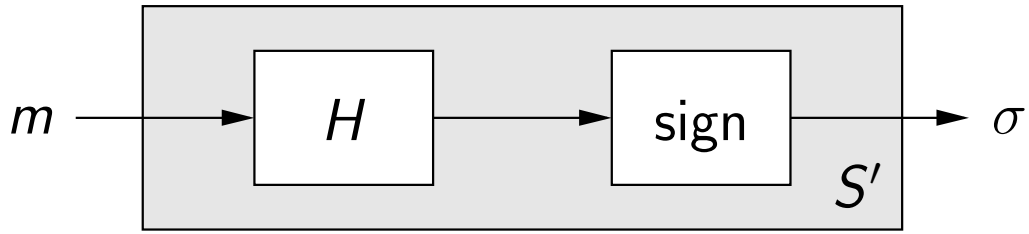
- sign longer messages
- achieve strong security

Collision Resistant Hash Function (CRHF)

Definition

$H : \{0,1\}^* \mapsto \{0,1\}^n$ is a CRHF if:
it is hard to find x, y s.t. $H(x) = H(y)$ and $x \neq y$.

We construct S':



Theorem

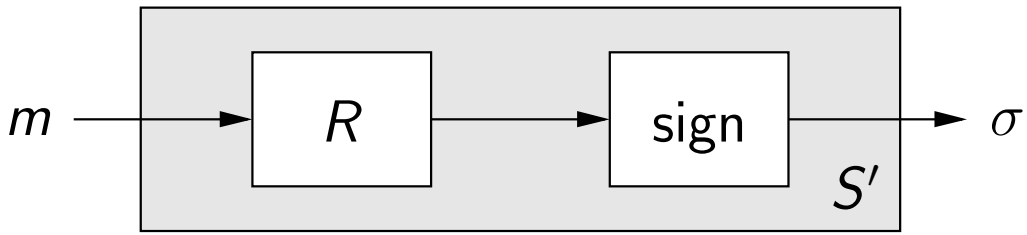
If H is a CRHF and S_0 is strongly secure,
then S' is strongly secure.

Random Oracle (RO)

Definition

A RO $R : \{0,1\}^* \mapsto \{0,1\}^n$ is a random function.

We construct S':



Theorem

If R is a RO and S_0 is weakly secure,
then S' is strongly secure.

Target Collision Resistant (TCR) Hash Function

TCR was introduced by Naor and Yung (1989) a.k.a. UOWHF.

Definition

A TCR hash function is a keyed function

$$H : \{0,1\}^k \times \{0,1\}^* \mapsto \{0,1\}^n$$

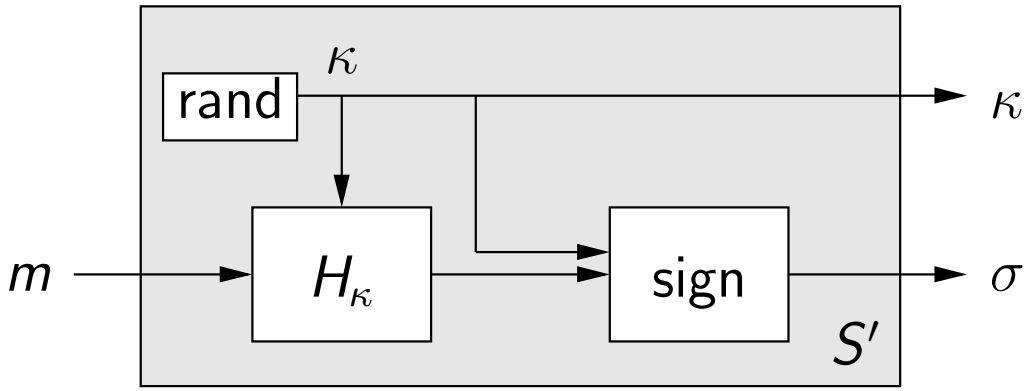
such that the following game is hard.

$$\begin{array}{ccc} \mathcal{A} & & \mathcal{C} \\ & \xrightarrow{m} & \\ & \xleftarrow{K} & \text{pick } K \in_U \{0,1\}^k \\ & \xrightarrow{\widehat{m}} & \end{array}$$

$\mathcal{A}$ **win if** $H_K(\widehat{m}) = H_K(m)$, $\widehat{m} \neq m$

Hash-and-Sign with TCR

Constuction from Bellare-Rogaway (1997):



Theorem (idea)

If $\exists G_0$ that makes sign $(K_s, G_0(m))$ strongly secure,
then S' is strongly secure (in the random oracle model).

Hash-and-Sign with TCR

Remaining problems:

1. No reduction to weak security of S_0
2. The signature enlarges
3. κ must be signed
4. We still need a random oracle

enhanced TCR (eTCR)

eTCR was introduced by Halevi-Krawczyk (2006).

Definition

An eTCR function is a stronger TCR function

$$H : \{0,1\}^k \times \{0,1\}^* \mapsto \{0,1\}^n$$

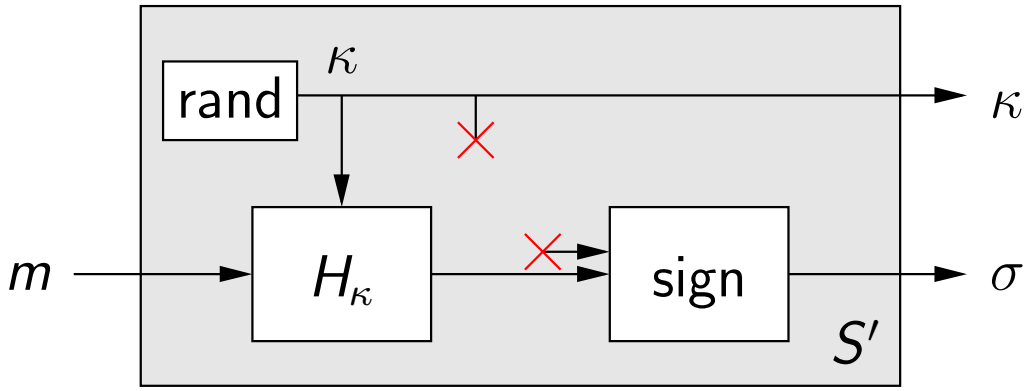
such that the following game is hard.

$$\begin{array}{ccc} \mathcal{A} & & \mathcal{C} \\ & \xrightarrow{m} & \\ & \xleftarrow{K} & \text{pick } K \in_U \{0,1\}^k \\ & \xrightarrow{\widehat{m} \| \widehat{K}} & \end{array}$$

$\mathcal{A}$ **win if** $H_{\widehat{K}}(\widehat{m}) = H_K(m)$, $(m, K) \neq (\widehat{m}, \widehat{K})$

Hash-and-Sign with eTCR

Construction suggested by Halevi-Krawczyk (2006):



In the paper, there is an eTCR construction and its security proof.
But, no formal proof of security of the signature construction.

In a nutshell

We saw the hash-and-sign paradigm with:

- CRHF (no security increase)
- Random Oracle (need a random oracle)
- TCR (still need a random oracle for the proof)
- eTCR (no formal security proof)

Note that hash functions are far from random oracles.

Our goals

Find a construction which

- is provably secure
- in an "better" (weaker) model than the random oracle model
- reuses actual implementations (preprocessing only)
- does not enlarge the signature


The Weak Hashing Model

Looking for a model...

Claim

Hash functions are becomming weaker and weaker...

Goal

Find (and use) a weaker model than the random oracle model.

Liskov (2006) proposed to modelize compression function with:

- a random oracle
- an additional breaking oracle
  - collision-tractable oracle
  - second preimage-tractable oracle
  - first preimage-tractable oracle (stronger model)

Preimage-Tractable Random Oracle

We consider weak hash functions:

preimages are computable (so collisions too).

We hope that SHA-1 and MD5 fit at least that model.

Preimage-Tractable Random Oracle Model

Consists of two oracles:

G: compute images (as a random oracle),
i.e. $r \leftarrow \mathsf{G}(m) \in_{\mathsf{u}} \{0,1\}^n$.

preimageG: find a preimage of a hashed value,
i.e. $m \leftarrow \mathsf{preimageG}(r) \in_{\mathsf{u}} \mathsf{G}^{-1}(r)$.

Preimage-Tractable Random Oracle, Note

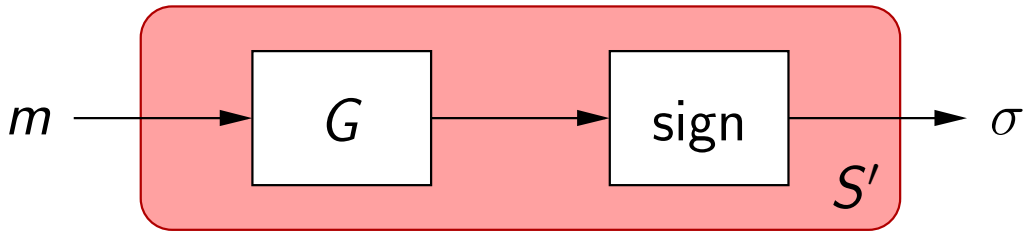
From a theoretical viewpoint, the preimage-tractable random oracle is as powerful as the random oracle.

Our motivation is to model weak hash functions.


A Secure Hash-and-Sign with Weak Hashing

Actual Implementations

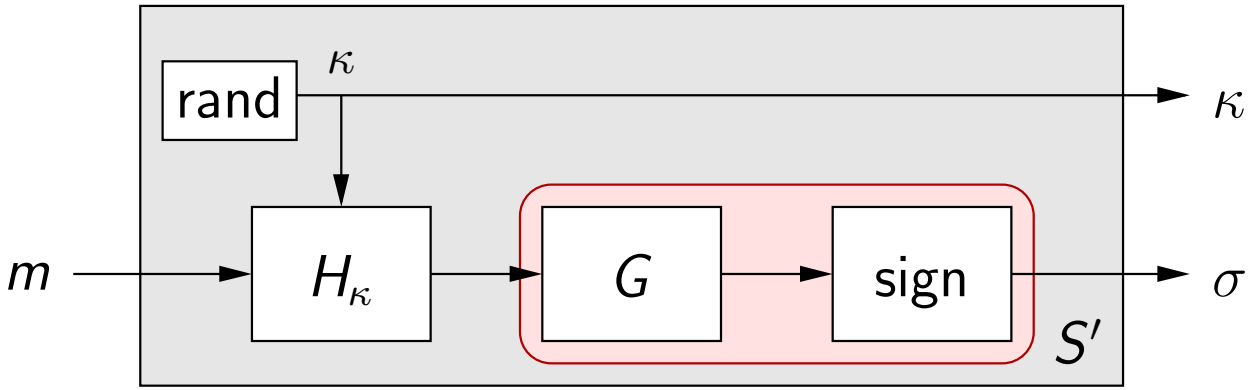
Today, most of the implementations use the hash-and-sign:



G is claimed to be collision-resistant,
but as it is becoming less secure,
the overall signature too.

Hash-and-Sign with eTCR and Weak Hashing

We propose this construction:



Theorem

Consider:

H_κ: an OW-eTCR hash function family

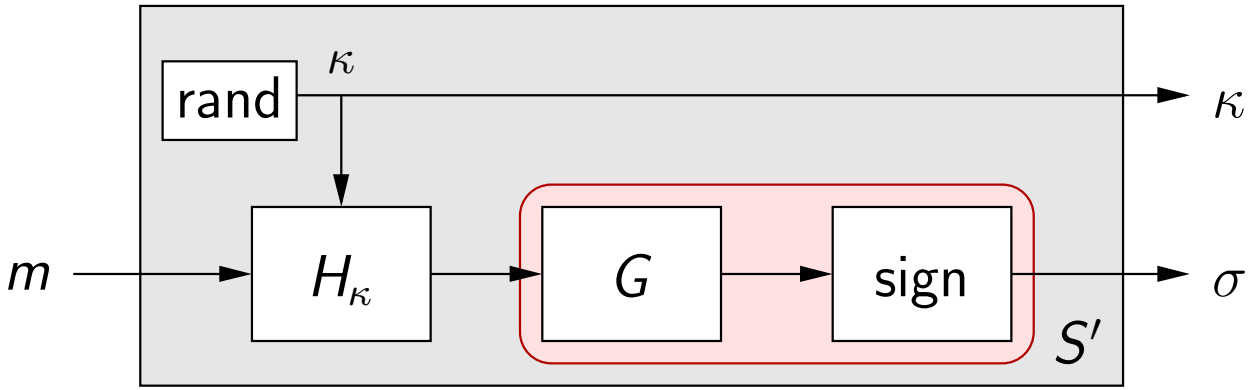
G: a preimage-tractable random oracle

If S_0 is weakly secure,

then S' is strongly secure.

Hash-and-Sign with eTCR and Weak Hashing

We propose this construction:



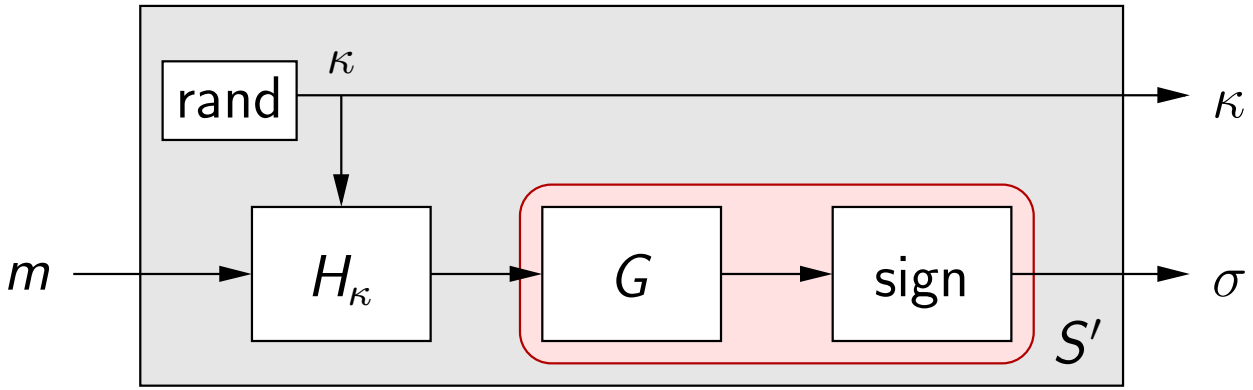
We only add an extra randomized preprocessing $H_\kappa(\cdot)$, and we recover the claimed security.

Price?

The signature enlarges.

Hash-and-Sign with eTCR and Weak Hashing

We propose this construction:



Is our goals fullfiled?

We were looking for a signature scheme which

- ✓ is provably secure
- ✓ in an better model than the random oracle model
- ✓ reuses actual implementations (preprocessing only)
- X does not enlarge the signature


The Entropy Recycling Technique

Definition

The idea of reusing randomness comes from Mironov.
He gave examples for DSA, RSA-PSS and Cramer-Shoup schemes.

Here,

- we formalize randomized signature schemes.
- we give a formal security proof for the generic case.

Signature with Randomized Precomputation

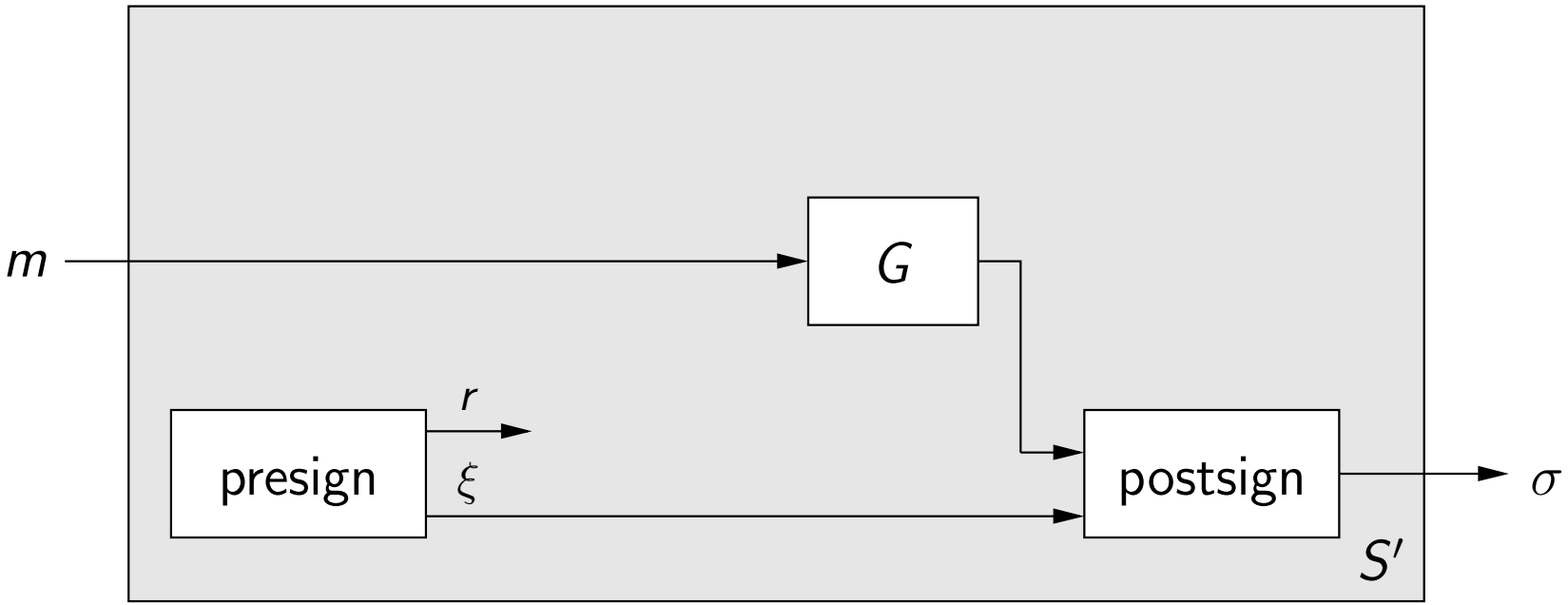
An SRP consists of five algorithms:

$$(K_p, K_s) \leftarrow \text{setup}()$$
$$(\xi, r) \leftarrow \text{presign}(K_s) \qquad r \leftarrow \text{extract}(K_p, \sigma)$$
$$\sigma \leftarrow \text{postsign}(K_s, m, \xi) \qquad b \leftarrow \text{verify}(K_p, m, \sigma)$$

All signature schemes can be written in this way (r can be void).

The Full Construction

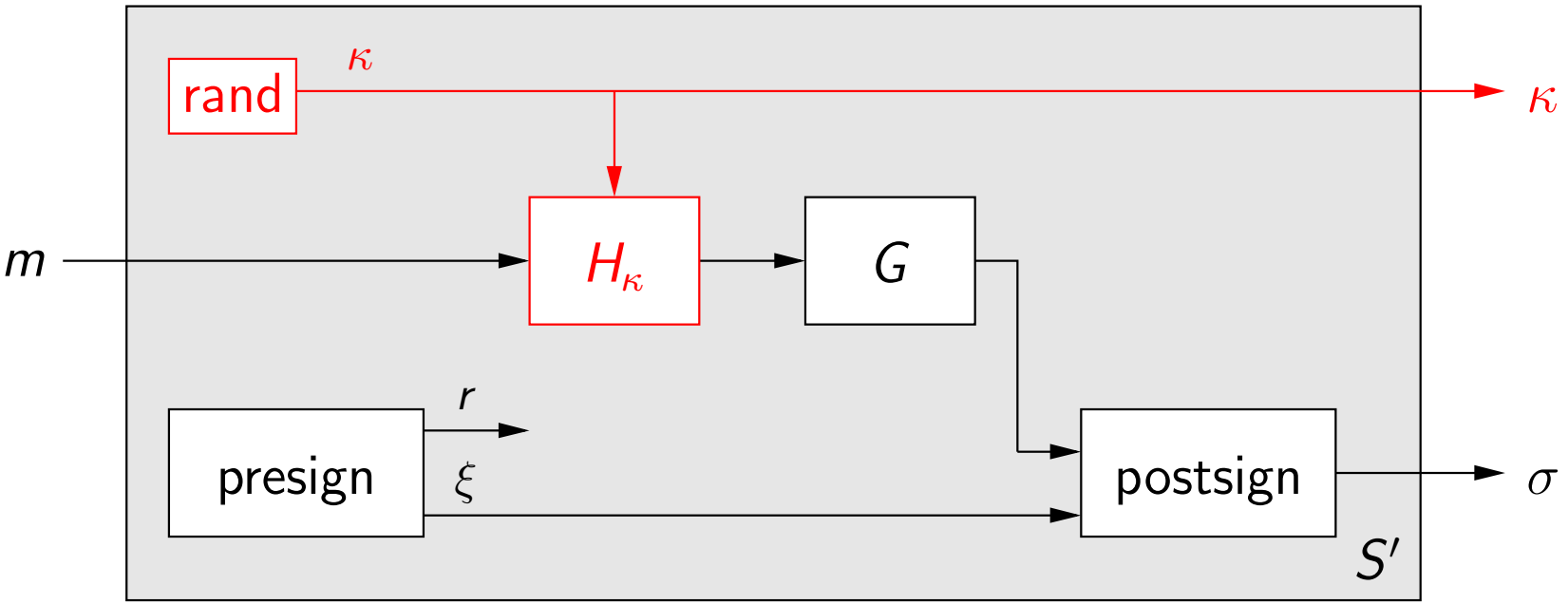
The standard implementations can be presented as follow:



Note that the presign algorithm can be empty.

The Full Construction

Our proposed construction with a random κ:

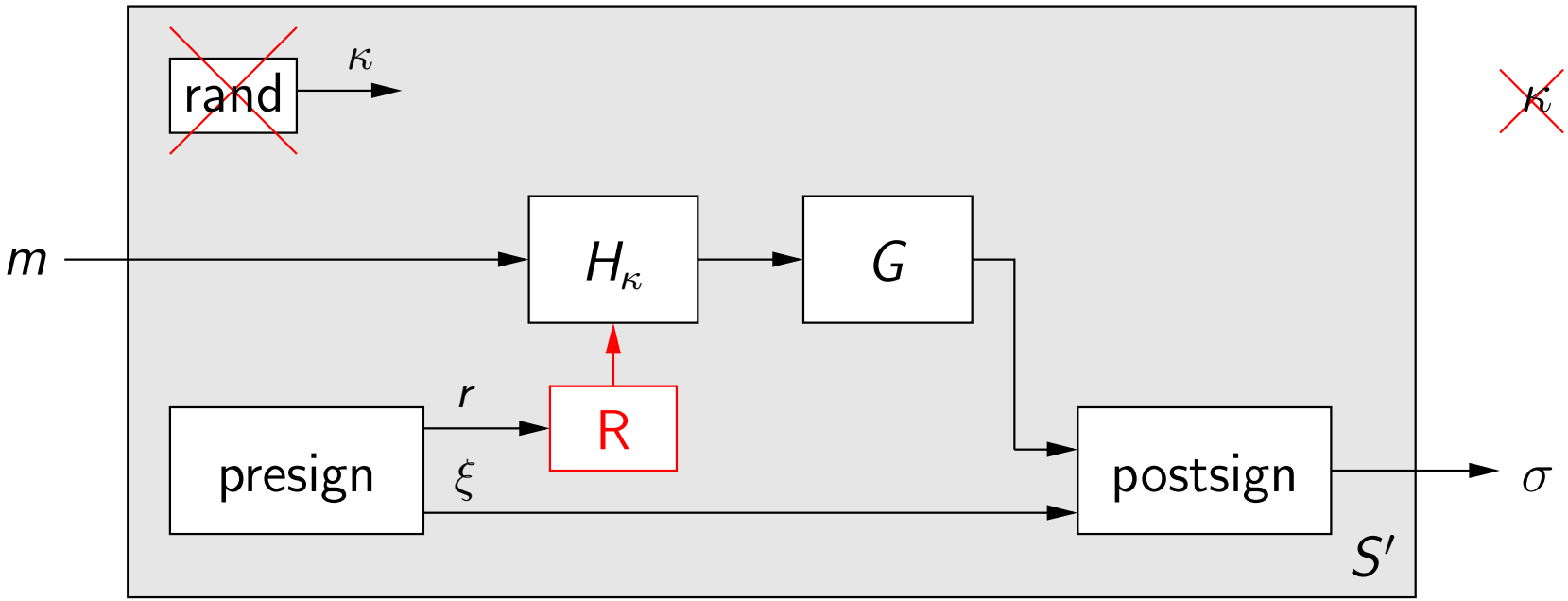


✓ This construction was proved strongly secure (previous slides)

X The signature length increases

The Full Construction

Reusing the randomness:

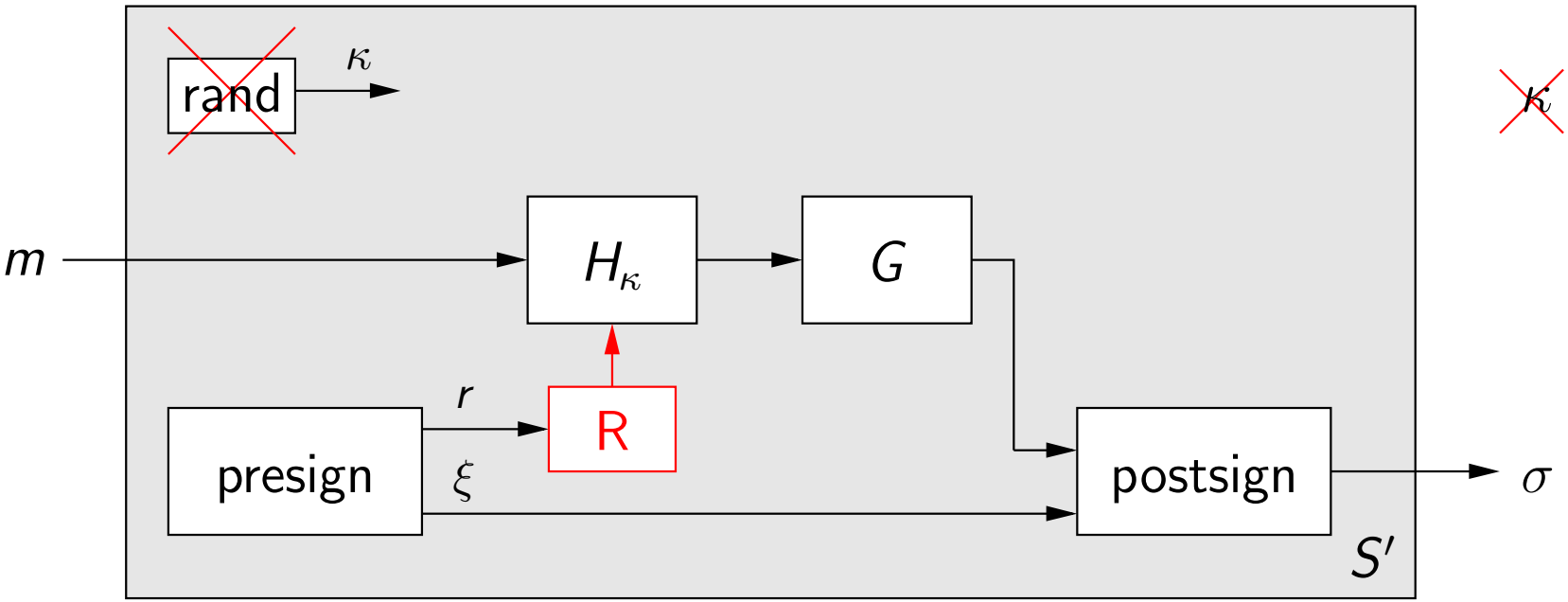


Theorem

If R is a random oracle and r has "enough" entropy,
then S' is strongly secure.

The Full Construction

Reusing the randomness:



✓ We solved the signature enlargement problem

X We introduced a random oracle


Conclusion

Conclusion

Consider any implementation S using the hash-and-sign with:

- a textbook signature scheme S_0,
- a collision-resistant hash function G,

Assume that

- S_0 is weakly secure,
- some weakness on G was reported.

Clearly, S is insecure.

Assuming G fit the weak hashing model:

- use the actual implementation S
- add an eTCR preprocssing on m, i.e. $H_\kappa(m)$

S becomes strongly secure.