From Identification to Signatures, Tightly: A Framework and Generic Transforms

Mihir Bellare, **Bertram Poettering**, Douglas Stebila
UCSD / Ruhr University Bochum / McMaster

ASIACRYPT 2016, Hanoi
December 6, 2016

RUHR UNIVERSITÄT BOCHUM

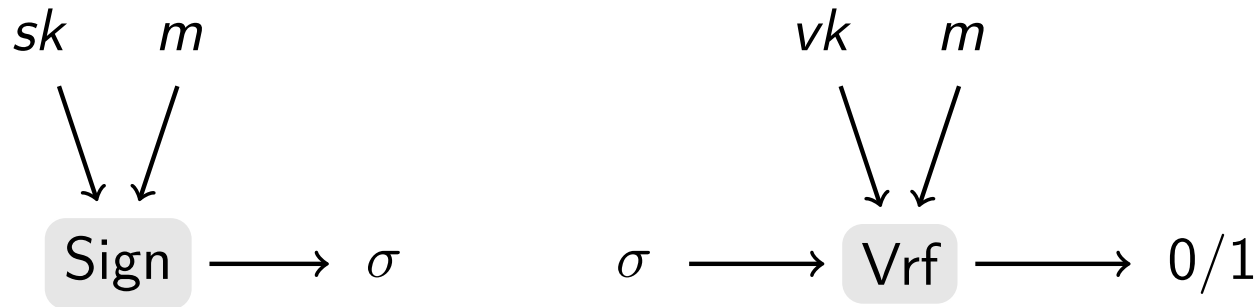
RUB

hgi
Horst Görtz Institut für IT-Sicherheit

Signature schemes

In a nutshell

- digital analogue to written signatures
- easy to create and verify
- security goal: unforgeability



Examples and applications

- 2×PKCS#1, DSA, ECDSA, EdDSA, ECSchnorr
- message authentication (emails), entity authentication (TLS, . . .)

Fiat-Shamir: Identification scheme $\rightarrow$ signature scheme

FS transform is versatile

- Fiat-Shamir from FACT
- Guillou-Quisquater from RSA
- Schnorr from DLP

Standardized instantiations of FS/Schnorr

- EdDSA
- ECSchnorr
- DSA/ECDSA

Evolution of security argument (always ROM)

- [FS] purely heuristic
- [PS] from ZK
- [OO,AABN] from ID scheme

Our contributions

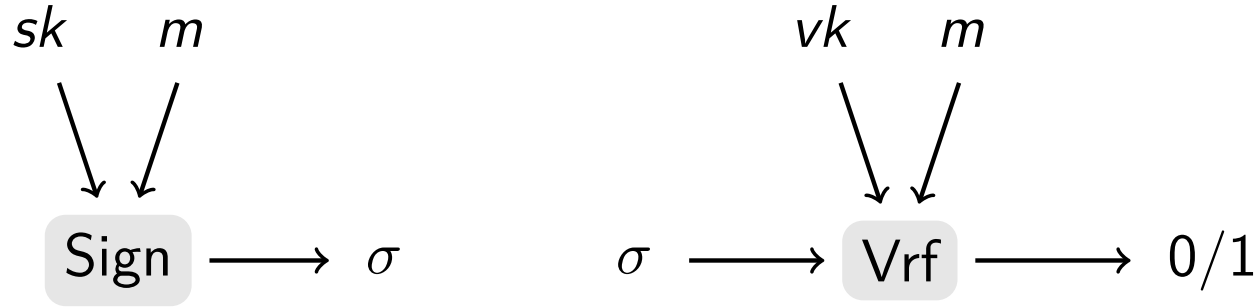
Observations

- FS reduction inherently untight
  - due to forking/reset lemma
  - consequence: large keys and signatures
- exception: FACT-based ad-hoc variant **Swap** [MR]

Contributions

- ID schemes with trapdoors
  - instantiations from GQ, MR, CFP
- new transforms: (trapdoor) ID $\rightarrow$ signature
  - depend on new security requirements for ID
  - tight reductions in all cases
- understanding Swap
  - finding the right abstraction boundaries

Security of signature schemes



Unforgeability (UF)

- signature oracle signs any message
- goal of adversary: craft signature on new message

Unique unforgeability (UUF)

- signature oracle signs any message **at most once**
- goal of adversary: craft signature on new message

Transforms UUF $\rightarrow$ UF?

- exist with tight reduction
- new goal: construct UUF signatures

Transforms UUF $\rightarrow$ UF

DR: Removing randomness

- idea: derandomize signing algorithm
- consequence: at most one signing query per message *w.l.o.g.*
- use private RO: $r \leftarrow H(sk, m)$; $\sigma \leftarrow \mathrm{Sign}(sk, m; r)$
- advantage: same signature size and verification procedure
- disadvantage: requires one more RO

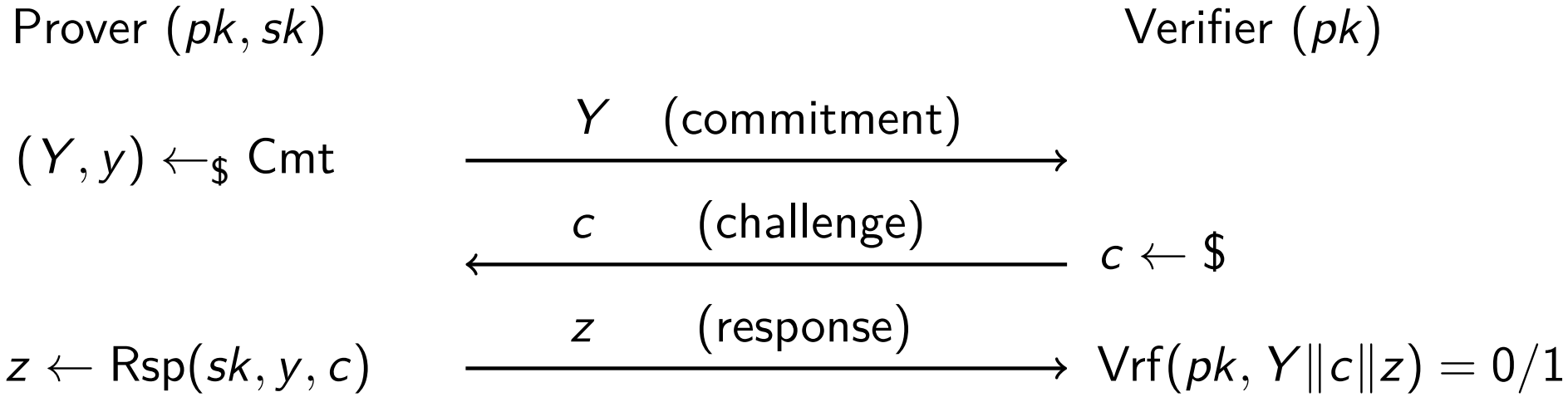
AR: Adding randomness

- idea: make messages unique by randomizing them
- consequence: at most one signing query per message *effectively*
- add salt to messages: $s \leftarrow \$$; $\sigma' \leftarrow \mathrm{Sign}(sk, m \| s)$; $\sigma \leftarrow \sigma' \| s$
- advantage: standard model
- disadvantage: larger signatures

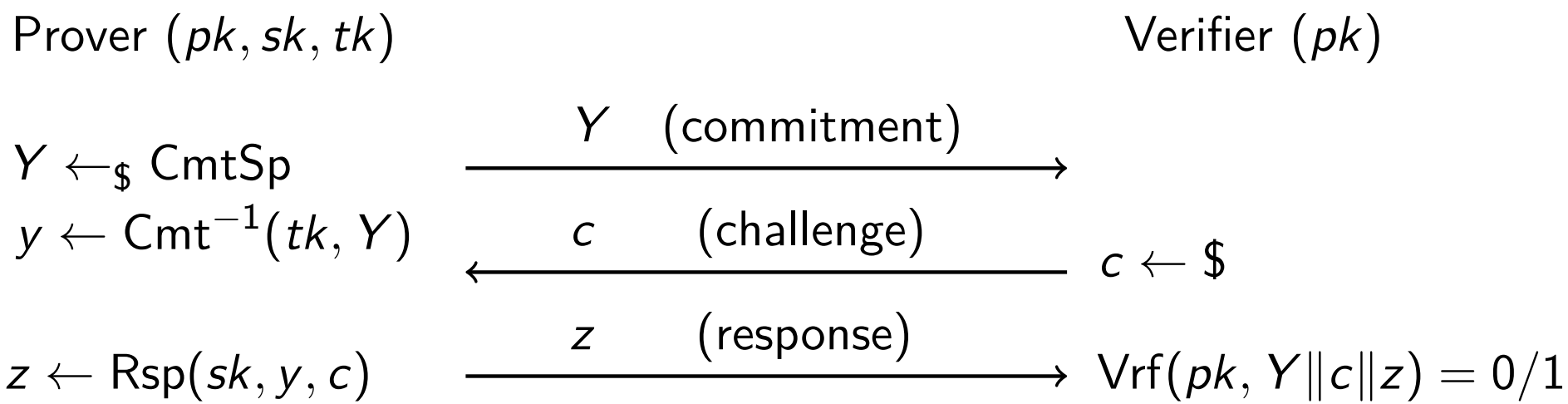
Security

- in both cases: tight reductions

Identification schemes



Identification schemes with trapdoor

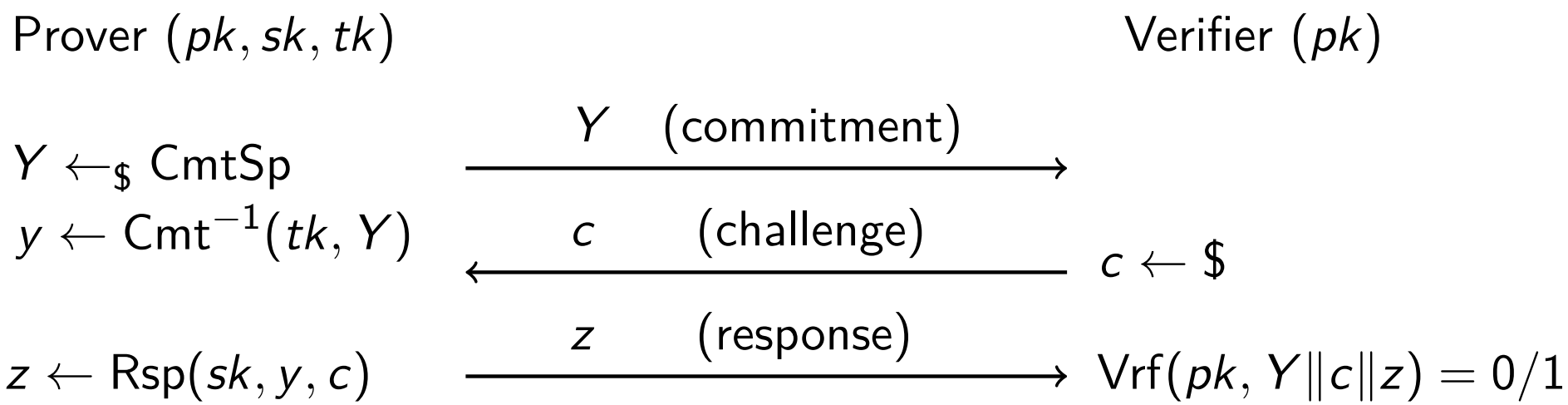


Trapdoor property

- given trapdoor tk, algorithm $\mathsf{Cmt}^{-1}(tk, \cdot)$ computes y from Y
- compatible distributions:

$$(Y, y) \leftarrow_\$ \mathsf{Cmt} \qquad \approx \qquad Y \leftarrow_\$ \mathsf{CmtSp};\ y \leftarrow \mathsf{Cmt}^{-1}(tk, Y)$$

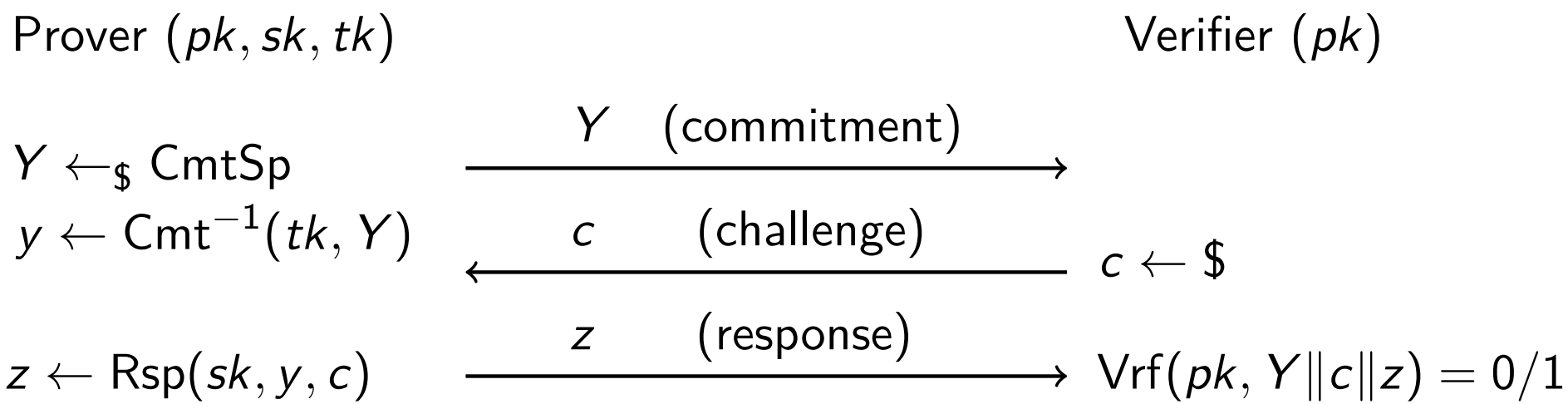
Identification schemes: classical security notions



Impersonation resilience

- adversary has access to
  - public key pk
  - transcript oracle: provides fresh Y, c, z
  - challenge oracle: on input Y provides fresh c, expects z
- goal of adversary: forge valid transcript
- transcript oracle models passive attack
- IMP-PA of [AABN] allows at most one challenge query

Identification schemes: obtaining signatures



Signatures from IMP-PA

- via Fiat-Shamir transform
- reduction from IMP-PA not tight: reset lemma loses factor q_H

Observations

- untight because of single challenge query
- untight because of free choice of commitment
- alternative notions that allow for tight reductions/instantiations?

Identification schemes: new security notions

Constrained impersonation framework

- four variants: CIMP-xy with $xy \in \{CC, CU, UC, UU\}$
- adversary has access to
  - public key pk
  - transcript oracle: provides fresh Y, c, z
  - challenge oracle of type xy
- goal of adversary: forge valid transcript
- multiple queries allowed to both oracles

Meaning of $xy \in \{CC, CU, UC, UU\}$

- C for 'chosen', U for 'unchosen'
- $x = C$: commitment chosen by adversary
- $x = U$: commitment reused from honest transcript
- $y = C$: challenge chosen by adversary
- $y = U$: challenge picked honestly (at random)

Note CIMP-CU is multi-challenge version of IMP-PA

Identification schemes: new security notions

Games for CIMP-$\{CU, CC, UC, UU\}$

Game **CIMP**

$(pk, sk) \leftarrow \mathsf{KGen}$

$z \leftarrow \mathcal{A}^{\mathrm{Tr},\mathrm{Ch}}(pk)$

$v \leftarrow \mathsf{Vrf}(pk, Y \| c \| z)$

Output v

Tr()

$(Y, y) \leftarrow \mathsf{Cmt}$

$c \leftarrow \$$

$z \leftarrow \mathsf{Rsp}(sk, y, c)$

Return $Y \| c \| z$

Ch(Y, c) CC

Return $Y \| c \| \_\_$

Ch(Y) CU

$c \leftarrow \$$

Return $Y \| c \| \_\_$

Ch(i, c) UC

$Y \leftarrow Y_i$

Return $Y \| c \| \_\_$

Ch(i) UU

$Y \leftarrow Y_i$

$c \leftarrow \$$

Return $Y \| c \| \_\_$

Identification schemes: new security notions

Games for CIMP-$\{CU, CC, UC, UU\}$

Game **CIMP**

$(pk, sk) \leftarrow \mathsf{KGen}$

$z \leftarrow \mathcal{A}^{\mathrm{Tr},\mathrm{Ch}}(pk)$

$v \leftarrow \mathsf{Vrf}(pk, Y\|c\|z)$

Output v

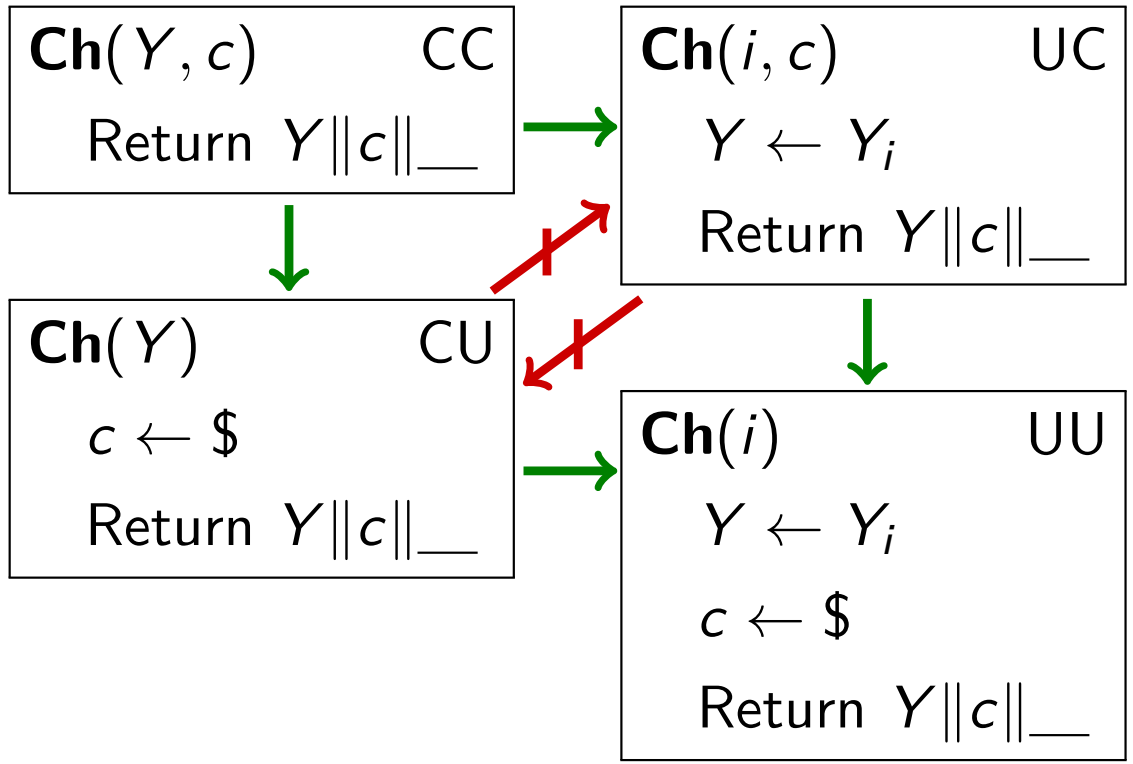
Tr()

$(Y, y) \leftarrow \mathsf{Cmt}$

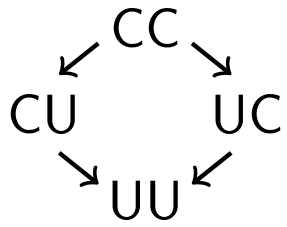
$c \leftarrow \$$

$z \leftarrow \mathsf{Rsp}(sk, y, c)$

Return $Y\|c\|z$



Identification schemes: new security notions



Games for CIMP-$\{CU, CC, UC, UU\}$

Game **CIMP**

$(pk, sk) \leftarrow \mathsf{KGen}$

$z \leftarrow \mathcal{A}^{\mathrm{Tr},\mathrm{Ch}}(pk)$

$v \leftarrow \mathsf{Vrf}(pk, Y\|c\|z)$

Output v

Tr()

$(Y, y) \leftarrow \mathsf{Cmt}$

$c \leftarrow \$$

$z \leftarrow \mathsf{Rsp}(sk, y, c)$

Return $Y\|c\|z$

Ch(Y, c) CC

Return $Y\|c\|\_\_$

Ch(Y) CU

$c \leftarrow \$$

Return $Y\|c\|\_\_$

Ch(i, c) UC

$Y \leftarrow Y_i$

Return $Y\|c\|\_\_$

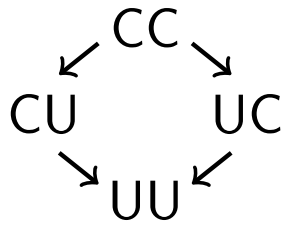
Ch(i) UU

$Y \leftarrow Y_i$

$c \leftarrow \$$

Return $Y\|c\|\_\_$

Signatures from ID schemes



Fiat-Shamir (our view on it)

- no restriction on commitment Y, challenge c from RO
- corresponds to CIMP-CU notion
- no trapdoor required for ID scheme

Sign(sk, m)

$(Y, y) \leftarrow_{\$} \mathsf{Cmt}$

$c \leftarrow H(Y, m)$

$z \leftarrow \mathsf{Rsp}(sk, y, c)$

$\sigma \leftarrow (Y, z)$

Vrf(vk, m, σ)

$(Y, z) \leftarrow \sigma$

$c \leftarrow H(Y, m)$

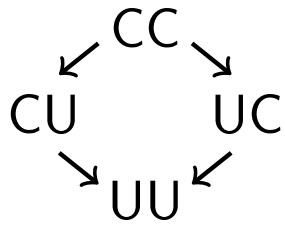
$T \leftarrow Y \| c \| z$

$v \leftarrow \mathsf{Vrf}(vk, T)$

Security

- UF tightly reduces to CIMP-CU

Signatures from ID schemes



MdCmt (message-dependent commitment)

- commitment Y from RO, no restriction on challenge c
- corresponds to CIMP-UC notion
- needs ID scheme with trapdoor

Sign(sk, m)

$Y \leftarrow H(m)$

$y \leftarrow \mathrm{Cmt}^{-1}(tk, Y)$

$c \leftarrow \$$

$z \leftarrow \mathrm{Rsp}(sk, y, c)$

$\sigma \leftarrow (c, z)$

Vrf(vk, m, σ)

$(c, z) \leftarrow \sigma$

$Y \leftarrow H(m)$

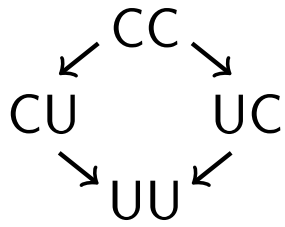
$T \leftarrow Y \| c \| z$

$v \leftarrow \mathrm{Vrf}(vk, T)$

Security

- UUF tightly reduces to CIMP-UC

Signatures from ID schemes



MdCmtCh (message-dependent commitment and challenge)

- commitment Y and challenge c from RO
- corresponds to CIMP-UU notion
- needs ID scheme with trapdoor

Sign(sk, m)

$Y \leftarrow H_1(m)$

$y \leftarrow \mathsf{Cmt}^{-1}(tk, Y)$

$b \leftarrow_{\$} \{0,1\}$

$c \leftarrow H_2(m \| b)$

$z \leftarrow \mathsf{Rsp}(sk, y, c)$

$\sigma \leftarrow (b, z)$

Vrf(vk, m, σ)

$(b, z) \leftarrow \sigma$

$Y \leftarrow H_1(m)$

$c \leftarrow H_2(m \| b)$

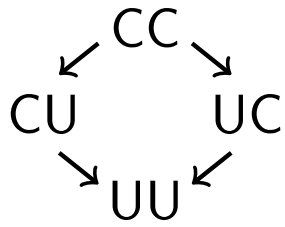
$T \leftarrow Y \| c \| z$

$v \leftarrow \mathsf{Vrf}(vk, T)$

Security

- UUF tightly reduces to CIMP-UU

Signatures from ID schemes



MdCh (message-dependent challenge)

- no restriction on commitment Y, challenge c from RO
- salt added to message
- no trapdoor required for ID scheme

Sign(sk, m)

$(Y, y) \leftarrow_{\$} \mathrm{Cmt}$

$s \leftarrow \$$

$c \leftarrow H(m \| s)$

$z \leftarrow \mathrm{Rsp}(sk, y, c)$

$\sigma \leftarrow (Y, s, z)$

Vrf(vk, m, σ)

$(Y, s, z) \leftarrow \sigma$

$c \leftarrow H(m \| s)$

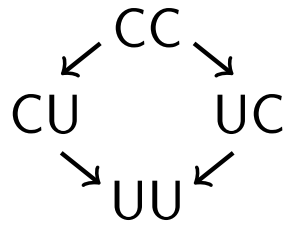
$T \leftarrow Y \| c \| z$

$v \leftarrow \mathrm{Vrf}(vk, T)$

Security

- UF tightly reduces to CIMP-CC

Achieving CIMP-xy security



Theory

If ID scheme is HVZK and extractable

- KR $\Rightarrow$ CIMP-UC (tight)
- KR $\Rightarrow$ CIMP-UU (tight)
- KR $\Rightarrow$ CIMP-CU (loses q_{ch})
- CIMP-CC cannot be reached

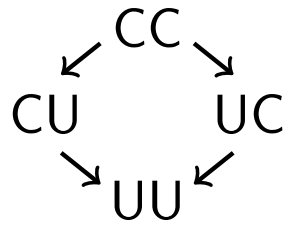
ID scheme where $Y = \epsilon$ and $z = \mathsf{Sign}(sk, c)$ provides CIMP-CC

Practice

Guillou-Quisquater is trapdoor and gives CIMP-UC, CIMP-UU, CIMP-CU

- In **RSA** setting: **secret key** $x \in \mathbb{Z}_N$; **public key** $X = x^e$
- **Cmt**: $y \leftarrow_\$ \mathbb{Z}_N$; $Y \leftarrow y^e$
- **Cmt**$^{-1}$: $y \leftarrow Y^d$
- **Rsp**: $z \leftarrow yx^c$

Understanding Swap



Hybrid AR ∘ MdCmt

- MdCmt: CIMP-UC ⇒ UUF
- AR: UUF ⇒ UF

Sign(sk, m)

$\underline{s} \leftarrow \$$

$Y \leftarrow H(m, \underline{s})$

$y \leftarrow \mathrm{Cmt}^{-1}(tk, Y)$

$c \leftarrow \$$

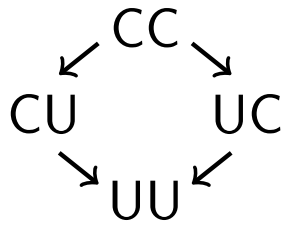
$z \leftarrow \mathrm{Rsp}(sk, y, c)$

$\sigma \leftarrow (c, z, \underline{s})$

Observations

- Swap is optimized AR ∘ MdCmt
- DR ∘ MdCmtCh has shorter signatures, requires weaker assumption

Understanding Swap



Hybrid AR ∘ MdCmt

- MdCmt: CIMP-UC ⇒ UUF
- AR: UUF ⇒ UF

Sign(sk, m)
$\underline{s} \leftarrow \$$
$Y \leftarrow H(m, \underline{s})$
$y \leftarrow \mathsf{Cmt}^{-1}(tk, Y)$
$c \leftarrow \$$
$z \leftarrow \mathsf{Rsp}(sk, y, c)$
$\sigma \leftarrow (c, z, \underline{s})$

Ad hoc

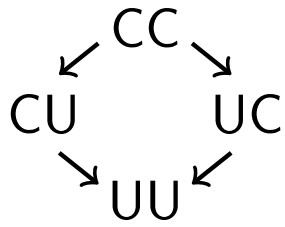
- Swap: CIMP-UC ⇒ UF
- actually: FACT ⇒ UF

Sign(sk, m)
$c \leftarrow \$$
$Y \leftarrow H(m, c)$
$y \leftarrow \mathsf{Cmt}^{-1}(tk, Y)$
$z \leftarrow \mathsf{Rsp}(sk, y, c)$
$\sigma \leftarrow (c, z)$

Observations

- Swap is optimized AR ∘ MdCmt
- DR ∘ MdCmtCh has shorter signatures, requires weaker assumption

Better than Swap



Hybrid DR $\circ$ MdCmtCh

- MdCmtCh: CIMP-UU $\Rightarrow$ UUF
- DR: UUF $\Rightarrow$ UF

Sign(sk, m)
$Y \leftarrow H_1(m)$
$y \leftarrow \mathsf{Cmt}^{-1}(tk, Y)$
$b \leftarrow H_3(sk, m)$
$c \leftarrow H_2(m \| b)$
$z \leftarrow \mathsf{Rsp}(sk, y, c)$
$\sigma \leftarrow (b, z)$

Ad hoc

- Swap: CIMP-UC $\Rightarrow$ UF
- actually: FACT $\Rightarrow$ UF

Sign(sk, m)
$c \leftarrow \$$
$Y \leftarrow H(m, c)$
$y \leftarrow \mathsf{Cmt}^{-1}(tk, Y)$
$z \leftarrow \mathsf{Rsp}(sk, y, c)$
$\sigma \leftarrow (c, z)$

Observations

- in practice: FACT $\rightarrow$ UF w/ tight reduction
- compact signature: only 1 bit overhead

Conclusion

Contributions

- ID schemes with trapdoors
  - instantiations from GQ, MR, CFP
- new transforms: (trapdoor) ID $\rightarrow$ signature
  - depend on new security requirements for ID
  - tight reductions in all cases
- understanding Swap
  - finding the right abstraction boundaries

Thanks

`http://eprint.iacr.org/2015/1157`