On the Non-Malleability of the Fiat-Shamir Transform

Sebastian Faust[1] Markulf Kohlweiss[2]
Giorgia Azzurra Marson[3] Daniele Venturi[1]

[1] Aarhus University

[2] Microsoft Research, Cambridge

[3] TU Darmstadt

INDOCRYPT 2012

TECHNISCHE UNIVERSITÄT DARMSTADT

CASED

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Our result in a nutshell

Sigma Protocol $\xrightarrow{\textbf{Fiat-Shamir}}$ **NIZK**

Our result in a nutshell

$$\textbf{Sigma Protocol} \xrightarrow{\textbf{Fiat-Shamir}} \text{non-malleable } \textbf{NIZK}$$

Our result in a nutshell

$$\textbf{Sigma Protocol} \xrightarrow{\textbf{Fiat-Shamir}} \text{non-malleable } \textbf{NIZK}$$

- Thought to be a folklore result...

Our result in a nutshell

Sigma Protocol $\xrightarrow{\textbf{Fiat-Shamir}}$ non-malleable **NIZK**

- Thought to be a folklore result. . .
- . . . but formalization non trivial

Our result in a nutshell

Sigma Protocol $\xrightarrow{\textbf{Fiat-Shamir}}$ non-malleable **NIZK**

- Thought to be a folklore result. . .
- . . . but formalization non trivial

Our contribution:

- Formalize notions in RO model
  (analog to CRS model)

Our result in a nutshell

$$\text{Sigma Protocol} \xrightarrow{\text{Fiat-Shamir}} \text{non-malleable NIZK}$$

- Thought to be a folklore result. . .
- . . . but formalization non trivial

Our contribution:

- Formalize notions in RO model
  (analog to CRS model)
- Prove Fiat–Shamir NIZKs to be simulation-sound and -extractable under mild requirements

Our result in a nutshell

Sigma Protocol $\xrightarrow{\textbf{Fiat-Shamir}}$ non-malleable **NIZK**

- Thought to be a folklore result...
- ...but formalization non trivial

Our contribution:

- Formalize notions in RO model
  (analog to CRS model)
- Prove Fiat–Shamir NIZKs to be simulation-sound and -extractable under mild requirements
- Corollary (of known applications of NIZKs):
  - efficient leakage-resilient CCA2-secure PKE
  - efficient KDM CCA2-secure PKE
  - efficient leakage-resilient signatures

Outline

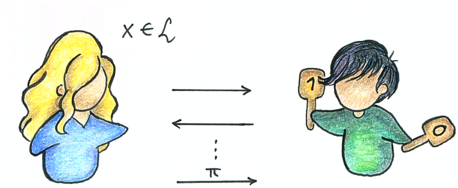
1. Established notions and known results
   - Interactive protocols
   - Non-interactive protocols
   - Non-malleability for NIZKs

Outline

1. Established notions and known results
    - Interactive protocols
    - Non-interactive protocols
    - Non-malleability for NIZKs

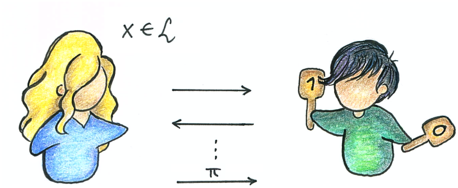
2. Our contribution
    - Properties of the Fiat–Shamir transform
    - Applications

Interactive proofs (IP)



Prover $\mathcal{P}$ **Verifier** $\mathcal{V}$

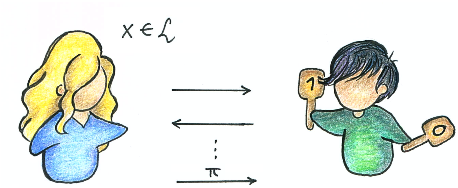
Interactive proofs (IP)



Prover $\mathcal{P}$ **Verifier $\mathcal{V}$**

- $\mathcal{P}$ wants to convince *efficient* $\mathcal{V}$ that string x belongs to language $\mathcal{L}$
- interaction leads to proof π

Interactive proofs (IP)



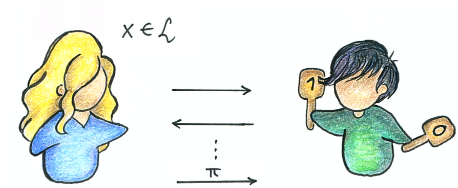
Prover $\mathcal{P}$

Verifier $\mathcal{V}$

- $\mathcal{P}$ wants to convince *efficient* $\mathcal{V}$ that string x belongs to language $\mathcal{L}$
- interaction leads to proof π

- $\mathcal{V}$ outputs verdict: accept or reject

Interactive proofs (IP)



Prover $\mathcal{P}$

Verifier $\mathcal{V}$

- $\mathcal{P}$ wants to convince *efficient* $\mathcal{V}$ that string x belongs to language $\mathcal{L}$
- interaction leads to proof π

- $\mathcal{V}$ outputs verdict: accept or reject

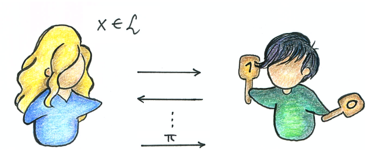
Completeness + Soundness

Zero knowledge

In a ***zero-knowledge*** proof, $\mathcal{P}$ convinces $\mathcal{V}$ that a statement is true, but $\mathcal{V}$ does not learn anything beyond its validity

Zero knowledge

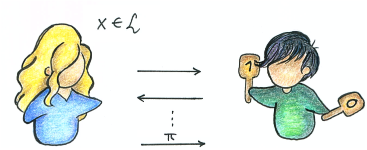
In a ***zero-knowledge*** proof, $\mathcal{P}$ convinces $\mathcal{V}$ that a statement is true, but $\mathcal{V}$ does not learn anything beyond its validity



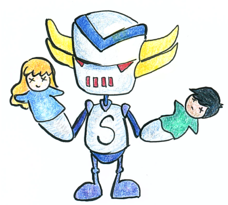
Whatever $\mathcal{V}$ learns from interaction with $\mathcal{P}$...

Zero knowledge

In a ***zero-knowledge*** proof, $\mathcal{P}$ convinces $\mathcal{V}$ that a statement is true, but $\mathcal{V}$ does not learn anything beyond its validity



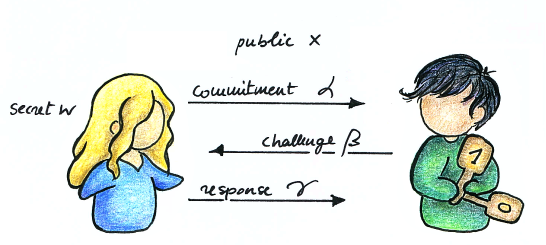
Whatever $\mathcal{V}$ learns from interaction with $\mathcal{P}$...



...can be **simulated** by efficient algorithm $\mathcal{S}$

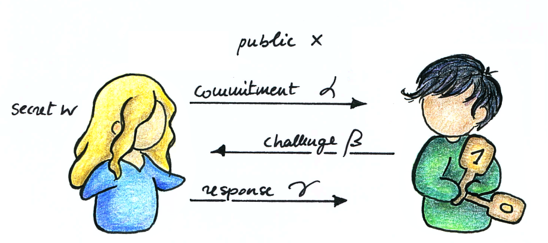
Sigma protocols

- $\mathcal{P}$ and $\mathcal{V}$ share input x
- $\mathcal{P}$ holds private input w (w wintess for $x \in \mathcal{L}$)
- 3-move interaction
  1. commitment
  2. challenge
  3. response



Sigma protocols

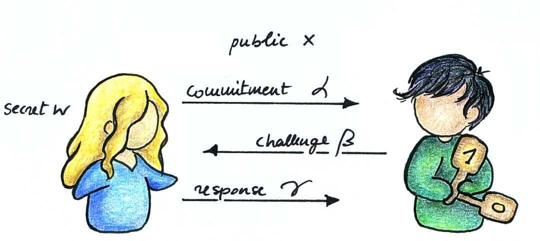
- $\mathcal{P}$ and $\mathcal{V}$ share input x
- $\mathcal{P}$ holds private input w (w wintess for $x \in \mathcal{L}$)
- 3-move interaction
  1. commitment
  2. challenge
  3. response



- **Honest-verifier zero knowledge (HVZK)**
  Zero knowledge only for *honest-but-curious* $\mathcal{V}$

Sigma protocols

- $\mathcal{P}$ and $\mathcal{V}$ share input x
- $\mathcal{P}$ holds private input w (w wintess for $x \in \mathcal{L}$)
- 3-move interaction
    1. commitment
    2. challenge
    3. response



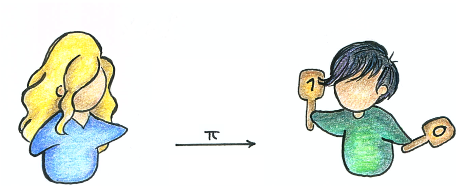
- **Honest-verifier zero knowledge (HVZK)**
  Zero knowledge only for *honest-but-curious* $\mathcal{V}$
- **Special soundness**
  Exists efficient extractor $\mathcal{E}_{sp}$ that outputs witness given two different accepting proof with same α

Fiat–Shamir transform

How to prove in zero knowledge without interaction

Non-interactive proofs

- $\mathcal{P}$ sends single message π
- Can it be **zero knowledge**?

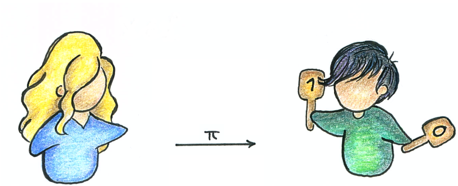


Fiat–Shamir transform

How to prove in zero knowledge without interaction

Non-interactive proofs

- $\mathcal{P}$ sends single message π
- Can it be **zero knowledge**?
- Standard model:
  non-interactive ZK (NIZK)
  exists only for trivial languages

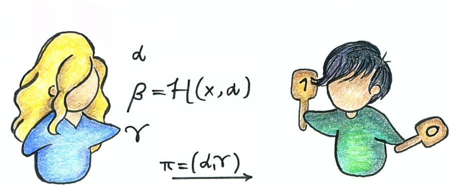


Fiat–Shamir transform

How to prove in zero knowledge without interaction

Non-interactive proofs

- $\mathcal{P}$ sends single message π
- Can it be **zero knowledge**?
- Standard model:
  non-interactive ZK (NIZK)
  exists only for trivial languages



Fiat–Shamir transform

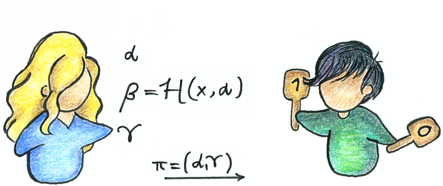
- Introduced to build efficient signature schemes [FS86]
- Turns 3-move IP into **non-interactive** ones
- $\mathcal{H}$ is a "good hash function" (modeled as a RO)

Fiat–Shamir transform

How to prove in zero knowledge without interaction

Non-interactive proofs

- $\mathcal{P}$ sends single message π
- Can it be **zero knowledge**?
- Standard model: non-interactive ZK (NIZK) exists only for trivial languages



Fiat–Shamir transform

- Introduced to build efficient signature schemes [FS86]
- Turns 3-move IP into **non-interactive** ones
- $\mathcal{H}$ is a "good hash function" (modeled as a RO)

> The Fiat–Shamir transform turns any Sigma protocol Σ into a *non-interactive zero-knowledge* protocol Σ_{FS}

Simulation soundness

Soundness not sufficiently strong for NIZKs

A proof is **sound** if
no malicious $\check{\mathcal{P}}$ can convince $\mathcal{V}$
to accept false statements

Simulation soundness

Soundness not sufficiently strong for NIZKs

A proof is **sound** if
no malicious $\check{\mathcal{P}}$ can convince $\mathcal{V}$
to accept false statements

- **Problem:** when malicious $\check{\mathcal{P}}$ observes simulated proofs
  - could forward simulated fake proofs
  - could create new fake proofs from simulated ones

Simulation soundness

Soundness not sufficiently strong for NIZKs

A proof is **sound** if
no malicious $\check{\mathcal{P}}$ can convince $\mathcal{V}$
to accept false statements

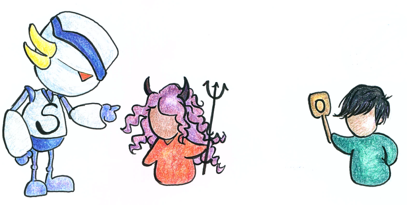
- **Problem:** when malicious $\check{\mathcal{P}}$ observes simulated proofs
  - could forward simulated fake proofs (no way to prevent!)
  - could create new fake proofs from simulated ones
- need to strengthen **soundness** [S99]

Simulation soundness

Soundness not sufficiently strong for NIZKs

A proof is **sound** if
no malicious $\check{\mathcal{P}}$ can convince $\mathcal{V}$
to accept false statements

- **Problem:** when malicious $\check{\mathcal{P}}$ observes simulated proofs
  - could forward simulated fake proofs (no way to prevent!)
  - could create new fake proofs from simulated ones
- need to strengthen **soundness** [S99]



A NIZK is ***simulation-sound*** if no $\check{\mathcal{P}}$ can produce fresh accepting proofs of false statements, even if she observes simulated (fake) proofs

Simulation extractability

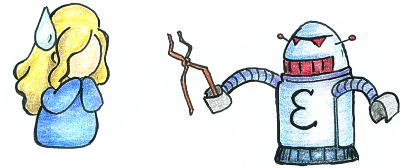
Knowledge extraction for IP

- $\mathcal{P}$ proves that she knows witness w for $x \in \mathcal{L}$
- Formally: if $\mathcal{P}$ convinces $\mathcal{V}$...

Simulation extractability

Knowledge extraction for IP

- $\mathcal{P}$ proves that she knows witness w for $x \in \mathcal{L}$
- Formally: if $\mathcal{P}$ convinces $\mathcal{V}$...
- ...then $\mathcal{E}$ can extract w ($\mathcal{E}$ can rewind $\mathcal{P}$)



Simulation extractability

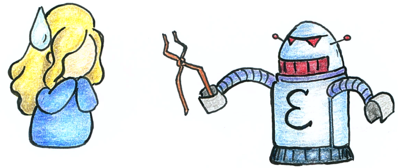
Knowledge extraction for IP

- $\mathcal{P}$ proves that she knows witness w for $x \in \mathcal{L}$
- Formally: if $\mathcal{P}$ convinces $\mathcal{V}$...

Analogously, for **NIZK** proofs:
Weak simulation extractability

- $\mathcal{P}$ obtains simulated proof by $\mathcal{S}$
- $\mathcal{P}$ succeeds if outputs fresh proof
- algorithm $\mathcal{E}$ can run $\mathcal{P}$
- $\mathcal{E}$ rewinds $\mathcal{P}$

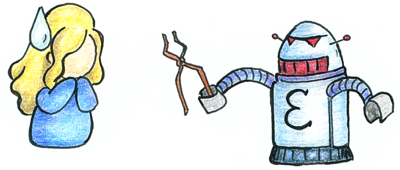
- ...then $\mathcal{E}$ can extract w ($\mathcal{E}$ can rewind $\mathcal{P}$)



Simulation extractability

Knowledge extraction for IP

- $\mathcal{P}$ proves that she knows witness w for $x \in \mathcal{L}$
- Formally: if $\mathcal{P}$ convinces $\mathcal{V}$...
- ...then $\mathcal{E}$ can extract w ($\mathcal{E}$ can rewind $\mathcal{P}$)



Analogously, for **NIZK** proofs:
Weak simulation extractability

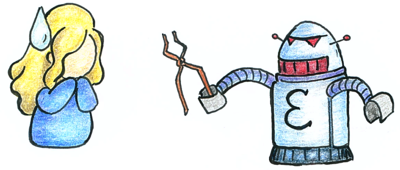
- $\mathcal{P}$ obtains simulated proof by $\mathcal{S}$
- $\mathcal{P}$ succeeds if outputs fresh proof
- algorithm $\mathcal{E}$ can run $\mathcal{P}$
- $\mathcal{E}$ rewinds $\mathcal{P}$

A NIZK proof $(\mathcal{P}, \mathcal{V})$ is ***simulation-extractable*** if $\mathcal{P}$ observes simulated proofs for (possibly false) statements and, whenever $\mathcal{P}$ succeeds, $\mathcal{E}$ extracts a valid witness

Simulation extractability

Knowledge extraction for IP

- $\mathcal{P}$ proves that she knows witness w for $x \in \mathcal{L}$
- Formally: if $\mathcal{P}$ convinces $\mathcal{V}$...
- ...then $\mathcal{E}$ can extract w ($\mathcal{E}$ can rewind $\mathcal{P}$)



Analogously, for **NIZK** proofs:
Weak simulation extractability

- $\mathcal{P}$ obtains simulated proof by $\mathcal{S}$
- $\mathcal{P}$ succeeds if outputs fresh proof
- algorithm $\mathcal{E}$ can run $\mathcal{P}$
- $\mathcal{E}$ rewinds $\mathcal{P}$

Strong simulation-extractability
$\mathcal{E}$ on-line extractor (does not rewind $\mathcal{P}$)

A NIZK proof $(\mathcal{P}, \mathcal{V})$ is ***simulation-extractable*** if $\mathcal{P}$ observes simulated proofs for (possibly false) statements and, whenever $\mathcal{P}$ succeeds, $\mathcal{E}$ extracts a valid witness

Outline

1. Established notions and known results
   - Interactive protocols
   - Non-interactive protocols
   - Non-malleability for NIZKs
2. Our contribution
   - Properties of the Fiat–Shamir transform
   - Applications

Efficient simulation-sound and extractable NIZKs

Fiat–Shamir paradigm applied to a specific Sigma protocol
to get simulation-sound NIZKs in the RO model [FP01]

Efficient simulation-sound and extractable NIZKs

Fiat–Shamir paradigm applied to a specific Sigma protocol to get simulation-sound NIZKs in the RO model [FP01]

In general?

Our main result:
The Fiat–Shamir transform yields **simulation sound** NIZKs under mild assumptions.

Efficient simulation-sound and extractable NIZKs

Fiat–Shamir paradigm applied to a specific Sigma protocol to get simulation-sound NIZKs in the RO model [FP01]

In general?

Our main result:

The Fiat–Shamir transform yields **simulation sound** NIZKs under mild assumptions.

Theorem 1. *Let Σ be a three-round HVZK interactive protocol with quasi-unique responses. Then, in the RO model, Σ_{FS} is simulation-sound.*

Efficient simulation-sound and extractable NIZKs

Fiat–Shamir paradigm applied to a specific Sigma protocol
to get simulation-sound NIZKs in the RO model [FP01]
In general?

Our main result:
The Fiat–Shamir transform yields **simulation sound** and **extractable** NIZKs under mild assumptions.

Theorem 1. *Let Σ be a three-round HVZK interactive protocol with quasi-unique responses. Then, in the RO model, Σ_{FS} is simulation-sound.*

Theorem 2. *Let Σ be a sigma-protocol with quasi-unique responses. Then, in the RO model, Σ_{FS} is weakly simulation-extractable.*

Efficient simulation-sound and extractable NIZKs

Fiat–Shamir paradigm applied to a specific Sigma protocol to get simulation-sound NIZKs in the RO model [FP01]

In general?

Our main result:

The Fiat–Shamir transform yields **simulation sound** and **extractable** NIZKs under mild* assumptions.

Theorem 1. *Let Σ be a three-round HVZK interactive protocol with quasi-unique responses. Then, in the RO model, Σ_{FS} is simulation-sound.*

Theorem 2. *Let Σ be a sigma-protocol with quasi-unique responses. Then, in the RO model, Σ_{FS} is weakly simulation-extractable.*

* A 3-move protocol has ***quasi-unique responses*** if it is hard to find two valid proofs which differ only in γ

Applications in Cryptography

Simulation-sound and extractable NIZKs as building-blocks:

- from CPA to CCA security for public-key encryption
- Key-dependent message (KDM) security
- Leakage-resilient signatures

Chosen-ciphertext security

Twin encryption and zero-knowledge proof

Naor–Yung transformation

- start from PKE scheme
- encrypt message twice under two independent public keys
- add proof of equality of plaintexts
  (witness $=$ message $+$ randomness used by Enc)

Chosen-ciphertext security

Twin encryption and zero-knowledge proof

Naor–Yung transformation

- start from PKE scheme
- encrypt message twice under two independent public keys
- add proof of equality of plaintexts (witness = message + randomness used by Enc)

CPA-secure **PKE** + **NIZK proof** yields CCA **security** [NY90]

Chosen-ciphertext security

Twin encryption and zero-knowledge proof

Naor–Yung transformation

- start from PKE scheme
- encrypt message twice under two independent public keys
- add proof of equality of plaintexts
  (witness = message + randomness used by Enc)

CPA-secure PKE + simulation-sound **NIZK proof**
yields CCA2 **security**
[NY90] [S99]

Chosen-ciphertext security

Twin encryption and zero-knowledge proof

Naor–Yung transformation

- start from PKE scheme
- encrypt message twice under two independent public keys
- add proof of equality of plaintexts
  (witness = message + randomness used by Enc)

LR-CPA-secure PKE + simulation-sound **NIZK proof**
yields LR-CCA2 **security**
[NY90] [S99] [NS09]

Chosen-ciphertext security

Twin encryption and zero-knowledge proof

Naor–Yung transformation

- start from PKE scheme
- encrypt message twice under two independent public keys
- add proof of equality of plaintexts
  (witness = message + randomness used by Enc)

LR-CPA-secure PKE + **simulation-sound NIZK proof**
yields **LR**-CCA2 **security**
[NY90] [S99] [NS09]

Our concrete instantiation:

- LR-CPA PKE scheme, generalization of ElGamal [BHHO09]
- NIZK protocol Σ_{FS} derived from sigma protocol associated with the corresponding NY language

Key-dependent message security

from CPA to CCA security

A PKE scheme has *key-dependent message* security if it remains secure even given the encryption of some (known) functions of the decryption key

Key-dependent message security

from CPA to CCA security

A PKE scheme has *key-dependent message* security if it remains secure even given the encryption of some (known) functions of the decryption key

The Naor–Yung paradigm preserves KDM security [CCS09]:

CPA + KDM-CPA PKEs + simulation-sound NIZK proof
yields **KDM-CCA2 security**

Key-dependent message security

from CPA to CCA security

A PKE scheme has *key-dependent message* security if it remains secure even given the encryption of some (known) functions of the decryption key

The Naor–Yung paradigm preserves KDM security [CCS09]:

CPA + KDM-CPA PKEs + simulation-sound NIZK proof
yields **KDM-CCA2 security**

Our concrete instantiation:

- ElGamal + BHHO PKE schemes
- NIZK protocol Σ_{FS} derived from sigma protocol associated with corresponding NY language

Leakage-resilient signatures

from simulation-extractable hard relations

A digital signature scheme is *leakage-resilient* if it is hard to forge signatures even given (bounded) leakage from the signing key

Leakage-resilient signatures

from simulation-extractable hard relations

A digital signature scheme is *leakage-resilient* if it is hard to forge signatures even given (bounded) leakage from the signing key

Generic construction based on hard relations [DHLW10]:

Leakage-resilient signatures

from simulation-extractable hard relations

A digital signature scheme is *leakage-resilient* if it is hard to forge signatures even given (bounded) leakage from the signing key

Generic construction based on hard relations [DHLW10]:

- leakage-resilient hard relation ρ
- **simulation-extractable** NIZK $(\mathcal{P}, \mathcal{V})$ for ρ'
  (ρ' derived from ρ by including message to be signed)

Leakage-resilient signatures

from simulation-extractable hard relations

A digital signature scheme is *leakage-resilient* if it is hard to forge signatures even given (bounded) leakage from the signing key

Generic construction based on hard relations [DHLW10]:

- leakage-resilient hard relation ρ
- **simulation-extractable** NIZK $(\mathcal{P}, \mathcal{V})$ for ρ'
  (ρ' derived from ρ by including message to be signed)

Our instantiation:

- NIZK protocol Σ_{FS} derived from sigma protocol associated to ρ'
- Σ_{FS} is only **weakly simulation-extractable**

Leakage-resilient signatures

from simulation-extractable hard relations

A digital signature scheme is *leakage-resilient* if it is hard to forge signatures even given (bounded) leakage from the signing key

Generic construction based on hard relations [DHLW10]:

- leakage-resilient hard relation ρ
- **simulation-extractable** NIZK $(\mathcal{P}, \mathcal{V})$ for ρ'
  (ρ' derived from ρ by including message to be signed)

Our instantiation:

- NIZK protocol Σ_{FS} derived from sigma protocol associated to ρ'
- Σ_{FS} is only **weakly simulation-extractable**
- Construction still works! (factor 2 loss in leakage)

Leakage-resilient signatures

from simulation-extractable hard relations

A digital signature scheme is *leakage-resilient* if it is hard to forge signatures even given (bounded) leakage from the signing key

Generic construction based on hard relations [DHLW10]:

- leakage-resilient hard relation ρ
- **simulation-extractable** NIZK $(\mathcal{P}, \mathcal{V})$ for ρ'
  (ρ' derived from ρ by including message to be signed)

Our instantiation:

- NIZK protocol Σ_{FS} derived from sigma protocol associated to ρ'
- Σ_{FS} is only **weakly simulation-extractable**
- Construction still works!* (factor 2 loss in leakage)
  * Weak simulation extractability guarantees that $\mathcal{E}$ extracts w with non-negligible probability

Summary

	CRS	RO
NIZK	✓	✓
Simulation soundness	✓	✓
Weak simulation extractability	✓	✓
Full simulation extractability	✓	?

Our contribution:

- Formalized security properties for NIZKs in the RO model
- Proved Fiat-Shamir transform to yield **simulation-sound** and **weakly simulation-extractable** NIZKs
- Applications: LR-CCA2 and KDM-CCA2 secure PKEs, LR signaures

Summary

	CRS	RO	
NIZK	✓	✓	
Simulation soundness	✓	✓	
Weak simulation extractability	✓	✓	[BPW12]
Full simulation extractability	✓	?	

Our contribution:

- Formalized security properties for NIZKs in the RO model
- Proved Fiat-Shamir transform to yield **simulation-sound** and **weakly simulation-extractable** NIZKs
- Applications: LR-CCA2 and KDM-CCA2 secure PKEs, LR signaures

Summary

	CRS	RO	
NIZK	✓	✓	
Simulation soundness	✓	✓	
Weak simulation extractability	✓	✓	[BPW12]
Full simulation extractability	✓	?	
		[F05]	

Our contribution:

- Formalized security properties for NIZKs in the RO model
- Proved Fiat-Shamir transform to yield **simulation-sound** and **weakly simulation-extractable** NIZKs
- Applications: LR-CCA2 and KDM-CCA2 secure PKEs, LR signaures

Open Problem:

Can we achieve **full simulation extractability**?

Thank you for your attention

TECHNISCHE
UNIVERSITÄT
DARMSTADT

CASED

001011100001011 Cryptoplexity
qed
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de