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

Connections between $S$ and $H_1, \ldots, H_n$ are usually not understood.
Hash Functions in Cryptosystems

How do broken hash functions impact cryptosystems?

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

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

OAEP padding
How do broken hash functions impact cryptosystems?

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

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

Connections between $S$ 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 $H_1, H_2$
How do broken hash functions impact cryptosystems?

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

Connections between $S$ 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
How do broken hash functions impact cryptosystems?

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

Connections between $S$ 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 $\text{COL}[H_1] \equiv 0$?
Security Relations between $S[H]$ and $H$

$S = S[H]$

We want to determine how the security of $H$ relates to the one of $S$

We see 4 types of connections:

- **Attack a reduction** $\text{Break}(H) \Rightarrow \text{Break}(S)$ (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** $\text{Break}(H) \Leftarrow \text{Break}(S)$

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

- **Impossibility of Security Proof** no reduction $\text{Break}(H) \Leftarrow \text{Break}(S)$

So there are positive security results and negative security results.
Security Relations between $S[H]$ and $H$

$S = S[H]$

We want to determine how the security of $H$ relates to the one of $S$

We see 4 types of connections

- **Attack** a reduction $\text{Break}(H) \Rightarrow \text{Break}(S)$
Security Relations between $S[H]$ and $H$

$S = S[H]$

We want to determine how the security of $H$ relates to the one of $S$

We see 4 types of connections

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

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

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

So there are positive security results and negative security results.
Security Relations between $S[H]$ and $H$

$S = S[H]$

We want to determine how the security of $H$ relates to the one of $S$

We see 4 types of connections

**Attack** a reduction $\text{Break}(H) \Rightarrow \text{Break}(S)$ (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 $\text{Break}(H) \Leftarrow \text{Break}(S)$

So there are positive security results and negative security results.
**Security Relations between $S[H]$ and $H$**

<table>
<thead>
<tr>
<th>Equation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S = S[H]$</td>
<td>We want to determine how the security of $H$ relates to the one of $S$</td>
</tr>
</tbody>
</table>

**We see 4 types of connections**

- **Attack**  a reduction $\text{Break}(H) \Rightarrow \text{Break}(S)$ (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 $\text{Break}(H) \Leftarrow \text{Break}(S)$
- **Impossible Attack** there is no reduction $\text{Break}(H) \Rightarrow \text{Break}(S)$
Security Relations between $S[H]$ and $H$

$S = S[H]$

We want to determine how the security of $H$ relates to the one of $S$

We see 4 types of connections

- **Attack** a reduction $\text{Break}(H) \Rightarrow \text{Break}(S)$ (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 $\text{Break}(H) \Leftarrow \text{Break}(S)$

- **Impossible Attack** there is no reduction $\text{Break}(H) \Rightarrow \text{Break}(S)$ (meta-reduction technique: if $\text{Break}(H) \Rightarrow R \Rightarrow M \text{Break}(S)$ then $R \Rightarrow M P$ where $P$ is auxiliary)
# Security Relations between $S[H]$ and $H$

We want to determine how the security of $H$ relates to the one of $S$.

We see 4 types of connections:

- **Attack** a reduction $\text{Break}(H) \Rightarrow \text{Break}(S)$ (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 $\text{Break}(H) \Leftarrow \text{Break}(S)$

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

- **Impossibility of Security Proof** no reduction $\text{Break}(H) \Leftarrow \text{Break}(S)$

So there are **positive security results** and **negative security results**.
Security Relations between $S[H]$ and $H$

$S = S[H]$

We want to determine how the security of $H$ relates to the one of $S$

We see 4 types of connections

- **Attack** a reduction $\text{Break}(H) \Rightarrow \text{Break}(S)$ (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 $\text{Break}(H) \Leftarrow \text{Break}(S)$

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

- **Impossibility of Security Proof** no reduction $\text{Break}(H) \Leftarrow \text{Break}(S)$

So there are *positive* security results and *negative* security results.
What We Do Here

<table>
<thead>
<tr>
<th>Focus on public-key signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections $S[H]/H$ heavily depend on the way $S$ makes use of $H$</td>
</tr>
</tbody>
</table>

| We clarify everything |
What We Do Here

Focus on public-key signatures

Connections $S[H]/H$ heavily depend on the way $S$ 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 $S[H]/H$ heavily depend on the way $S$ 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 $S[H]/H$ heavily depend on the way $S$ 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 $S[H]/H$ heavily depend on the way $S$ 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

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
What We Do Here

Focus on public-key signatures

Connections $S[H]/H$ heavily depend on the way $S$ 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

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
What We Do Here

Focus on public-key signatures

Connections $S[H]/H$ heavily depend on the way $S$ 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 $S[H]/H$ heavily depend on the way $S$ 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 $S[H]/H$ heavily depend on the way $S$ 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 $S[H]/H$ heavily depend on the way $S$ 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 ($\kappa \to \infty$) or concrete setting
Security Reductions

Different semantics of proofs

- polynomial setting \((\kappa \to \infty)\) or concrete setting
Different semantics of proofs

- **polynomial** setting \((\kappa \to \infty)\) or **concrete** setting
  - given problem \(P\), \(\mathcal{A} (\tau, \varepsilon)\)-solves or \((\tau, \varepsilon)\)-breaks \(P\) if \(\mathcal{A}\) outputs a solution of \(P\) wrt \(\tau, \varepsilon\)
Security Reductions

Different semantics of proofs

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

Different semantics of proofs

- **polynomial** setting ($\kappa \rightarrow \infty$) or **concrete** setting
  - given problem $P$, $A(\tau, \varepsilon)$-solves or $(\tau, \varepsilon)$-breaks $P$ if $A$ outputs a solution of $P$ wrt $\tau, \varepsilon$
  - $\tau$ relates to some fixed model of computation
  - reduction $R$ between two computational problems $P_1$ and $P_2$ is a probabilistic algorithm $R$ which $(\tau_1, \varepsilon_1)$-solves $P_1$ given black-box access to an oracle $(\tau_2, \varepsilon_2)$-solving $P_2$
### Security Reductions

#### Different semantics of proofs

- **polynomial** setting \((\kappa \to \infty)\) or **concrete** setting
  - given problem \(P\), \(A(\tau, \varepsilon)\)-solves or \((\tau, \varepsilon)\)-breaks \(P\) if \(A\) outputs a solution of \(P\) wrt \(\tau, \varepsilon\)
  - \(\tau\) relates to some fixed model of computation
  - reduction \(R\) between two computational problems \(P_1\) and \(P_2\) is a probabilistic algorithm \(R\) which \((\tau_1, \varepsilon_1)\)-solves \(P_1\) given black-box access to an oracle \((\tau_2, \varepsilon_2)\)-solving \(P_2\)
  - \(P_1 \leq_R P_2\) when \(R\) 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 $P$, $A (\tau, \epsilon)$-solves or $(\tau, \epsilon)$-breaks $P$ if $A$ outputs a solution of $P$ wrt $\tau, \epsilon$
  - $\tau$ 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 $(\tau_1, \epsilon_1)$-solves $P_1$ given black-box access to an oracle $(\tau_2, \epsilon_2)$-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 $\epsilon_1 \simeq \epsilon_2$

- black-box or non-black-box
Security Reductions

**Different semantics of proofs**

- **polynomial** setting ($\kappa \to \infty$) or **concrete** setting
  - given problem $P$, $A$ $(\tau, \varepsilon)$-solves or $(\tau, \varepsilon)$-breaks $P$ if $A$ outputs a solution of $P$ wrt $\tau, \varepsilon$
  - $\tau$ 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 $(\tau_1, \varepsilon_1)$-solves $P_1$ given black-box access to an oracle $(\tau_2, \varepsilon_2)$-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 \((\kappa \rightarrow \infty)\) or **concrete** setting
  - given problem \(P\), \(A(\tau, \varepsilon)\)-solves or \((\tau, \varepsilon)\)-breaks \(P\) if \(A\) outputs a solution of \(P\) wrt \(\tau, \varepsilon\)
  - \(\tau\) 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 \((\tau_1, \varepsilon_1)\)-solves \(P_1\) given black-box access to an oracle \((\tau_2, \varepsilon_2)\)-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:

\[ P_1 \leq_\mathcal{R} P_2, \quad P_1 \leftrightarrow P_2, \quad etc. \]
Interpreting Security Reductions

**Success in breaking** \( P \)

We define \( \text{Succ} (P, \tau) = \max_A \text{Succ}^P (A, \tau) \) taken over all \( \tau \)-time probabilistic \( A \)'s. \( \text{Succ} (P, \tau) \) is a **function** here.
Interpreting Security Reductions

Success in breaking $P$

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

What does a security reduction mean?
Interpreting Security Reductions

Success in breaking $P$

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

What does a security reduction mean?

- take $P_1 = \text{Break}(S_1)$ and $P_2 = \text{Break}(S_2)$
Interpreting Security Reductions

**Success in breaking** $P$

We define $\text{Succ}(P, \tau) = \max_A \text{Succ}^P(A, \tau)$ taken over all $\tau$-time probabilistic $A$’s. $\text{Succ}(P, \tau)$ is a function here.

**What does a security reduction mean?**

- take $P_1 = \text{Break}(S_1)$ and $P_2 = \text{Break}(S_2)$
- assume you find $R$ such that $\text{Break}(S_1) \leftarrow_R \text{Break}(S_2)$
## Interpreting Security Reductions

**Success in breaking $P$**

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

**What does a security reduction mean?**

- take $P_1 = \text{Break}(S_1)$ and $P_2 = \text{Break}(S_2)$
- assume you find $\mathcal{R}$ such that $\text{Break}(S_1) \leftarrow_{\mathcal{R}} \text{Break}(S_2)$
- this means $\text{Succ} (\text{Break}(S_1), \tau_1) \geq \text{Succ} (\text{Break}(S_2), \tau_2)$ for $\tau_1 \approx \tau_2$
Interpreting Security Reductions

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

What does a security reduction mean?
- take $P_1 = \text{Break}(S_1)$ and $P_2 = \text{Break}(S_2)$
- assume you find $R$ such that $\text{Break}(S_1) \leftarrow_R \text{Break}(S_2)$
- this means $\text{Succ} (\text{Break}(S_1), \tau_1) \geq \text{Succ} (\text{Break}(S_2), \tau_2)$ for $\tau_1 \simeq \tau_2$

What happens if $\text{Break}(S_1)$ has no solution?
Well then $S_1$ is perfectly (IT) secure, and so must be $S_2$
## Interpreting Security Reductions

### Success in breaking $P$

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

### What does a security reduction mean?

- take $P_1 = \text{Break}(S_1)$ and $P_2 = \text{Break}(S_2)$
- assume you find $R$ such that $\text{Break}(S_1) \iff_R \text{Break}(S_2)$
- this means $\text{Succ}(\text{Break}(S_1), \tau_1) \geq \text{Succ}(\text{Break}(S_2), \tau_2)$ for $\tau_1 \simeq \tau_2$

### What happens if $\text{Break}(S_2)$ has no solution?

Then the reduction just tells us $\text{Succ}(\text{Break}(S_1)) \geq 0$, no big deal.
Interpreting Security Reductions

Success in breaking $P$

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

What does a security reduction mean?

- take $P_1 = Break(S_1)$ and $P_2 = Break(S_2)$
- assume you find $R$ such that $Break(S_1) \leftarrow_{R} Break(S_2)$
- this means $Succ\left(Break(S_1), \tau_1\right) \geq Succ\left(Break(S_2), \tau_2\right)$ for $\tau_1 \simeq \tau_2$
Interpreting Security Reductions

**Success in breaking $P$**

We define $\text{Succ} (P, \tau) = \max_A \text{Succ}^P (A, \tau)$ taken over all $\tau$-time probabilistic $A$’s. $\text{Succ} (P, \tau)$ is a function here.

**What does a security reduction mean?**

- take $P_1 = \text{Break}(S_1)$ and $P_2 = \text{Break}(S_2)$
- assume you find $R$ such that $\text{Break}(S_1) \leftarrow_R \text{Break}(S_2)$
- this means $\text{Succ} (\text{Break}(S_1), \tau_1) \geq \text{Succ} (\text{Break}(S_2), \tau_2)$ for $\tau_1 \simeq \tau_2$

**What happens if $\text{Break}(S_1)$ always has a solution?**

Then

\[
\text{Succ} (\text{Break}(S_1), \tau) = 1 \quad \text{for any } \tau
\]

No big deal, restrict maximum on known adversaries $A$. 

Hash Functions

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

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

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

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

Iterated hashing allows to build “$H$ from $f$”
Security Notions for Hash Functions

Collision-resistance $\text{COL}^{n_1,n_2}[H]$ 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 $\text{Succ} (\text{COL}^{n_1,n_2}[H]) = 1$ or $0$. 
Security Notions for Hash Functions

Collision-resistance $\text{COL}^{n_1,n_2} [H]$ 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 $\text{Succ} (\text{COL}^{n_1,n_2} [H]) = 1$ or 0.

Second-preimage-resistance $\text{SEC}^{n_2} [H]$ 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 $M_2 \neq M_1$. 

Most efficient definition for security statements.
Security Notions for Hash Functions

Collision-resistance $\text{COL}^{n_1,n_2}[H]$ 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 $\text{Succ}(\text{COL}^{n_1,n_2}[H]) = 1$ or $0$.

Second-preimage-resistance $\text{SEC}^{n_2}[H]$ 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 $\text{COL}^{n_1, n_2} [H]$ 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 $\text{Succ} (\text{COL}^{n_1, n_2} [H]) = 1$ or 0

Second-preimage-resistance $\text{SEC}^{n_2} [H]$ 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 :

$\text{PRE}^{n_2} [H]$ 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 $H(M_2) = m$
Collision-resistance $\text{COL}^{n_1,n_2} [H]$ 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 $\text{Succ (COL}^{n_1,n_2} [H]) = 1$ or 0.

Second-preimage-resistance $\text{SEC}^{n_2} [H]$ 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 :

$\text{PRE}^{n_2}_{n_1} [H]$ 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 $H(M_2) = m$.

$\text{PRE}^n [H]$ Given a random $m \leftarrow \{0,1\}^m$, find an $n$-bit string $M$ such that $H(M) = m$. 

Most efficient definition for security statements
Security Notions for Hash Functions

Collision-resistance \(\text{COL}^{n_1,n_2}[H]\) 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 \(\text{Succ}(\text{COL}^{n_1,n_2}[H]) = 1\) or 0.

Second-preimage-resistance \(\text{SEC}^{n_2}[H]\) 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:

\(\text{PRE}^{n_2}[H]\) 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 \(H(M_2) = m\).

\(\text{PRE}^n[H]\) Given a random \(m \leftarrow \{0,1\}^m\), find an \(n\)-bit string \(M\) such that \(H(M) = m\).

Most efficient definition for security statements.
Let \( H : \{0, 1\}^* \rightarrow \{0, 1\}^m \) be a hash function.

Then for any \( n_1, n_2 > 0 \),

\[
\text{COL}^{n_1, n_2} [H] \iff \text{SEC}_{n_1}^{n_2} [H] \iff (1) \text{ PRE}_{n_1}^{n_2} [H] \iff (2) \text{ PRE}_{n_2} [H]
\]

(1) only if \( n_2 \gg m \)

(2) when \( H \) is well-balanced
Hash Function Family

Hash function family

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

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 $r \leftarrow \{0, 1\}^r$, 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\(n_2\)[\(F\)]** Given \(M_1 \leftarrow \{0, 1\}^{n_1}\), find \((M_2, r)\) with \(F(M_1, r) = F(M_2, r)\)
- **U-SEC\(n_2\)[\(F\)]** Given \(M_1 \leftarrow \{0, 1\}^{n_1}\) and \(r \leftarrow \{0, 1\}^r\), find \(M_2\) with \(F(M_1, r) = F(M_2, r)\)
- **A-SEC\(n_2\)[\(F\)]** 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 \(m \leftarrow \{0, 1\}^m\), find \((M, r)\) such that \(F(M, r) = m\)
- **U-PRE\(n\)[\(F\)]** Given \(m \leftarrow \{0, 1\}^m\) and \(r \leftarrow \{0, 1\}^r\), 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

\[
\begin{align*}
E\text{-PRE}^{n_2} [F] &\iff U\text{-PRE}^{n_2} [F] \\
\downarrow^{(1)} &\downarrow^{(1)} \\
E\text{-SEC}^{n_2}_{n_1} [F] &\iff U\text{-SEC}^{n_2}_{n_1} [F] &\iff A\text{-SEC}^{n_2}_{n_1} [F] \\
\downarrow &\downarrow &\downarrow \\
E\text{-COL}^{n_1,n_2} [F] &\iff U\text{-COL}^{n_1,n_2} [F] &\iff A\text{-COL}^{n_1,n_2} [F]
\end{align*}
\]

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

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

**Key Gen.** \((pk, sk) \leftarrow S.\text{Gen}()\)

**Sign.** given message \(M \in \mathcal{M}\)

\[ \text{pick } u \leftarrow \{0,1\}^u \quad \text{then} \quad \sigma = S.\text{Sign}(sk, M, u) \]

**Verify.** \(S.\text{Ver}(pk, M, \sigma) \) outputs \(0/1\)

Message space can be
- \(\mathcal{M} = \{0,1\}^m\) or
- \(\mathcal{M} = \{0,1\}^*\)
Security Notions

 Forms of Unforgeability:

\( \text{UF}_{n}^{\text{-KOA}} [S] \) Given \( \text{pk} \leftarrow S.\text{Gen()} \) and \( M \leftarrow \{0, 1\}^{n} \), get 
\( \sigma = S.\text{Sign}(sk, M, u) \)

\( \text{EF}_{n}^{\text{-KOA}} [S] \) Given \( \text{pk} \leftarrow S.\text{Gen()} \), get \((M, \sigma)\) where \( M \in \{0, 1\}^{n} \) and 
\( \sigma = S.\text{Sign}(sk, M, u) \)

\( \text{KMA}_{n} \) You are given a list of \((M_{i}, \sigma_{i})\) where \( M_{i} \leftarrow \{0, 1\}^{n} \) and 
\( u_{i} \leftarrow \{0, 1\}^{u} \)

\( \text{CMA} \) You have access to signing oracle

 Forms of Non-Repudiation:

\( \text{ER}_{n_{2}}^{n_{1}} [S] \) Given \((\text{pk}, \text{sk}) \leftarrow S.\text{Gen()}\), find \((M_{1}, M_{2}, \sigma_{1} = \sigma_{2})\)

\( \text{UR}_{n_{2}}^{n_{1}} [S] \) Given \((\text{pk}, \text{sk}) \leftarrow S.\text{Gen()}\) and \( M_{1} \leftarrow \{0, 1\}^{n_{1}} \), find 
\( M_{2} \in \{0, 1\}^{n_{2}} \) and \( \sigma \)
Security Profile of Signatures

\[ UF_{n_1} \text{-CMA} [S] \iff UF_{n_1} \text{-KMA}_{n_2} [S] \iff UF_{n_1} \text{-KOA} [S] \]
\[ \Downarrow \quad \Downarrow \quad \Downarrow \]
\[ EF^{n_1} \text{-CMA} [S] \iff EF^{n_1} \text{-KMA}_{n_2} [S] \iff EF^{n_1} \text{-KOA} [S] \]

\[ UR^{n_2} [S], UR^{n_1} [S] \]
\[ \Downarrow \]
\[ ER^{n_1, n_2} [S] \]
Deterministic Hash-and-Sign Signatures

Given

- $\Sigma$ signing $m$-bit messages under $u$ bits of randomness
Deterministic Hash-and-Sign Signatures

Given

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

we construct $S = \langle H, \Sigma \rangle$ where
Deterministic Hash-and-Sign Signatures

Given

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

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

Key Gen. \ $S.Gen \triangleq \Sigma.Gen$

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

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

Verify. \ $S.Ver(pk, M, \sigma)$ outputs \ $\Sigma.Ver(pk, H(M), \sigma)$
Two-Step Signatures

\( \Sigma \) can be split into four functions

\[ \Sigma_1, \Sigma_2, \Upsilon_1, \Upsilon_2 \]

To sign:

1. pick \( u \leftarrow \{0, 1\}^u \)
2. \( (r, \text{aux}) = \Sigma_1(sk, u) \)
3. \( \sigma = \Sigma_2(sk, m, r, \text{aux}) \)

To verify:

1. \( \hat{r} = \Upsilon_1(pk, \sigma) \)
2. output \( \Upsilon_2(pk, m, \sigma, \hat{r}) \)

If \( \sigma \) is valid then \( \hat{r} = r \) is unique and \( r \) must be uniform over \( \{0, 1\}^r \) if \( u \) is uniform over \( \{0, 1\}^u \)
We assemble $\Sigma$ and $F$ to build $S = \langle F, \Sigma \rangle$

To sign:

1. Pick $u \leftarrow \{0, 1\}^u$
2. $(r, aux) = \Sigma_1(sk, u)$
3. $m = F(M, r)$
4. $\sigma = \Sigma_2(sk, m, r, aux)$

To verify:

1. $\hat{r} = \Upsilon_1(pk, \sigma)$
2. $\hat{m} = F(M, \hat{r})$
3. Output $\Upsilon_2(pk, m, \sigma, \hat{r})$
Primitiveness of $S = \langle F, \Sigma \rangle$

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

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

$$(m, \sigma = \Sigma.\text{Sign}(sk, m, u))$$

- $m$ is uniformly distributed over $\{0, 1\}^m$
- $u$ is uniformly distributed over $\{0, 1\}^u$
Injectivity of $S = \langle F, \Sigma \rangle$

$S$ is injective when

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

such that

- $\sigma = \Sigma_2(sk, m, r, aux)$ and
- $(r, aux) = \Sigma_1(sk, u)$ for some $u, aux$
### Classifying Common Signature Schemes

<table>
<thead>
<tr>
<th>Signature Scheme</th>
<th>Det. H&amp;S</th>
<th>Prob. H&amp;S</th>
<th>Primitive</th>
<th>Injective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schnorr</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>FDH</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>PFDH</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>PSS</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>EMSA-PSS</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>BLS</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Generic DSA</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>GHR</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>CS</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Breaking $S$ by breaking $H$: attacks

\[
\begin{align*}
UF_{n_1} \text{-CMA}[S] & \iff UF_{n_1} \text{-KMA}_{n_2}[S] \iff UF_{n_1} \text{-KOA}[S] \\
& \Downarrow \quad \Downarrow \quad \Downarrow \\
EF_{n_1} \text{-CMA}[S] & \iff EF_{n_1} \text{-KMA}_{n_2}[S] \iff EF_{n_1} \text{-KOA}[S]
\end{align*}
\]
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Breaking $S$ by breaking $H$: attacks

\[
\begin{align*}
UF_{n_1}^\text{-CMA}[S] & \iff UF_{n_1}^\text{-KMA}_{n_2}[S] \iff UF_{n_1}^\text{-KOA}[S] \\
\downarrow & \quad \downarrow & \quad \downarrow \\
EF_{n_1}^\text{-CMA}[S] & \iff EF_{n_1}^\text{-KMA}_{n_2}[S] \iff EF_{n_1}^\text{-KOA}[S] \\
& \uparrow \uparrow \\
\text{COL}_{n_1,n_2}^n[H] & 
\end{align*}
\]
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Breaking $S$ by breaking $H$ : attacks

\[ \text{SEC}^{n_2}_{n_1}[H] \]
\[ \Downarrow \]
\[ \text{UF}^{n_1}_{n_1}\text{-CMA}[S] \iff \text{UF}^{n_1}_{n_2}\text{-KMA}_{n_2}[S] \iff \text{UF}^{n_1}_{n_1}\text{-KOA}[S] \]
\[ \Downarrow \quad \Downarrow \quad \Downarrow \]
\[ \text{EF}^{n_1}_{n_1}\text{-CMA}[S] \iff \text{EF}^{n_1}_{n_2}\text{-KMA}_{n_2}[S] \iff \text{EF}^{n_1}_{n_1}\text{-KOA}[S] \]
\[ \Uparrow \]
\[ \text{COL}^{n_1,n_2}[H] \]
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Breaking $S$ by breaking $H$: attacks

\[
\begin{align*}
\text{SEC}_{n_1}^{n_2} [H] \\
\Downarrow \\
\text{UF}_{n_1}^{n_1} - \text{CMA} [S] \iff \text{UF}_{n_1}^{n_1} - \text{KMA}_{n_2} [S] \iff \text{UF}_{n_1}^{n_1} - \text{KOA} [S] \\
\Downarrow \\
\text{EF}_{n_1}^{n_1} - \text{CMA} [S] \iff \text{EF}_{n_1}^{n_1} - \text{KMA}_{n_2} [S] \iff \text{EF}_{n_1}^{n_1} - \text{KOA} [S] \\
\Uparrow \\
\text{COL}_{n_1, n_2}^{n_1, n_2} [H] \\
\text{SEC}_{n_2}^{n_1} [H]
\end{align*}
\]
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Breaking $S$ by breaking $H$: attacks

\[ \text{SEC}^{n_2}_{n_1} [H] \]
\[ \Downarrow \]
\[ \text{UF}^{n_1}_{n_1} - \text{CMA} [S] \iff \text{UF}^{n_1}_{n_1} - \text{KMA}_{n_2} [S] \iff \text{UF}^{n_1}_{n_1} - \text{KOA} [S] \]
\[ \Downarrow \quad \Downarrow \quad \Downarrow \]
\[ \text{EF}^{n_1}_{n_1} - \text{CMA} [S] \iff \text{EF}^{n_1}_{n_1} - \text{KMA}_{n_2} [S] \iff \text{EF}^{n_1}_{n_1} - \text{KOA} [S] \]
\[ \Uparrow \quad \Uparrow \quad \Uparrow^{(1)} \]
\[ \text{COL}^{n_1,n_2} [H] \quad \text{SEC}^{n_1}_{n_2} [H] \quad \text{PRE}^{n_1} [H] \]

(1) if $S$ is primitive
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Breaking $S$ by breaking $H$ : attacks

\[
\begin{array}{ccc}
\text{SEC}_{n_1}^n [H] & \Downarrow & \text{PRE}_{n_1}^1 [H] & \Downarrow \text{??}
\end{array}
\]

\[
\begin{array}{ccc}
\text{UF}_{n_1}^\text{-CMA} [S] & \Leftarrow & \text{UF}_{n_1}^\text{-KMA}_{n_2} [S] & \Leftarrow & \text{UF}_{n_1}^\text{-KOA} [S]
\end{array}
\]

\[
\begin{array}{ccc}
\Downarrow & \Downarrow & \Downarrow
\end{array}
\]

\[
\begin{array}{ccc}
\text{EF}_{n_1}^\text{-CMA} [S] & \Leftarrow & \text{EF}_{n_1}^\text{-KMA}_{n_2} [S] & \Leftarrow & \text{EF}_{n_1}^\text{-KOA} [S]
\end{array}
\]

\[
\begin{array}{ccc}
\Uparrow & \Uparrow & \Uparrow_{(1)}
\end{array}
\]

\[
\begin{array}{ccc}
\text{COL}_{n_1,n_2} [H] & \text{SEC}_{n_2}^1 [H] & \text{PRE}_{n_1}^1 [H]
\end{array}
\]

(1) if $S$ is primitive
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Repudiation: attacks...

\[
\begin{align*}
\text{UR}^{n_2}_{n_1} [S] & \quad \Downarrow \quad \text{ER}^{n_1,n_2} [S]
\end{align*}
\]
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Repudiation: attacks...

\[ \text{UR}^{n_2}_{n_1} [S] \quad \downarrow \quad \text{ER}^{n_1,n_2} [S] \quad \uparrow \quad \text{COL}^{n_1,n_2} [H] \]
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Repudiation: attacks...

$\text{SEC}_{n_1}^{n_2}[H]$
$\Downarrow$
$\text{UR}_{n_1}^{n_2}[S]$
$\Downarrow$
$\text{ER}_{n_1,n_2}[S]$
$\Uparrow$
$\text{COL}_{n_1,n_2}[H]$
Relations between $S = \langle H, \Sigma \rangle$ and $H$

Repudiation: attacks...and security proofs

\[
\begin{align*}
\text{SEC}^{n_2}_{n_1} [H] & \iff (2) \\downarrow \\
\text{UR}^{n_2}_{n_1} [S] & \downarrow \\
\text{ER}^{n_1,n_2} [S] & \iff (2) \\
\text{COL}^{n_1,n_2} [H] & \\
\end{align*}
\]

(2) if $S$ is injective
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Breaking $S$ by breaking $F$ : attacks again

\[
\begin{align*}
UF_{n_1}-\text{CMA}[S] & \iff UF_{n_1}-\text{KMA}_{n_2}[S] \iff UF_{n_1}-\text{KOA}[S] \\
\downarrow & \quad \downarrow & \quad \downarrow \\
EF^{n_1}-\text{CMA}[S] & \iff EF^{n_1}-\text{KMA}_{n_2}[S] \iff EF^{n_1}-\text{KOA}[S]
\end{align*}
\]
Relations between $\mathcal{S} = \langle F, \Sigma \rangle$ and $F$

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

\[
\begin{align*}
\text{UF}_{n_1}\text{-CMA}[\mathcal{S}] & \iff \text{UF}_{n_1}\text{-KMA}_{n_2}[\mathcal{S}] \iff \text{UF}_{n_1}\text{-KOA}[\mathcal{S}] \\
\downarrow & \downarrow \downarrow \\
\text{EF}^{n_1}\text{-CMA}[\mathcal{S}] & \iff \text{EF}^{n_1}\text{-KMA}_{n_2}[\mathcal{S}] \iff \text{EF}^{n_1}\text{-KOA}[\mathcal{S}] \\
\uparrow & \\
\text{A-COL}^{n_1,n_2}[F]
\end{align*}
\]
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Breaking $S$ by breaking $F$ : attacks again

\[
\begin{align*}
&\text{A-SEC}_{n_1}^{n_2}[F] \\
&\quad \Downarrow \\
&\text{UF}_{n_1}^{\text{CMA}}[S] \iff \text{UF}_{n_1}^{\text{KMA}_{n_2}}[S] \iff \text{UF}_{n_1}^{\text{KOA}}[S] \\
&\quad \Downarrow \quad \Downarrow \quad \Downarrow \\
&\text{EF}_{n_1}^{\text{CMA}}[S] \iff \text{EF}_{n_1}^{\text{KMA}_{n_2}}[S] \iff \text{EF}_{n_1}^{\text{KOA}}[S] \\
&\quad \Uparrow \\
&\text{A-COL}_{n_1,n_2}^{n_1}[F]
\end{align*}
\]
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Breaking $S$ by breaking $F$: attacks again

\[
\begin{align*}
\text{A-SEC}_{n_1}^n [F] & \Downarrow & \text{UF}_{n_1} - \text{CMA} [S] & \iff \text{UF}_{n_1} - \text{KMA}_{n_2} [S] & \iff \text{UF}_{n_1} - \text{KOA} [S] \\
& & \Downarrow & \Downarrow & \Downarrow \\
\text{EF}_{n_1} - \text{CMA} [S] & \iff \text{EF}_{n_1} - \text{KMA}_{n_2} [S] & \iff \text{EF}_{n_1} - \text{KOA} [S] \\
& \Uparrow & \Uparrow & \Uparrow & \Uparrow \\
\text{A-COL}^{n_1, n_2} [F] & & \text{U-SEC}_{n_2}^n [F] 
\end{align*}
\]
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Breaking $S$ by breaking $F$: attacks again

\[
\text{A-SEC}^n_{12} [F] \\
\downarrow \\
\text{UF}^n_1\text{-CMA} [S] \iff \text{UF}^n_1\text{-KMA}^n_{12} [S] \iff \text{UF}^n_1\text{-KOA} [S] \\
\downarrow \\
\text{EF}^n_1\text{-CMA} [S] \iff \text{EF}^n_1\text{-KMA}^n_{12} [S] \iff \text{EF}^n_1\text{-KOA} [S] \\
\uparrow \\
\text{A-COL}^{n_1,n_2} [F] \\
\text{U-SEC}^n_{12} [F] \\
\text{U-PRE}^n_{12} [F]
\]

(1) if $S$ is primitive
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Breaking $S$ by breaking $F$: attacks again

\[
\begin{array}{ccc}
\text{A-SEC}_{n_2}^n [F] & \xrightarrow{\Downarrow} & \text{U-PRE}_{n_1}^n [F] & \xleftarrow{\Downarrow \text{??}} & \text{U-PRE}_{n_1}^n [F] \\
\text{UF}_{n_1}^n \text{-CMA} [S] & \xleftarrow{\Downarrow} & \text{UF}_{n_1}^n \text{-KMA}_{n_2} [S] & \xleftarrow{\Downarrow} & \text{UF}_{n_1}^n \text{-KOA} [S] \\
\text{EF}_{n_1}^n \text{-CMA} [S] & \xleftarrow{\Downarrow} & \text{EF}_{n_1}^n \text{-KMA}_{n_2} [S] & \xleftarrow{\Downarrow} & \text{EF}_{n_1}^n \text{-KOA} [S] \\
\text{A-COL}_{n_1,n_2}^n [F] & \xrightarrow{\Uparrow} & \text{U-SEC}_{n_2}^n [F] & \xrightarrow{\Uparrow} & \text{U-PRE}_{n_1}^n [F] \quad (1)
\end{array}
\]

(1) if $S$ is primitive
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Repudiation: attacks...

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

$\Downarrow$

$\text{ER}^{n_1, n_2} [S]$
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Repudiation: attacks...
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Repudiation: attacks...

\[
\begin{align*}
&\text{U-SEC}^{n_2}_{n_1} [F] \\
&\Downarrow \\
&\text{UR}^{n_2}_{n_1} [S] \\
&\Downarrow \\
&\text{ER}^{n_1,n_2} [S] \\
&\Uparrow \\
&\text{U-COL}^{n_1,n_2} [F]
\end{align*}
\]
Relations between $S = \langle F, \Sigma \rangle$ and $F$

Repudiation: attacks... + security proofs

$\downarrow$

$E-\text{SEC}^{n_2}_{n_1}[F] \iff UR^{n_2}_{n_1}[S]$

$\downarrow$

$E-\text{COL}^{n_1,n_2}[F] \iff ER^{n_1,n_2}[S]$

$\uparrow$

$U-\text{COL}^{n_1,n_2}[F]$
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 $IV_0 \in \{0, 1\}^m$.

- let $H_0 = \text{iterated } f \text{ without MD strengthening}$
- let $H_S = \text{iterated } f \text{ with MD strengthening}$
\[ F(m, r) = H_s(m \parallel r) \]

Terrible, since for any signature scheme \( \Sigma \)

\[ \langle F, \Sigma \rangle = \langle H_0, \Sigma' \rangle \]

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

\[
\begin{align*}
A-SEC_n^n [F] & \iff SEC_n^n [H_s] \iff SEC_n^n [H_0] \\
\downarrow & \downarrow & \downarrow \\
A-COL^{n,n}_n [F] & \iff COL^{n,n}_n [H_s] \iff COL^{n,n}_n [H_0]
\end{align*}
\]
\[ F(m, r) = H_s(r \| m) \]

No known way to break \( S \) in any sense even if

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

are all easy

Concrete estimations of \( \tau \) for \( \varepsilon \approx 1 \) given in paper