Revisiting Security Relations Between Signature Schemes and their Inner Hash Functions

French Saphir Project (Cryptolog, DCSSI, Ecole Normale Supérieure, France Telecom and Gemalto)

Saphir Partners

Ecrypt Hash Workshop

Outline

1. Hash Functions in Cryptosystems
2. Security reductions
3. Hash Functions
4. Hash-and-Sign Signature Schemes
5. Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H
6. Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F
7. Merkle-Damgård Instantiations

Hash Functions in Cryptosystems

How do broken hash functions impact cryptosystems ?

Let $\mathcal{S} = \mathcal{S}[H_1, \ldots, H_n]$ be a cryptosystem based on hash functions $H_1, \ldots, H_n$. We want to explore the interplay between the security of $\mathcal{S}$ and the security of $H_1, \ldots, H_n$.

Connections between $\mathcal{S}$ and $H_1, \ldots, H_n$ are usually not understood

Hash Functions in Cryptosystems

How do broken hash functions impact cryptosystems ?

Let $\mathcal{S} = \mathcal{S}[H_1, \ldots, H_n]$ be a cryptosystem based on hash functions $H_1, \ldots, H_n$. We want to explore the interplay between the security of $\mathcal{S}$ and the security of $H_1, \ldots, H_n$.

Connections between $\mathcal{S}$ and $H_1, \ldots, H_n$ are usually not understood

OAEP padding

Hash Functions in Cryptosystems

How do broken hash functions impact cryptosystems ?

Let $\mathcal{S} = \mathcal{S}[H_1, \ldots, H_n]$ be a cryptosystem based on hash functions $H_1, \ldots, H_n$. We want to explore the interplay between the security of $\mathcal{S}$ and the security of $H_1, \ldots, H_n$.

Connections between $\mathcal{S}$ and $H_1, \ldots, H_n$ are usually not understood

OAEP padding

- used in conjunction with a trapdoor permutation to yield random-oracle secure encryption

Hash Functions in Cryptosystems

How do broken hash functions impact cryptosystems ?

Let $\mathcal{S} = \mathcal{S}[H_1, \ldots, H_n]$ be a cryptosystem based on hash functions $H_1, \ldots, H_n$. We want to explore the interplay between the security of $\mathcal{S}$ and the security of $H_1, \ldots, H_n$.

Connections between $\mathcal{S}$ and $H_1, \ldots, H_n$ are usually not understood

OAEP padding

- used in conjunction with a trapdoor permutation to yield random-oracle secure encryption
- uses two hash functions H_1, H_2

Hash Functions in Cryptosystems

How do broken hash functions impact cryptosystems?

Let $\mathcal{S} = \mathcal{S}[H_1, \ldots, H_n]$ be a cryptosystem based on hash functions $H_1, \ldots, H_n$. We want to explore the interplay between the security of $\mathcal{S}$ and the security of $H_1, \ldots, H_n$.

Connections between $\mathcal{S}$ and $H_1, \ldots, H_n$ are usually not understood

OAEP padding

- used in conjunction with a trapdoor permutation to yield random-oracle secure encryption
- uses two hash functions H_1, H_2
- proven IND-CCA secure $\equiv$ RSA in RO model, unlikely in plain model

Hash Functions in Cryptosystems

How do broken hash functions impact cryptosystems?

Let $\mathcal{S} = \mathcal{S}[H_1, \ldots, H_n]$ be a cryptosystem based on hash functions $H_1, \ldots, H_n$. We want to explore the interplay between the security of $\mathcal{S}$ and the security of $H_1, \ldots, H_n$.

Connections between $\mathcal{S}$ and $H_1, \ldots, H_n$ are usually not understood

OAEP padding

- used in conjunction with a trapdoor permutation to yield random-oracle secure encryption
- uses two hash functions H_1, H_2
- proven IND-CCA secure $\equiv$ RSA in RO model, unlikely in plain model
- Question : is OAEP secure when COL $[H_1] \equiv 0$?

Security Relations between $\mathcal{S}[H]$ and H

$\mathcal{S} = \mathcal{S}[H]$

We want to determine how the security of H relates to the one of $\mathcal{S}$

We see 4 types of connections

Security Relations between $\mathcal{S}[H]$ and H

$\mathcal{S} = \mathcal{S}[H]$

We want to determine how the security of H relates to the one of $\mathcal{S}$

We see 4 types of connections

Attack a reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$)

Security Relations between $\mathcal{S}[H]$ and H

$\mathcal{S} = \mathcal{S}[H]$

We want to determine how the security of H relates to the one of $\mathcal{S}$

We see 4 types of connections

Attack a reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (the reduction makes explicit how an attack of a given type on the hash function is enough to break the scheme in a prescribed way)

Security Relations between $\mathcal{S}[H]$ and H

$\mathcal{S} = \mathcal{S}[H]$

We want to determine how the security of H relates to the one of $\mathcal{S}$

We see 4 types of connections

Attack: a reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (the reduction makes explicit how an attack of a given type on the hash function is enough to break the scheme in a prescribed way)

Security Proof: a reduction Break(H) $\Leftarrow$ Break($\mathcal{S}$)

Security Relations between $\mathcal{S}[H]$ and H

$\mathcal{S} = \mathcal{S}[H]$

We want to determine how the security of H relates to the one of $\mathcal{S}$

We see 4 types of connections

Attack
: a reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (the reduction makes explicit how an attack of a given type on the hash function is enough to break the scheme in a prescribed way)

Security Proof
: a reduction Break(H) $\Leftarrow$ Break($\mathcal{S}$)

Impossible Attack
: there is no reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$)

Security Relations between $\mathcal{S}[H]$ and H

$\mathcal{S} = \mathcal{S}[H]$

We want to determine how the security of H relates to the one of $\mathcal{S}$

We see 4 types of connections

Attack
: a reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (the reduction makes explicit how an attack of a given type on the hash function is enough to break the scheme in a prescribed way)

Security Proof
: a reduction Break(H) $\Leftarrow$ Break($\mathcal{S}$)

Impossible Attack
: there is no reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (meta-reduction technique : if Break(H) $\Rightarrow_{\mathcal{R}}$ Break($\mathcal{S}$) then $\mathcal{R} \Rightarrow_{\mathcal{M}} P$ where P is auxiliary)

Security Relations between $\mathcal{S}[H]$ and H

$\mathcal{S} = \mathcal{S}[H]$

We want to determine how the security of H relates to the one of $\mathcal{S}$

We see 4 types of connections

- **Attack** a reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (the reduction makes explicit how an attack of a given type on the hash function is enough to break the scheme in a prescribed way)
- **Security Proof** a reduction Break(H) $\Leftarrow$ Break($\mathcal{S}$)
- **Impossible Attack** there is no reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (meta-reduction technique : if Break(H) $\Rightarrow_{\mathcal{R}}$ Break($\mathcal{S}$) then $\mathcal{R} \Rightarrow_{\mathcal{M}} P$ where P is auxiliary)
- **Impossibility of Security Proof** no reduction Break(H) $\Leftarrow$ Break($\mathcal{S}$)

Security Relations between $\mathcal{S}[H]$ and H

$\mathcal{S} = \mathcal{S}[H]$

We want to determine how the security of H relates to the one of $\mathcal{S}$

We see 4 types of connections

Attack: a reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (the reduction makes explicit how an attack of a given type on the hash function is enough to break the scheme in a prescribed way)

Security Proof: a reduction Break(H) $\Leftarrow$ Break($\mathcal{S}$)

Impossible Attack: there is no reduction Break(H) $\Rightarrow$ Break($\mathcal{S}$) (meta-reduction technique : if Break(H) $\Rightarrow_{\mathcal{R}}$ Break($\mathcal{S}$) then $\mathcal{R} \Rightarrow_{\mathcal{M}} P$ where P is auxiliary)

Impossibility of Security Proof: no reduction Break(H) $\Leftarrow$ Break($\mathcal{S}$)

So there are *positive* security results and *negative* security results.

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families
- Crystal clear classification of signatures

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families
- Crystal clear classification of signatures
  - deterministic versus probabilistic hash-and-sign signatures

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families
- Crystal clear classification of signatures
  - deterministic versus probabilistic hash-and-sign signatures
  - primitiveness

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families
- Crystal clear classification of signatures
  - deterministic versus probabilistic hash-and-sign signatures
  - primitiveness
  - injectivity

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families
- Crystal clear classification of signatures
    - deterministic versus probabilistic hash-and-sign signatures
    - primitiveness
    - injectivity
    - we capture all signature schemes we know of

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families
- Crystal clear classification of signatures
  - deterministic versus probabilistic hash-and-sign signatures
  - primitiveness
  - injectivity
  - we capture all signature schemes we know of
- Merkle-Damgård Instantiations

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families
- Crystal clear classification of signatures
  - deterministic versus probabilistic hash-and-sign signatures
  - primitiveness
  - injectivity
  - we capture all signature schemes we know of
- Merkle-Damgård Instantiations
  - identify more specific results in the case of functions such as MD5 and SHA-1

What We Do Here

Focus on public-key signatures

Connections $\mathcal{S}[H]/H$ heavily depend on the way $\mathcal{S}$ makes use of H

We clarify everything

- Suitable security notions for hash functions & HF families
- Crystal clear classification of signatures
  - deterministic versus probabilistic hash-and-sign signatures
  - primitiveness
  - injectivity
  - we capture all signature schemes we know of
- Merkle-Damgård Instantiations
  - identify more specific results in the case of functions such as MD5 and SHA-1
  - security gain inherent to using probabilistic hash-and-sign paradigm may be lost completely if unwise operating mode

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \longrightarrow \infty$) or concrete setting

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \longrightarrow \infty$) or concrete setting

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \longrightarrow \infty$) or concrete setting
  - given problem P, $\mathcal{A}$ (τ, ε)-solves or (τ, ε)-breaks P if $\mathcal{A}$ outputs a solution of P wrt τ, ε

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \longrightarrow \infty$) or concrete setting
  - given problem P, $\mathcal{A}$ (τ, ε)-solves or (τ, ε)-breaks P if $\mathcal{A}$ outputs a solution of P wrt τ, ε
  - τ relates to some fixed model of computation

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \to \infty$) or concrete setting
  - given problem P, $\mathcal{A}$ (τ, ε)-solves or (τ, ε)-breaks P if $\mathcal{A}$ outputs a solution of P wrt τ, ε
  - τ relates to some fixed model of computation
  - reduction $\mathcal{R}$ between two computational problems P_1 and P_2 is a probabilistic algorithm $\mathcal{R}$ which (τ_1, ε_1)-solves P_1 given black-box access to an oracle (τ_2, ε_2)-solving P_2

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \to \infty$) or concrete setting
  - given problem P, $\mathcal{A}$ (τ, ε)-solves or (τ, ε)-breaks P if $\mathcal{A}$ outputs a solution of P wrt τ, ε
  - τ relates to some fixed model of computation
  - reduction $\mathcal{R}$ between two computational problems P_1 and P_2 is a probabilistic algorithm $\mathcal{R}$ which (τ_1, ε_1)-solves P_1 given black-box access to an oracle (τ_2, ε_2)-solving P_2
  - $P_1 \leq_{\mathcal{R}} P_2$ when $\mathcal{R}$ is known to reduce P_1 to P_2 with $\tau_1 \simeq \tau_2$ and $\varepsilon_1 \simeq \varepsilon_2$

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \to \infty$) or concrete setting
  - given problem P, $\mathcal{A}$ (τ, ε)-solves or (τ, ε)-breaks P if $\mathcal{A}$ outputs a solution of P wrt τ, ε
  - τ relates to some fixed model of computation
  - reduction $\mathcal{R}$ between two computational problems P_1 and P_2 is a probabilistic algorithm $\mathcal{R}$ which (τ_1, ε_1)-solves P_1 given black-box access to an oracle (τ_2, ε_2)-solving P_2
  - $P_1 \leq_{\mathcal{R}} P_2$ when $\mathcal{R}$ is known to reduce P_1 to P_2 with $\tau_1 \simeq \tau_2$ and $\varepsilon_1 \simeq \varepsilon_2$
- black-box or non-black-box

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \longrightarrow \infty$) or concrete setting
  - given problem P, $\mathcal{A}$ (τ, ε)-solves or (τ, ε)-breaks P if $\mathcal{A}$ outputs a solution of P wrt τ, ε
  - τ relates to some fixed model of computation
  - reduction $\mathcal{R}$ between two computational problems P_1 and P_2 is a probabilistic algorithm $\mathcal{R}$ which (τ_1, ε_1)-solves P_1 given black-box access to an oracle (τ_2, ε_2)-solving P_2
  - $P_1 \leq_{\mathcal{R}} P_2$ when $\mathcal{R}$ is known to reduce P_1 to P_2 with $\tau_1 \simeq \tau_2$ and $\varepsilon_1 \simeq \varepsilon_2$
- black-box or non-black-box
- constructive or non constructive

Security Reductions

Different semantics of proofs

- polynomial setting ($\kappa \longrightarrow \infty$) or concrete setting
  - given problem P, $\mathcal{A}$ (τ, ε)-solves or (τ, ε)-breaks P if $\mathcal{A}$ outputs a solution of P wrt τ, ε
  - τ relates to some fixed model of computation
  - reduction $\mathcal{R}$ between two computational problems P_1 and P_2 is a probabilistic algorithm $\mathcal{R}$ which (τ_1, ε_1)-solves P_1 given black-box access to an oracle (τ_2, ε_2)-solving P_2
  - $P_1 \leq_{\mathcal{R}} P_2$ when $\mathcal{R}$ is known to reduce P_1 to P_2 with $\tau_1 \simeq \tau_2$ and $\varepsilon_1 \simeq \varepsilon_2$
- black-box or non-black-box
- constructive or non constructive

We only care about concrete, black-box, constructive reductions here :

$$P_1 \Leftarrow_R P_2 \,, \quad P_1 \Leftrightarrow P_2 \,, \quad etc.$$

Interpreting Security Reductions

Success in breaking P

We define $\mathsf{Succ}(P,\tau) = \max_{\mathcal{A}} \mathsf{Succ}^{P}(\mathcal{A},\tau)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\mathsf{Succ}(P,\tau)$ is a function here.

Interpreting Security Reductions

Success in breaking P

We define $\mathrm{Succ}\left(P,\tau\right) = \max_{\mathcal{A}} \mathrm{Succ}^{P}\left(\mathcal{A},\tau\right)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\mathrm{Succ}\left(P,\tau\right)$ is a function here.

What does a security reduction mean ?

Interpreting Security Reductions

Success in breaking P

We define $\mathrm{Succ}\,(P, \tau) = \max_{\mathcal{A}} \mathrm{Succ}^{P}\,(\mathcal{A}, \tau)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\mathrm{Succ}\,(P, \tau)$ is a function here.

What does a security reduction mean ?

- take $P_1 = \mathrm{Break}(\mathcal{S}_1)$ and $P_2 = \mathrm{Break}(\mathcal{S}_2)$

Interpreting Security Reductions

Success in breaking P

We define $\mathrm{Succ}\left(P,\tau\right) = \max_{\mathcal{A}} \mathrm{Succ}^{P}\left(\mathcal{A},\tau\right)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\mathrm{Succ}\left(P,\tau\right)$ is a function here.

What does a security reduction mean ?

- take $P_1 = \mathrm{Break}(\mathcal{S}_1)$ and $P_2 = \mathrm{Break}(\mathcal{S}_2)$
- assume you find $\mathcal{R}$ such that $\mathrm{Break}(\mathcal{S}_1) \Leftarrow_{\mathcal{R}} \mathrm{Break}(\mathcal{S}_2)$

Interpreting Security Reductions

Success in breaking P

We define $\mathsf{Succ}\left(P, \tau\right) = \max_{\mathcal{A}} \mathsf{Succ}^{P}\left(\mathcal{A}, \tau\right)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\mathsf{Succ}\left(P, \tau\right)$ is a function here.

What does a security reduction mean ?

- take $P_1 = \mathsf{Break}(\mathcal{S}_1)$ and $P_2 = \mathsf{Break}(\mathcal{S}_2)$
- assume you find $\mathcal{R}$ such that $\mathsf{Break}(\mathcal{S}_1) \Leftarrow_{\mathcal{R}} \mathsf{Break}(\mathcal{S}_2)$
- this means $\mathsf{Succ}\left(\mathsf{Break}(\mathcal{S}_1), \tau_1\right) \geq \mathsf{Succ}\left(\mathsf{Break}(\mathcal{S}_2), \tau_2\right)$ for $\tau_1 \simeq \tau_2$

Interpreting Security Reductions

Success in breaking P

We define $\mathrm{Succ}\,(P, \tau) = \max_{\mathcal{A}} \mathrm{Succ}^{P}\,(\mathcal{A}, \tau)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\mathrm{Succ}\,(P, \tau)$ is a function here.

What does a security reduction mean ?

- take $P_1 = \mathrm{Break}(\mathcal{S}_1)$ and $P_2 = \mathrm{Break}(\mathcal{S}_2)$
- assume you find $\mathcal{R}$ such that $\mathrm{Break}(\mathcal{S}_1) \Leftarrow_{\mathcal{R}} \mathrm{Break}(\mathcal{S}_2)$
- this means $\mathrm{Succ}\,(\mathrm{Break}(\mathcal{S}_1), \tau_1) \geq \mathrm{Succ}\,(\mathrm{Break}(\mathcal{S}_2), \tau_2)$ for $\tau_1 \simeq \tau_2$

What happens if $\mathrm{Break}(\mathcal{S}_1)$ has no solution ?

Well then $\mathcal{S}_1$ is perfectly (IT) secure, and so must be $\mathcal{S}_2$

Interpreting Security Reductions

Success in breaking P

We define $\text{Succ}\left(P,\tau\right) = \max_{\mathcal{A}} \text{Succ}^{P}\left(\mathcal{A},\tau\right)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\text{Succ}\left(P,\tau\right)$ is a function here.

What does a security reduction mean ?

- take $P_1 = \text{Break}(\mathcal{S}_1)$ and $P_2 = \text{Break}(\mathcal{S}_2)$
- assume you find $\mathcal{R}$ such that $\text{Break}(\mathcal{S}_1) \Leftarrow_{\mathcal{R}} \text{Break}(\mathcal{S}_2)$
- this means $\text{Succ}\left(\text{Break}(\mathcal{S}_1),\tau_1\right) \geq \text{Succ}\left(\text{Break}(\mathcal{S}_2),\tau_2\right)$ for $\tau_1 \simeq \tau_2$

What happens if $\text{Break}(\mathcal{S}_2)$ has no solution ?

Then the reduction just tells us $\text{Succ}\left(\text{Break}(\mathcal{S}_1)\right) \geq 0$, no big deal

Interpreting Security Reductions

Success in breaking P

We define $\mathrm{Succ}\left(P, \tau\right) = \max_{\mathcal{A}} \mathrm{Succ}^{P}\left(\mathcal{A}, \tau\right)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\mathrm{Succ}\left(P, \tau\right)$ is a function here.

What does a security reduction mean ?

- take $P_1 = \mathrm{Break}(\mathcal{S}_1)$ and $P_2 = \mathrm{Break}(\mathcal{S}_2)$
- assume you find $\mathcal{R}$ such that $\mathrm{Break}(\mathcal{S}_1) \Leftarrow_{\mathcal{R}} \mathrm{Break}(\mathcal{S}_2)$
- this means $\mathrm{Succ}\left(\mathrm{Break}(\mathcal{S}_1), \tau_1\right) \geq \mathrm{Succ}\left(\mathrm{Break}(\mathcal{S}_2), \tau_2\right)$ for $\tau_1 \simeq \tau_2$

Interpreting Security Reductions

Success in breaking P

We define $\mathrm{Succ}\,(P, \tau) = \max_{\mathcal{A}} \mathrm{Succ}^{P}\,(\mathcal{A}, \tau)$ taken over all τ-time probabilistic $\mathcal{A}$'s. $\mathrm{Succ}\,(P, \tau)$ is a function here.

What does a security reduction mean ?

- take $P_1 = \mathrm{Break}(\mathcal{S}_1)$ and $P_2 = \mathrm{Break}(\mathcal{S}_2)$
- assume you find $\mathcal{R}$ such that $\mathrm{Break}(\mathcal{S}_1) \Leftarrow_{\mathcal{R}} \mathrm{Break}(\mathcal{S}_2)$
- this means $\mathrm{Succ}\,(\mathrm{Break}(\mathcal{S}_1), \tau_1) \geq \mathrm{Succ}\,(\mathrm{Break}(\mathcal{S}_2), \tau_2)$ for $\tau_1 \simeq \tau_2$

What happens if $\mathrm{Break}(\mathcal{S}_1)$ always has a solution ?

Then

$$\mathrm{Succ}\,(\mathrm{Break}(\mathcal{S}_1), \tau) = 1 \quad \text{for any } \tau$$

No big deal, restrict maximum on known adversaries $\mathcal{A}$

Hash Functions

Hash function

A function H is a hash function if it maps $\{0,1\}^*$ to $\{0,1\}^{\mathrm{m}}$ for some integer $\mathrm{m} > 0$ called the output size of H.

Compression function

A compression function is a function $f : \{0,1\}^{\mathrm{m}} \times \{0,1\}^{\mathrm{b}} \rightarrow \{0,1\}^{\mathrm{m}}$ where m, b are integers such that $\mathrm{m} > 0$ and $\mathrm{b} > 0$.

SAPHIR

Hash Functions

Hash function

A function H is a hash function if it maps $\{0,1\}^*$ to $\{0,1\}^{\mathrm{m}}$ for some integer $\mathrm{m} > 0$ called the output size of H.

Compression function

A compression function is a function $f : \{0,1\}^{\mathrm{m}} \times \{0,1\}^{\mathrm{b}} \to \{0,1\}^{\mathrm{m}}$ where m, b are integers such that $\mathrm{m} > 0$ and $\mathrm{b} > 0$.

Iterated hashing allows to build “H from f”

Security Notions for Hash Functions

Collision-resistance $\mathrm{COL}^{n_1,n_2}[H]$ Find $M_1 \in \{0,1\}^{n_1}$ and $M_2 \in \{0,1\}^{n_2}$ such that $M_1 \neq M_2$ and $H(M_1) = H(M_2)$. We know that $\mathrm{Succ}\left(\mathrm{COL}^{n_1,n_2}[H]\right) = 1$ or 0

Security Notions for Hash Functions

Collision-resistance $\mathrm{COL}^{n_1,n_2}[H]$ Find $M_1 \in \{0,1\}^{n_1}$ and $M_2 \in \{0,1\}^{n_2}$ such that $M_1 \neq M_2$ and $H(M_1) = H(M_2)$. We know that $\mathrm{Succ}\left(\mathrm{COL}^{n_1,n_2}[H]\right) = 1$ or 0

Second-preimage-resistance $\mathrm{SEC}_{n_1}^{n_2}[H]$ Given a random $M_1 \leftarrow \{0,1\}^{n_1}$, find $M_2 \in \{0,1\}^{n_2}$ such that $H(M_2) = H(M_1)$ and $M_2 \neq M_1$

Security Notions for Hash Functions

Collision-resistance $\mathrm{COL}^{n_1,n_2}[H]$ Find $M_1 \in \{0,1\}^{n_1}$ and $M_2 \in \{0,1\}^{n_2}$ such that $M_1 \neq M_2$ and $H(M_1) = H(M_2)$. We know that $\mathrm{Succ}\left(\mathrm{COL}^{n_1,n_2}[H]\right) = 1$ or 0

Second-preimage-resistance $\mathrm{SEC}_{n_1}^{n_2}[H]$ Given a random $M_1 \leftarrow \{0,1\}^{n_1}$, find $M_2 \in \{0,1\}^{n_2}$ such that $H(M_2) = H(M_1)$ and $M_2 \neq M_1$

Preimage-resistance Well, (at least) two notions :

Security Notions for Hash Functions

Collision-resistance $\mathrm{COL}^{n_1,n_2}[H]$ Find $M_1 \in \{0,1\}^{n_1}$ and $M_2 \in \{0,1\}^{n_2}$ such that $M_1 \neq M_2$ and $H(M_1) = H(M_2)$. We know that $\mathrm{Succ}\left(\mathrm{COL}^{n_1,n_2}[H]\right) = 1$ or 0

Second-preimage-resistance $\mathrm{SEC}_{n_1}^{n_2}[H]$ Given a random $M_1 \leftarrow \{0,1\}^{n_1}$, find $M_2 \in \{0,1\}^{n_2}$ such that $H(M_2) = H(M_1)$ and $M_2 \neq M_1$

Preimage-resistance Well, (at least) two notions :

$\overline{\mathrm{PRE}}_{n_1}^{n_2}[H]$ Given a random $M_1 \leftarrow \{0,1\}^{n_1}$, take $m = H(M_1)$ and find an n_2-bit string M_2 such that $H(M_2) = m$

Security Notions for Hash Functions

Collision-resistance $\mathrm{COL}^{n_1,n_2}[H]$ Find $M_1 \in \{0,1\}^{n_1}$ and $M_2 \in \{0,1\}^{n_2}$ such that $M_1 \neq M_2$ and $H(M_1) = H(M_2)$. We know that $\mathrm{Succ}\left(\mathrm{COL}^{n_1,n_2}[H]\right) = 1$ or 0

Second-preimage-resistance $\mathrm{SEC}_{n_1}^{n_2}[H]$ Given a random $M_1 \leftarrow \{0,1\}^{n_1}$, find $M_2 \in \{0,1\}^{n_2}$ such that $H(M_2) = H(M_1)$ and $M_2 \neq M_1$

Preimage-resistance Well, (at least) two notions :

- $\overline{\mathrm{PRE}}_{n_1}^{n_2}[H]$ Given a random $M_1 \leftarrow \{0,1\}^{n_1}$, take $m = H(M_1)$ and find an n_2-bit string M_2 such that $H(M_2) = m$
- $\mathrm{PRE}^{n}[H]$ Given a random $m \leftarrow \{0,1\}^{\mathrm{m}}$, find an n-bit string M such that $H(M) = m$.

Security Notions for Hash Functions

Collision-resistance $\mathrm{COL}^{n_1,n_2}[H]$ Find $M_1 \in \{0,1\}^{n_1}$ and $M_2 \in \{0,1\}^{n_2}$ such that $M_1 \neq M_2$ and $H(M_1) = H(M_2)$. We know that $\mathrm{Succ}\left(\mathrm{COL}^{n_1,n_2}[H]\right) = 1$ or 0

Second-preimage-resistance $\mathrm{SEC}_{n_1}^{n_2}[H]$ Given a random $M_1 \leftarrow \{0,1\}^{n_1}$, find $M_2 \in \{0,1\}^{n_2}$ such that $H(M_2) = H(M_1)$ and $M_2 \neq M_1$

Preimage-resistance Well, (at least) two notions :

$\overline{\mathrm{PRE}}_{n_1}^{n_2}[H]$ Given a random $M_1 \leftarrow \{0,1\}^{n_1}$, take $m = H(M_1)$ and find an n_2-bit string M_2 such that $H(M_2) = m$

$\mathrm{PRE}^{n}[H]$ Given a random $m \leftarrow \{0,1\}^{\mathrm{m}}$, find an n-bit string M such that $H(M) = m$.
Most efficient definition for security statements

Security Profile of a Hash Function

Let $H : \{0,1\}^* \rightarrow \{0,1\}^{\mathrm{m}}$ be a hash function.

Then for any $n_1, n_2 > 0$,

$$\begin{array}{ccccc} \mathrm{COL}^{n_1,n_2}[H] & \Leftarrow & \mathrm{SEC}_{n_1}^{n_2}[H] & \Leftarrow^{(1)} & \overline{\mathrm{PRE}}_{n_1}^{n_2}[H] \\ & & & & \Updownarrow^{(2)} \\ & & & & \mathrm{PRE}^{n_2}[H] \end{array}$$

(1) only if $n_2 \gg \mathrm{m}$

(2) when H is well-balanced

Hash Function Family

Hash function family

A hash function family F is a function $F : \{0,1\}^* \times \{0,1\}^{\mathrm{r}} \rightarrow \{0,1\}^{\mathrm{m}}$ for integers $\mathrm{m}, \mathrm{r} > 0$

We find definitions of interest for provable security :

E-COL^{n_1,n_2} $[F]$

Find (M_1, M_2, r) with $F(M_1, r) = F(M_2, r)$

U-COL^{n_1,n_2} $[F]$

Given $r \leftarrow \{0,1\}^{\mathrm{r}}$, find (M_1, M_2) with $F(M_1, r) = F(M_2, r)$

A-COL^{n_1,n_2} $[F]$

Find (M_1, M_2) with $F(M_1, r) = F(M_2, r)$ **for any** r

Security Notions for HF Families

Forms of second preimage resistance :

E-SEC$^{n_2}_{n_1}[F]$	Given $M_1 \leftarrow \{0,1\}^{n_1}$, find (M_2, r) with $F(M_1, r) = F(M_2, r)$
U-SEC$^{n_2}_{n_1}[F]$	Given $M_1 \leftarrow \{0,1\}^{n_1}$ and $r \leftarrow \{0,1\}^{\mathrm{r}}$, find M_2 with $F(M_1, r) = F(M_2, r)$
A-SEC$^{n_2}_{n_1}[F]$	Given $M_1 \leftarrow \{0,1\}^{n_1}$, find M_2 with $F(M_1, r) = F(M_2, r)$ **for any** r

Forms of preimage resistance :

E-PRE$^n[F]$	Given $m \leftarrow \{0,1\}^{\mathrm{m}}$, find (M, r) such that $F(M, r) = m$
U-PRE$^n[F]$	Given $m \leftarrow \{0,1\}^{\mathrm{m}}$ and $r \leftarrow \{0,1\}^{\mathrm{r}}$, find M such that $F(M, r) = m$

Can make use of [RS04] where $M \leftarrow \{0,1\}^*$ and $m = H(M)$ is given to adversary

Security Profile of a Hash Function Family

$$
\begin{array}{ccccc}
\text{E-PRE}^{n_2}[F] & \Leftarrow & \text{U-PRE}^{n_2}[F] & & \\
\Downarrow^{(1)} & & \Downarrow^{(1)} & & \\
\text{E-SEC}_{n_1}^{n_2}[F] & \Leftarrow & \text{U-SEC}_{n_1}^{n_2}[F] & \Leftarrow & \text{A-SEC}_{n_1}^{n_2}[F] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\text{E-COL}^{n_1,n_2}[F] & \Leftarrow & \text{U-COL}^{n_1,n_2}[F] & \Leftarrow & \text{A-COL}^{n_1,n_2}[F]
\end{array}
$$

(1) if F is well balanced on average over $r \leftarrow \{0,1\}^{\mathrm{r}}$

Signature Schemes

$\mathcal{S} \triangleq (\mathcal{S}.\mathrm{Gen}, \mathcal{S}.\mathrm{Sign}, \mathcal{S}.\mathrm{Ver})$ with message space $\mathcal{M} \subseteq \{0,1\}^*$:

Key Gen. $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathcal{S}.\mathrm{Gen}()$

Sign. given message $M \in \mathcal{M}$

pick $u \leftarrow \{0,1\}^{\mathrm{u}}$ then $\sigma = \mathcal{S}.\mathrm{Sign}(\mathrm{sk}, M, u)$

Verify. $\mathcal{S}.\mathrm{Ver}(\mathrm{pk}, M, \sigma)$ outputs $0/1$

Message space can be

- $\mathcal{M} = \{0,1\}^{\mathrm{m}}$ or
- $\mathcal{M} = \{0,1\}^*$

Security Notions

Forms of Unforgeability :

- $\mathrm{UF}_n\text{-KOA}\,[\mathcal{S}]$ Given $\mathsf{pk} \leftarrow \mathcal{S}.\mathsf{Gen}()$ and $M \leftarrow \{0,1\}^n$, get $\sigma = \mathcal{S}.\mathsf{Sign}(\mathsf{sk}, M, u)$
- $\mathrm{EF}^n\text{-KOA}\,[\mathcal{S}]$ Given $\mathsf{pk} \leftarrow \mathcal{S}.\mathsf{Gen}()$, get (M, σ) where $M \in \{0,1\}^n$ and $\sigma = \mathcal{S}.\mathsf{Sign}(\mathsf{sk}, M, u)$
- KMA_n You are given a list of (M_i, σ_i) where $M_i \leftarrow \{0,1\}^n$ and $u_i \leftarrow \{0,1\}^{\mathsf{u}}$
- CMA You have access to signing oracle

Forms of Non-Repudiation :

- $\mathrm{ER}_{n_1}^{n_2}\,[\mathcal{S}]$ Given $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{S}.\mathsf{Gen}()$, find $(M_1, M_2, \sigma_1 = \sigma_2)$
- $\mathrm{UR}_{n_1}^{n_2}\,[\mathcal{S}]$ Given $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{S}.\mathsf{Gen}()$ and $M_1 \leftarrow \{0,1\}^{n_1}$, find $M_2 \in \{0,1\}^{n_2}$ and σ

Security Profile of Signatures

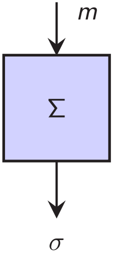
$$\begin{array}{ccccc}
\mathsf{UF}_{n_1}\text{-}\mathsf{CMA}\,[\mathcal{S}] & \Leftarrow & \mathsf{UF}_{n_1}\text{-}\mathsf{KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathsf{UF}_{n_1}\text{-}\mathsf{KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\mathsf{EF}^{n_1}\text{-}\mathsf{CMA}\,[\mathcal{S}] & \Leftarrow & \mathsf{EF}^{n_1}\text{-}\mathsf{KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathsf{EF}^{n_1}\text{-}\mathsf{KOA}\,[\mathcal{S}]
\end{array}$$

$$\begin{array}{c}
\mathsf{UR}_{n_1}^{n_2}\,[\mathcal{S}]\,,\,\mathsf{UR}_{n_2}^{n_1}\,[\mathcal{S}] \\
\Downarrow \\
\mathsf{ER}^{n_1,n_2}\,[\mathcal{S}]
\end{array}$$

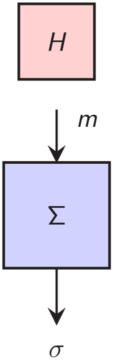
Deterministic Hash-and-Sign Signatures

Given

- Σ signing m-bit messages under u bits of randomness



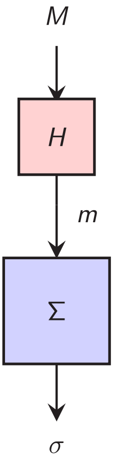
Deterministic Hash-and-Sign Signatures



Given

- Σ signing m-bit messages under u bits of randomness
- a hash function $H : \{0,1\}^* \rightarrow \{0,1\}^{\mathrm{m}}$

Deterministic Hash-and-Sign Signatures

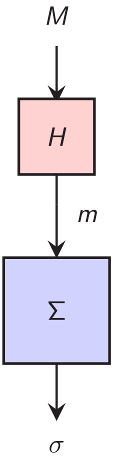


Given

- Σ signing m-bit messages under u bits of randomness
- a hash function $H : \{0,1\}^* \to \{0,1\}^{\mathrm{m}}$

we construct $\mathcal{S} = \langle H, \Sigma \rangle$ where

Deterministic Hash-and-Sign Signatures



Given

- Σ signing m-bit messages under u bits of randomness
- a hash function $H : \{0,1\}^* \to \{0,1\}^{\mathsf{m}}$

we construct $\mathcal{S} = \langle H, \Sigma \rangle$ where

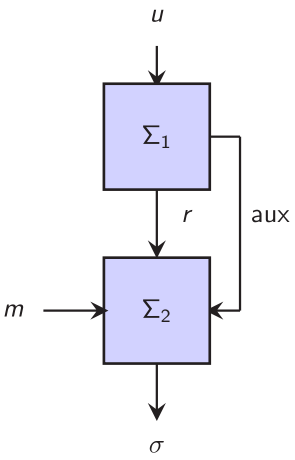
Key Gen. $\mathcal{S}.\mathsf{Gen} \triangleq \Sigma.\mathsf{Gen}$

Sign. given $M \in \{0,1\}^*$

- pick $u \leftarrow \{0,1\}^{\mathsf{u}}$
- $m = H(M)$
- $\sigma = \Sigma.\mathsf{Sign}(\mathsf{sk}, m, u)$

Verify. $\mathcal{S}.\mathsf{Ver}(\mathsf{pk}, M, \sigma)$ outputs $\Sigma.\mathsf{Ver}(\mathsf{pk}, H(M), \sigma)$

Two-Step Signatures



Σ can be split into four functions

$$\Sigma_1, \Sigma_2, \Upsilon_1, \Upsilon_2$$

To sign :

pick $u \leftarrow \{0,1\}^{\mathsf{u}}$

Step 1. $(r, \mathsf{aux}) = \Sigma_1(\mathsf{sk}, u)$

Step 2. $\sigma = \Sigma_2(\mathsf{sk}, m, r, \mathsf{aux})$

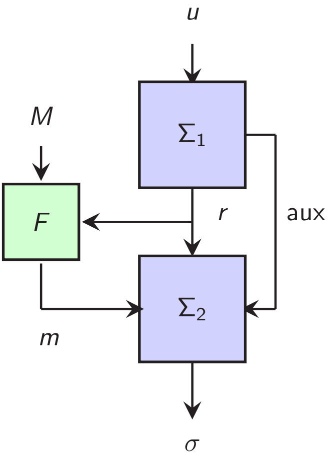
To verify :

Step 1. $\hat{r} = \Upsilon_1(\mathsf{pk}, \sigma)$

Step 2. output $\Upsilon_2(\mathsf{pk}, m, \sigma, \hat{r})$

If σ is valid then $\hat{r} = r$ is unique and r must be uniform over $\{0,1\}^{\mathsf{r}}$ if u is uniform over $\{0,1\}^{\mathsf{u}}$

Probabilistic Hash-and-Sign Signatures



We assemble Σ and F to build $\mathcal{S} = \langle F, \Sigma \rangle$

To sign :

pick $u \leftarrow \{0,1\}^{\mathsf{u}}$

Step 1. $(r, \mathsf{aux}) = \Sigma_1(\mathsf{sk}, u)$

$m = F(M, r)$

Step 2. $\sigma = \Sigma_2(\mathsf{sk}, m, r, \mathsf{aux})$

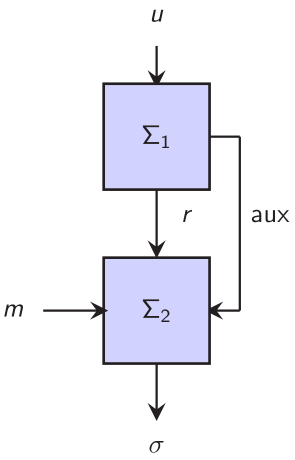
To verify :

Step 1. $\hat{r} = \Upsilon_1(\mathsf{pk}, \sigma)$

$\hat{m} = F(M, \hat{r})$

Step 2. output $\Upsilon_2(\mathsf{pk}, m, \sigma, \hat{r})$

Primitiveness of $\mathcal{S} = \langle F, \Sigma \rangle$



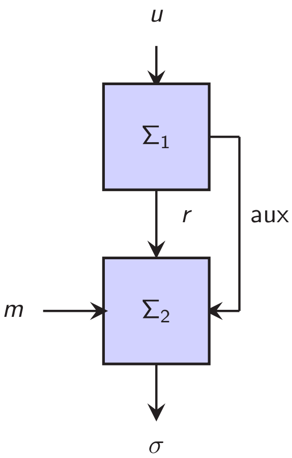
We know a probabilistic algorithm $\mathcal{S}$.Prim which

- for any key pair (pk, sk)
- given pk only
- generates a random pair

$$\left(m, \sigma = \Sigma.\mathrm{Sign}(\mathrm{sk}, m, u)\right)$$

- m is uniformly distributed over $\{0,1\}^{\mathrm{m}}$
- u is uniformly distributed over $\{0,1\}^{\mathrm{u}}$

Injectivity of $\mathcal{S} = \langle F, \Sigma \rangle$



$\mathcal{S}$ is injective when

- for any key pair $(\mathsf{pk}, \mathsf{sk})$
- for any $\sigma \in \{0,1\}^{\mathsf{s}}$
- there exists at most one pair

$$(m, r) \in \{0,1\}^{\mathsf{m}} \times \{0,1\}^{\mathsf{r}}$$

such that

- $\sigma = \Sigma_2(\mathsf{sk}, m, r, \mathsf{aux})$ and $(r, \mathsf{aux}) = \Sigma_1(\mathsf{sk}, u)$ for some u, aux

Classifying Common Signature Schemes

SIGNATURE SCHEME	*Det. H&S*	*Prob. H&S*	*Primitive*	*Injective*
Schnorr		×	×	×
FDH	×		×	×
PFDH		×	×	×
PSS		×	×	×
EMSA-PSS	×		×	×
BLS	×		×	×
Generic DSA	×			×
GHR	×			×
CS	×			

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Breaking $\mathcal{S}$ by breaking H : attacks

$$
\begin{array}{ccccc}
\mathrm{UF}_{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\mathrm{EF}^{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-KOA}\,[\mathcal{S}]
\end{array}
$$

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Breaking $\mathcal{S}$ by breaking H : attacks

$$
\begin{array}{ccccc}
\mathrm{UF}_{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\color{red}{\mathrm{EF}^{n_1}\text{-CMA}\,[\mathcal{S}]} & \Leftarrow & \mathrm{EF}^{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-KOA}\,[\mathcal{S}] \\
\color{red}{\Uparrow} & & & & \\
\mathrm{COL}^{n_1,n_2}\,[H] & & & &
\end{array}
$$

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Breaking $\mathcal{S}$ by breaking H : attacks

$$
\begin{array}{ccccc}
\mathrm{SEC}_{n_1}^{n_2}[H] & & & & \\
\Downarrow & & & & \\
\mathrm{UF}_{n_1}\text{-}\mathrm{CMA}[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-}\mathrm{KMA}_{n_2}[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-}\mathrm{KOA}[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\mathrm{EF}^{n_1}\text{-}\mathrm{CMA}[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-}\mathrm{KMA}_{n_2}[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-}\mathrm{KOA}[\mathcal{S}] \\
\Uparrow & & & & \\
\mathrm{COL}^{n_1,n_2}[H] & & & &
\end{array}
$$

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Breaking $\mathcal{S}$ by breaking H : attacks

$$
\begin{array}{ccccc}
\mathrm{SEC}_{n_1}^{n_2}\,[H] & & & & \\
\color{red}{\Downarrow} & & & & \\
\mathrm{UF}_{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\mathrm{EF}^{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \color{red}{\mathrm{EF}^{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}]} & \Leftarrow & \mathrm{EF}^{n_1}\text{-KOA}\,[\mathcal{S}] \\
\color{red}{\Uparrow} & & \color{red}{\Uparrow} & & \\
\mathrm{COL}^{n_1,n_2}\,[H] & & \mathrm{SEC}_{n_2}^{n_1}\,[H] & &
\end{array}
$$

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Breaking $\mathcal{S}$ by breaking H : attacks

$$
\begin{array}{ccccc}
\mathrm{SEC}_{n_1}^{n_2}[H] & & & & \\
\Downarrow & & & & \\
\mathrm{UF}_{n_1}\text{-}\mathrm{CMA}[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-}\mathrm{KMA}_{n_2}[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-}\mathrm{KOA}[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\mathrm{EF}^{n_1}\text{-}\mathrm{CMA}[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-}\mathrm{KMA}_{n_2}[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-}\mathrm{KOA}[\mathcal{S}] \\
\Uparrow & & \Uparrow & & \Uparrow^{(1)} \\
\mathrm{COL}^{n_1,n_2}[H] & & \mathrm{SEC}_{n_2}^{n_1}[H] & & \mathrm{PRE}^{n_1}[H]
\end{array}
$$

(1) if $\mathcal{S}$ is primitive

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Breaking $\mathcal{S}$ by breaking H : attacks

$$
\begin{array}{ccccc}
\mathrm{SEC}_{n_1}^{n_2}\,[H] & & \mathrm{PRE}^{n_1}\,[H] & & \mathrm{PRE}^{n_1}\,[H] \\
\Downarrow & & \Downarrow ??? & & \Downarrow ??? \\
\mathrm{UF}_{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\mathrm{EF}^{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Uparrow & & \Uparrow & & \Uparrow^{(1)} \\
\mathrm{COL}^{n_1,n_2}\,[H] & & \mathrm{SEC}_{n_2}^{n_1}\,[H] & & \mathrm{PRE}^{n_1}\,[H]
\end{array}
$$

(1) if $\mathcal{S}$ is primitive

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Repudiation : attacks...

$$\mathrm{UR}_{n_1}^{n_2}[\mathcal{S}]$$

$$\Downarrow$$

$$\mathrm{ER}^{n_1,n_2}[\mathcal{S}]$$

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Repudiation : attacks...

$$\mathrm{UR}_{n_1}^{n_2}\,[\mathcal{S}]$$

$$\Downarrow$$

$$\mathrm{ER}^{n_1,n_2}\,[\mathcal{S}]$$

$$\Uparrow$$

$$\mathrm{COL}^{n_1,n_2}\,[H]$$

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Repudiation : attacks...

$$\mathrm{SEC}_{n_1}^{n_2}\,[H]$$

$$\Downarrow$$

$$\mathrm{UR}_{n_1}^{n_2}\,[\mathcal{S}]$$

$$\Downarrow$$

$$\mathrm{ER}^{n_1,n_2}\,[\mathcal{S}]$$

$$\Uparrow$$

$$\mathrm{COL}^{n_1,n_2}\,[H]$$

Relations between $\mathcal{S} = \langle H, \Sigma \rangle$ and H

Repudiation : attacks. . .and security proofs

$$\mathrm{SEC}_{n_1}^{n_2}[H]$$

$$\Updownarrow^{(2)}$$

$$\mathrm{UR}_{n_1}^{n_2}[\mathcal{S}]$$

$$\Downarrow$$

$$\mathrm{ER}^{n_1,n_2}[\mathcal{S}]$$

$$\Updownarrow^{(2)}$$

$$\mathrm{COL}^{n_1,n_2}[H]$$

(2) if $\mathcal{S}$ is injective

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Breaking $\mathcal{S}$ by breaking F : attacks again

$$\begin{array}{ccccc}
\mathrm{UF}_{n_1}\text{-}\mathrm{CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-}\mathrm{KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-}\mathrm{KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\mathrm{EF}^{n_1}\text{-}\mathrm{CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-}\mathrm{KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-}\mathrm{KOA}\,[\mathcal{S}]
\end{array}$$

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Breaking $\mathcal{S}$ by breaking F : attacks again

$$
\begin{array}{ccccc}
\mathrm{UF}_{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{UF}_{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\color{red}{\mathrm{EF}^{n_1}\text{-CMA}\,[\mathcal{S}]} & \Leftarrow & \mathrm{EF}^{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \mathrm{EF}^{n_1}\text{-KOA}\,[\mathcal{S}] \\
\color{red}{\Uparrow} & & & & \\
\text{A-COL}^{n_1,n_2}\,[F] & & & &
\end{array}
$$

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Breaking $\mathcal{S}$ by breaking F : attacks again

$$
\begin{array}{ccccc}
\text{A-SEC}_{n_1}^{n_2}[F] & & & & \\
\Downarrow & & & & \\
\text{UF}_{n_1}\text{-CMA}[\mathcal{S}] & \Leftarrow & \text{UF}_{n_1}\text{-KMA}_{n_2}[\mathcal{S}] & \Leftarrow & \text{UF}_{n_1}\text{-KOA}[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\text{EF}^{n_1}\text{-CMA}[\mathcal{S}] & \Leftarrow & \text{EF}^{n_1}\text{-KMA}_{n_2}[\mathcal{S}] & \Leftarrow & \text{EF}^{n_1}\text{-KOA}[\mathcal{S}] \\
\Uparrow & & & & \\
\text{A-COL}^{n_1,n_2}[F] & & & &
\end{array}
$$

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Breaking $\mathcal{S}$ by breaking F : attacks again

$$
\begin{array}{ccccc}
\text{A-SEC}_{n_1}^{n_2}\,[F] & & & & \\
\Downarrow & & & & \\
\text{UF}_{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \text{UF}_{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \text{UF}_{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\text{EF}^{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \text{EF}^{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \text{EF}^{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Uparrow & & \Uparrow & & \\
\text{A-COL}^{n_1,n_2}\,[F] & & \text{U-SEC}_{n_2}^{n_1}\,[F] & &
\end{array}
$$

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Breaking $\mathcal{S}$ by breaking F : attacks again

$$
\begin{array}{ccccc}
\text{A-SEC}^{n_2}_{n_1}[F] & & & & \\
\Downarrow & & & & \\
\text{UF}_{n_1}\text{-CMA}[\mathcal{S}] & \Leftarrow & \text{UF}_{n_1}\text{-KMA}_{n_2}[\mathcal{S}] & \Leftarrow & \text{UF}_{n_1}\text{-KOA}[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\text{EF}^{n_1}\text{-CMA}[\mathcal{S}] & \Leftarrow & \text{EF}^{n_1}\text{-KMA}_{n_2}[\mathcal{S}] & \Leftarrow & \text{EF}^{n_1}\text{-KOA}[\mathcal{S}] \\
\Uparrow & & \Uparrow & & \Uparrow^{(1)} \\
\text{A-COL}^{n_1,n_2}[F] & & \text{U-SEC}^{n_1}_{n_2}[F] & & \text{U-PRE}^{n_1}[F]
\end{array}
$$

(1) if $\mathcal{S}$ is primitive

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Breaking $\mathcal{S}$ by breaking F : attacks again

$$
\begin{array}{ccccc}
\text{A-SEC}_{n_1}^{n_2}\,[F] & & \text{U-PRE}^{n_1}\,[F] & & \text{U-PRE}^{n_1}\,[F] \\
\Downarrow & & \Downarrow ??? & & \Downarrow ??? \\
\text{UF}_{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \text{UF}_{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \text{UF}_{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\text{EF}^{n_1}\text{-CMA}\,[\mathcal{S}] & \Leftarrow & \text{EF}^{n_1}\text{-KMA}_{n_2}\,[\mathcal{S}] & \Leftarrow & \text{EF}^{n_1}\text{-KOA}\,[\mathcal{S}] \\
\Uparrow & & \Uparrow & & \Uparrow^{(1)} \\
\text{A-COL}^{n_1,n_2}\,[F] & & \text{U-SEC}_{n_2}^{n_1}\,[F] & & \text{U-PRE}^{n_1}\,[F]
\end{array}
$$

(1) if $\mathcal{S}$ is primitive

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Repudiation : attacks. . .

$$\mathrm{UR}_{n_1}^{n_2}\,[\mathcal{S}]$$
$$\Downarrow$$
$$\mathrm{ER}^{n_1, n_2}\,[\mathcal{S}]$$

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Repudiation : attacks...

$$\mathrm{UR}_{n_1}^{n_2}\,[\mathcal{S}]$$

$$\Downarrow$$

$$\mathrm{ER}^{n_1,n_2}\,[\mathcal{S}]$$

$$\Uparrow$$

$$\text{U-COL}^{n_1,n_2}\,[F]$$

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Repudiation : attacks...

$$\text{U-SEC}_{n_1}^{n_2}[F]$$

$$\Downarrow$$

$$\text{UR}_{n_1}^{n_2}[\mathcal{S}]$$

$$\Downarrow$$

$$\text{ER}^{n_1,n_2}[\mathcal{S}]$$

$$\Uparrow$$

$$\text{U-COL}^{n_1,n_2}[F]$$

Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and F

Repudiation : attacks... + security proofs

$$
\begin{array}{ccc}
 & & \text{U-SEC}_{n_1}^{n_2}[F] \\
 & & \Downarrow \\
\text{E-SEC}_{n_1}^{n_2}[F] & \Leftarrow & \text{UR}_{n_1}^{n_2}[\mathcal{S}] \\
 & & \Downarrow \\
\text{E-COL}^{n_1,n_2}[F] & \Leftarrow & \text{ER}^{n_1,n_2}[\mathcal{S}] \\
 & & \Uparrow \\
 & & \text{U-COL}^{n_1,n_2}[F]
\end{array}
$$

Merkle-Damgård Instantiations

What is done in practice

- Tempting to build F from H in practice...
- Tempting to build H from f using iteration

Take fixed compression function f and $IV_0 \in \{0,1\}^{\mathrm{m}}$.

- let H_0 = iterated f without MD strengthening
- let H_S = iterated f with MD strengthening

$$F(m, r) = H_s(m \| r)$$

Terrible, since for any signature scheme Σ

$$\langle F, \Sigma \rangle = \langle H_0, \Sigma' \rangle$$

The security gain inherent to using the probabilistic hash-and-sign paradigm collapses. More precisely, for any $n > 0$

$$\begin{array}{ccccc}
\text{A-SEC}_n^n[F] & \Leftarrow & \text{SEC}_n^n[H_s] & \Leftarrow & \text{SEC}_n^n[H_0] \\
\Downarrow & & \Downarrow & & \Downarrow \\
\text{A-COL}^{n,n}[F] & \Leftarrow & \text{COL}^{n,n}[H_s] & \Leftarrow & \text{COL}^{n,n}[H_0]
\end{array}$$

$$F(m,r) = H_s(r\|m)$$

No known way to break $\mathcal{S}$ in any sense even if

$$\mathrm{COL}^{n,n}[H_0], \quad \mathrm{SEC}_n^n[H_0] \quad \text{and} \quad \mathrm{PRE}^n[H_0]$$

are all easy

$\boxed{\text{Concrete estimations of } \tau \text{ for } \varepsilon \simeq 1 \text{ given in paper}}$