Forking Lemmas for Different Signature Scenarios

Maryam Rajabzadeh Asaar

Sharif University of Technology

7 January 2016 (17 Day 1394)

The 2nd Workshop on Mathematical Aspects of Computer Science

Foundations of Cryptography

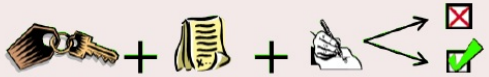
Table of contents

Digital signature schemes

- Key generation: $\mathrm{Gen}(1^k) \longrightarrow (PK, SK)$

- Signing: $\mathrm{Sign}(SK, M) \longrightarrow sig$

- Verifying: $\mathrm{Ver}(PK, M, sig) \longrightarrow$ "valid" or "invalid"



What does it mean to *break* a signature scheme?

Breaking scenarios of a signature scheme:

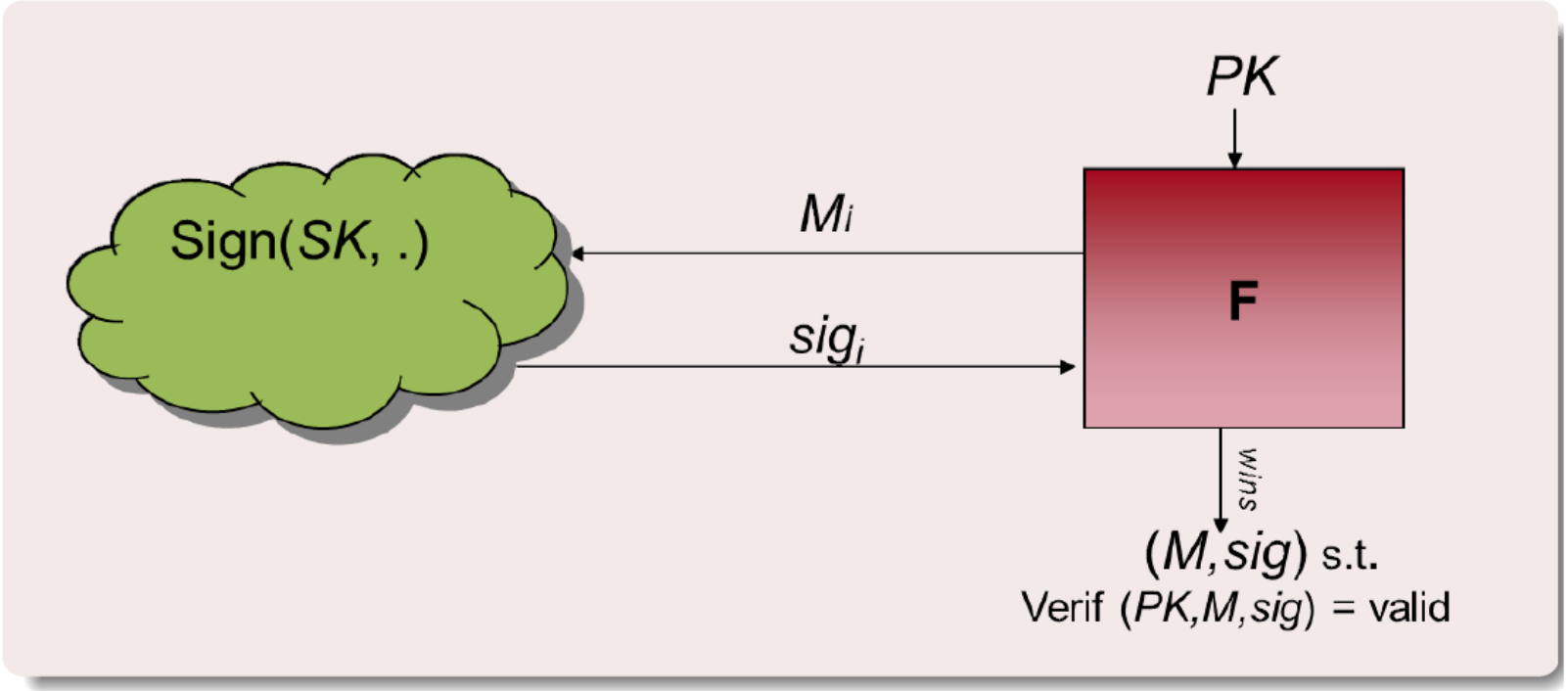
- Total break: private key is compromised.
- Universal forgery: finding an efficient signing algorithm equivalent to the original signing algorithm.
- Selective forgery: adversary can create a valid signature on a preselected message.
- Existential forgery: adversary can create a valid signature with no control over the message.

Types of attacks

Attack scenarios for signature schemes:

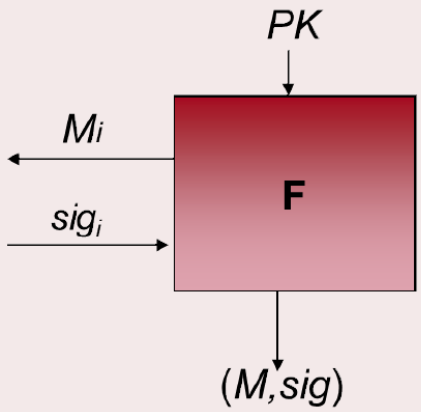
- Key-only: the adversary knows only the public key of the signer.
- Message attacks:
  - Known-message attack: the adversary has signatures for a set of messages which are known to the adversary but not chosen by him.
  - Chosen-message attack: the adversary obtains valid signatures from a chosen list of his choice (non adaptive).
  - Adaptive chosen-message attack: the adversary can use the signer as an oracle.

The standard security notion of signature schemes



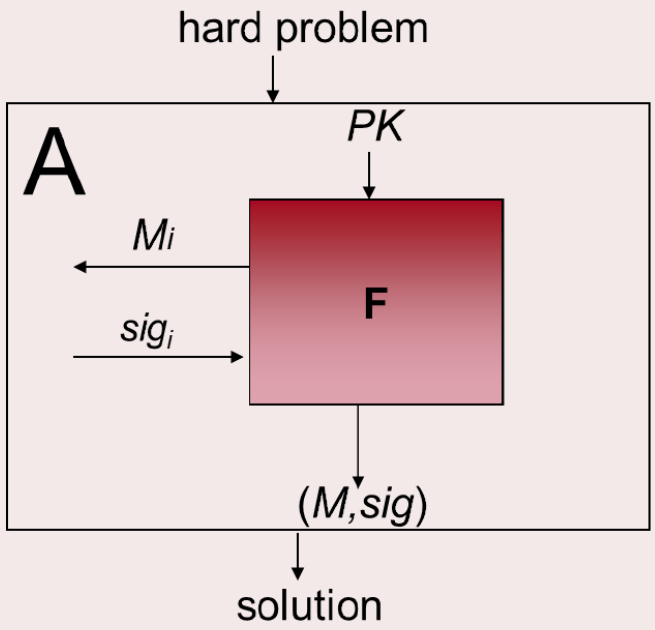
Proof by reduction

- Let **F** be an adversary that breaks the scheme

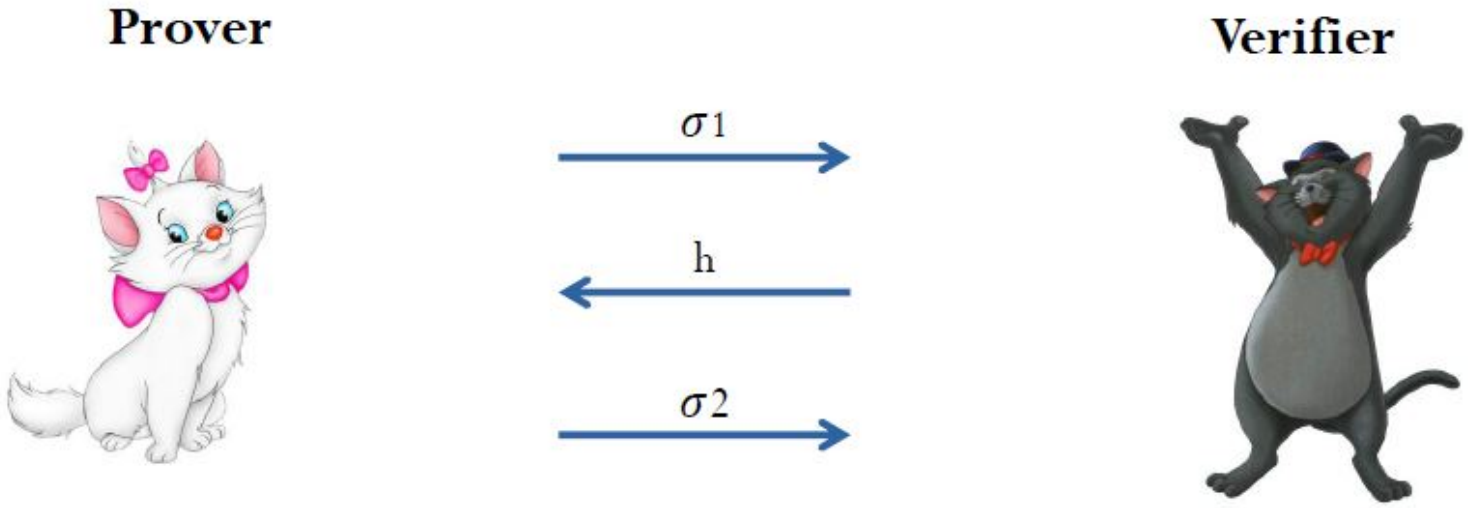


Proof by reduction

- Let **F** be an adversary that breaks the scheme
- Then **F** can be used to solve P (**A** exists)



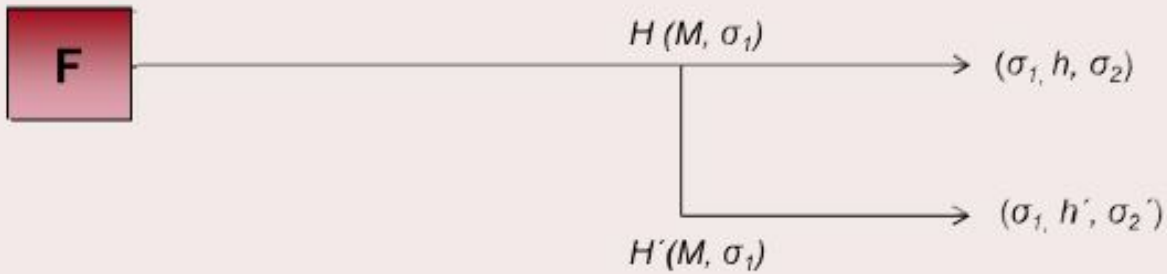
Identification protocols and generic standard signatures



Generic signature scheme: The signature on the message m is (σ_1, h, σ_2), where $\sigma_2 = H(m, \sigma_1)$.
(H is modeled as a Random Oracle (RO))

The idea of forking lemma proposed by Pointcheval and Stern

The idea of the security proof is to use a forking lemma to obtain from the forger F two related forgeries $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$ such that $h \neq h'$. Then, the solution of a hard problem from the ability to forge such pairs is extracted.



- If F returns $(m, \sigma_1, h, \sigma_2)$.
- Rewind F with a different RO to return $(m, \sigma_1, h', \sigma_2')$.

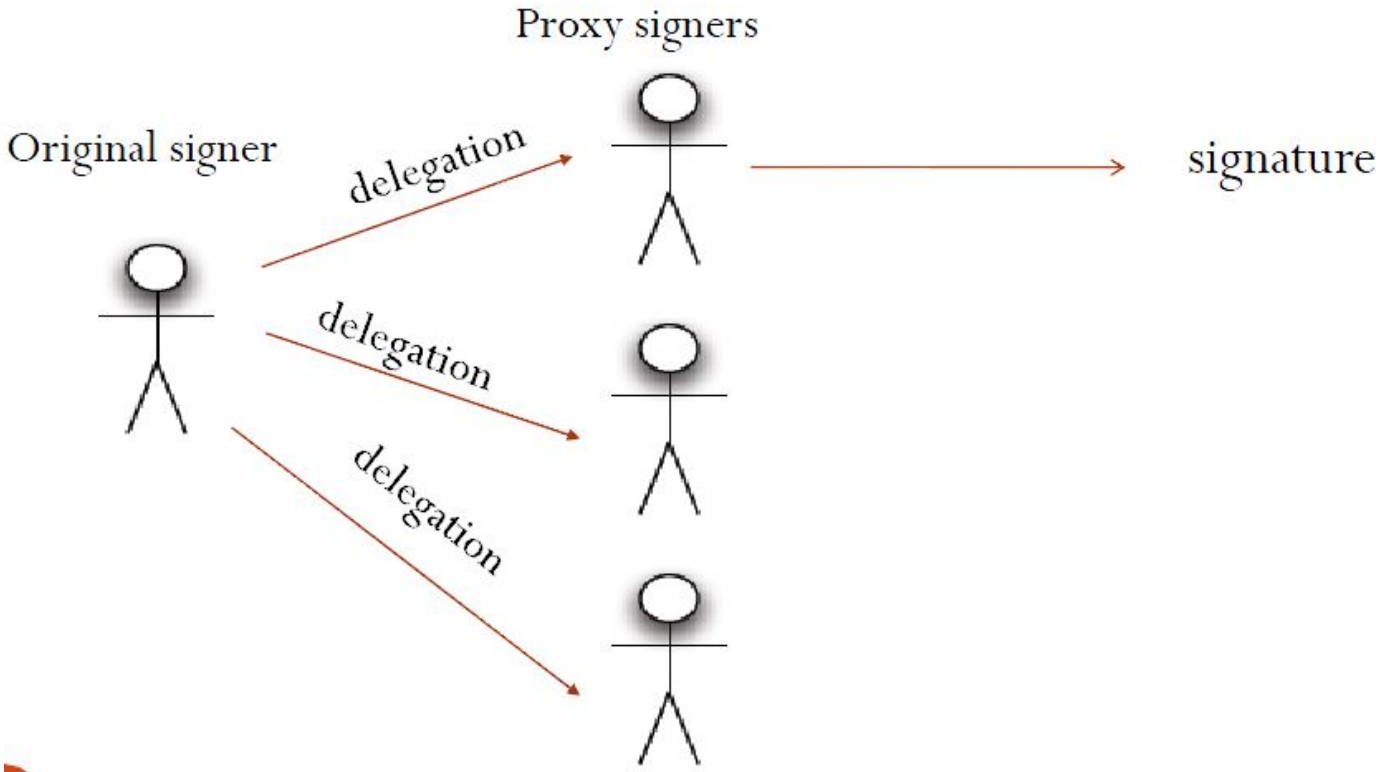
Some existing forking lemmas

- Ring forking lemma was proposed by Herranz and Saez in 2003.
- Generic forking lemma was presented by Bellare and Neven in 2006.
- Proxy ring forking lemma was introduced by A., Salmasizadeh and Susilo in 2014.
- Multi-proxy multi-signature forking lemma was introduced by A., Salmasizadeh and Susilo in 2014.

Proxy ring forking lemma

proxy ring signatures

In this type of signatures, an original signer delegates its signing capability to a set of n proxy signers, and each proxy signer can generate a proxy ring signature while its privacy is preserved.



Outline of proxy ring signatures

A proxy ring signature consists of the following algorithms:

- KeyGen: $(Para, (sk, pk)) \leftarrow KeyGen(k)$
- DelegationGen:
  $\sigma_0 \leftarrow DelegationGen(Para, pk_0, \mathbf{pk_p}, w, x_0)$.
- ProxyRingSign:
  $\theta \leftarrow ProxyRingSign(Para, pk_0, \mathbf{pk_p}, m, w, \sigma_0, sk_j)$
- ProxyRingVer:
  $\{0, 1\} \leftarrow ProxyRingVer(Para, pk_0, \mathbf{pk_p}, w, m, \theta)$

Security model of generic proxy ring signatures

There are two types for forgers in this kind of signatures:

- Forger of type I which can play the role of a malicious proxy signer and tries to forge a valid proxy ring signature.
  - The adversary of type I who has access to the DelegationGen oracle.
- Forger of type II which plays the role of a malicious original signer and tries to forge a valid proxy ring signature.
  - The adversary of type II who has access to the ProxyRingSign oracle.

Generic proxy ring signatures

A class of proxy ring signature schemes that is called generic is defined as follows.

- Consider a security parameter k, a hash function $H(.) : \{0,1\}^* \rightarrow \{0,1\}^k$ and a ring of n members.
- A generic proxy ring signature is in form of $(m, w, R_0, R_1, ..., R_n, h_0, h_1, ..., h_n, s)$, where $R_i \neq R_j$ for all $i \neq j$, $h_0 = H(w, R_0)$ and $h_i = H(m, w, R_0, R_i)$ for $1 \leq i \leq n$, and s is determined by h_0, R_0, h_i, R_i, $1 \leq i \leq n$, the warrant w and the message m.

Sketch of proof for the generic proxy ring signature

The idea of the proof is to employ a Forking Lemma to obtain from the forger F (type I or II) two related forgeries $(m, w, R_o, R_1, ..., R_n, h_0, h_1, ..., h_n, s)$ and $(m, w, R_o, R_1, ..., R_n, h'_0, h'_1, ..., h'_n, s')$ such that $h_0 \neq h'_0$ and $h_i = h'_i$, $1 \leq i \leq n$ for Forger of type I or $h_j \neq h'_j$ for some j, $1 \leq j \leq n$ and others are the same for Forger of type II. Then, the solution of a hard problem from these pairs is extracted.

If the original (general) forking lemma can be applied to our generic construction or not?

The idea of proxy ring forking lemma's proof

- Suppose that there exists a PPT forger F with success probability at least ϵ.
- $\vec{\rho} = (\rho_1, ..., \rho_q)$.
- $u_i \in \{1, ..., q\}$, for $0 \leq i \leq n$ such that $Q_{u_i} = (M, R_i)$, and if a query is never asked, $u_i = \infty$.
- $\vec{u}$ is defined as $(u_0, ..., u_n)$.
- Let $\beta = \max\{u \in (u_0, ..., u_n)\}$.
- Let S be $\{(\omega, \vec{\rho}) |\ F(\omega, \vec{\rho})$ succeeds $\&\ \ \beta \neq \infty\}$.
- Let $S_{\vec{u}}$ be $\{(\omega, \vec{\rho}) |\ F(\omega, \vec{\rho})$ succeeds $\&\ \ Ind(\omega, \vec{\rho}) = \vec{u}\}$.

The idea of proxy ring forking lemma's proof

- Let J be $\{(u_0, ..., u_n) \mid 1 \leq u_i \leq q \ \& \ \forall i \neq j \ u_i \neq u_j \ \& \ u_0 > \max\{u_i \text{ for } 1 \leq i \leq n\}\}$ for type I Forger.
- Let J be $\{(u_0, ..., u_n) \mid 1 \leq u_i \leq q \ \& \ \forall i \neq j \ u_i \neq u_j \ \& \ u_0 < \max\{u_i \text{ for } 1 \leq i \leq n\}\}$ for type II Forger.
- $|J| = \pi = \sum_{j=1}^{q-n}[\prod_{i=0}^{n-1}(q-i-j)]$.

The idea of proxy ring forking lemma's proof

- Let I be $\{\vec{u} \in J | \Pr[S_{\vec{u}}|S] \geq \frac{1}{2}\frac{1}{\pi}\}$.
- There exists a subset $\Omega_{\vec{u}}$ of the pairs $(\omega, \vec{\rho})$ such that $\Pr[\Omega_{\vec{u}}|S_{\vec{u}}] \geq \frac{1}{2}$ and for each $(\omega, \vec{\rho}) \in \Omega_{\vec{u}}$, $\Pr_{\vec{\rho'}}[(\omega, \vec{\rho'}) \in S_{\vec{u}}] \geq \frac{\Pr[S]}{4\pi}$.
- For each vector of a successful pair, $\vec{u}$, $\Pr[\vec{u} \in I \ \& \ (\omega, \vec{\rho}) \in \Omega_{\vec{u}} \cap S_{\vec{u}}|S] \geq \frac{1}{4}$.

The idea of proxy ring forking lemma's proof

- With probability $\frac{\Pr[S]}{4}$, $\vec{u} \in I$ and $(\omega, \rho) \in \Omega_{\vec{u}} \cap S_{\vec{u}}$.
- Replay the attack with fixed $(\omega, (\rho_1, ..., \rho_{\beta-1}))$ and randomly chosen $(\rho'_\beta, ..., \rho'_q)$, we get another successful pair $(\omega, (\rho_1, ..., \rho_{\beta-1}, \rho'_\beta, ..., \rho'_q))$ such that $\rho_\beta \neq \rho'_\beta$ with probability $\frac{\Pr[S](1-2^{-k})}{4\pi}$.
- The probability of having two valid forgeries with a suitable relation is $\frac{(\Pr[S])^2(1-2^{-k})}{16\pi}$.

Extension the result to adaptively chosen message and warrant attack

The only difference is that the probability of the forger changed due to:

- collisions of DelegationGen queries
- collisions of ProxyRingSign queries

Collisions of DelegationGen queries:

- A pair (w, R_i) that the simulator outputs has been asked from the random oracle by the forger.
- A pair (w, R_i) that the simulator outputs is exactly similar to another pair generated by the simulator.

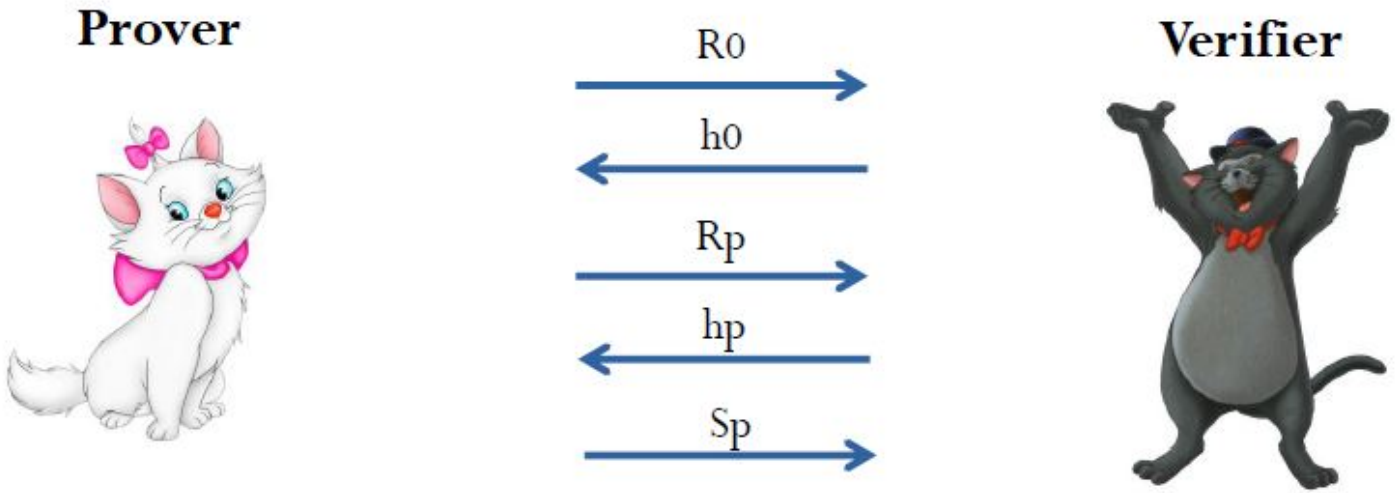
Multi-proxy multi-signature forking lemma

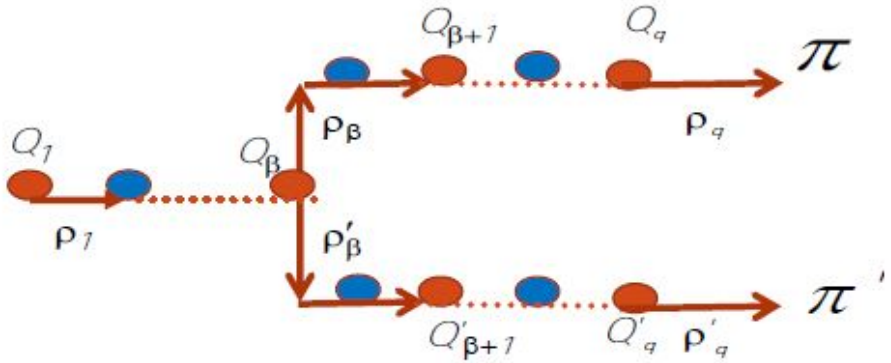
Generic multi-proxy multi-signatures

In this type, a set of original signers delegates its signing capability to a set of proxy signers such that all proxy signers can corporately sign messages on behalf of the original signers. The generic multi-proxy multi-signature is presented as follows.

- Consider a security parameter k, a hash function $H(.) : \{0,1\}^* \rightarrow \{0,1\}^k$ and $f : \{0,1\}^{nk} \rightarrow \{0,1\}^k$.
- A generic multi-proxy multi-signature is in form of $(m, w, R_o, R_p, h_o, h_p, s)$, where $R_o \neq R_p$, $R_o = f(R_1, ..., R_d)$ and $R_p = f(R_1, ..., R_n)$, $h_o = H(R_o, w)$, $h_p = H(R_o, R_p, w, m)$, and s is determined by h_o, h_p, R_o, R_p, the warrant w and the message m.

The idea of multi-proxy multi-signature forking lemma





Concluding remarks

- Reviewing some preliminaries for security analysis of signature schemes.
- Reviewing different forking lemmas for various signatures' scenarios.
- Extension of the oiginal forking lemma for other types of signature schemes.
- Giving a unified forking lemma to capture all different scenarios.

Thank You!

Questions?