RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CRYP-F02

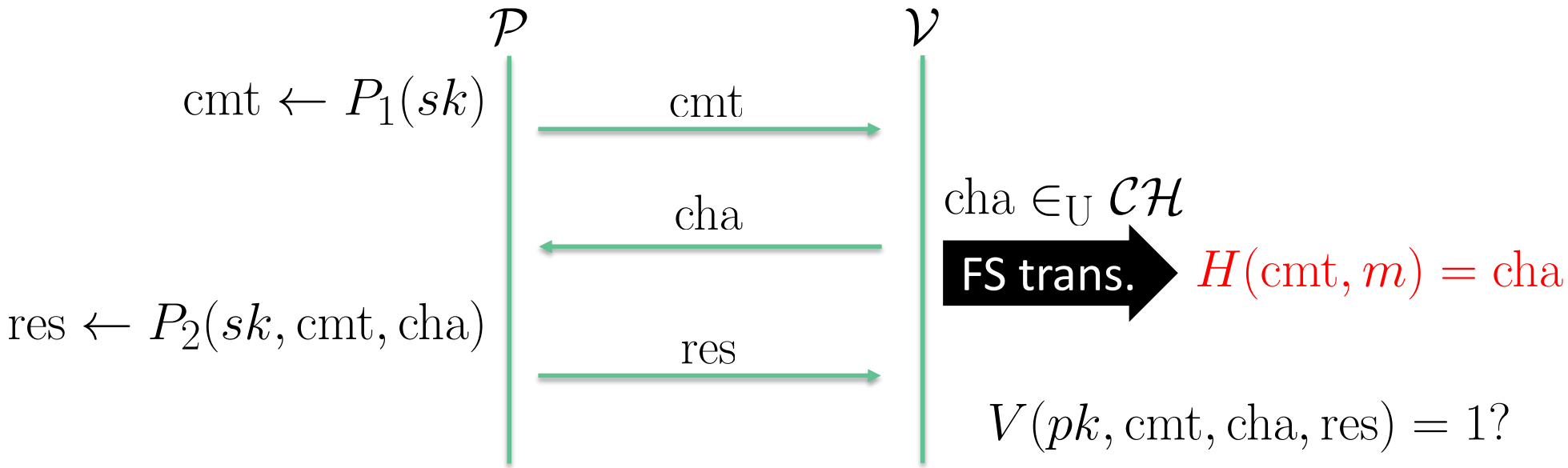
Public Key Cryptography: Theory One-More Assumptions Do Not Help Fiat-Shamir-type Signature Schemes in NPROM

Masayuki Fukumitsu, Shingo Hasegawa

Associate Professor, Assistant Professor
Hokkaido Information University, Tohoku University

Fiat-Shamir-type (FS-type) Signature Schemes

Signature Schemes derived via the FS transformation [FS87]
e.g. Schnorr [Sch91], Guillou-Quisquater (GQ) [GQ88], Okamoto [Oka93], Lyubashevsky [Lyu08]



Security Proofs in Random Oracle Model

There are affirmative results on the provable security of FS-type sig.

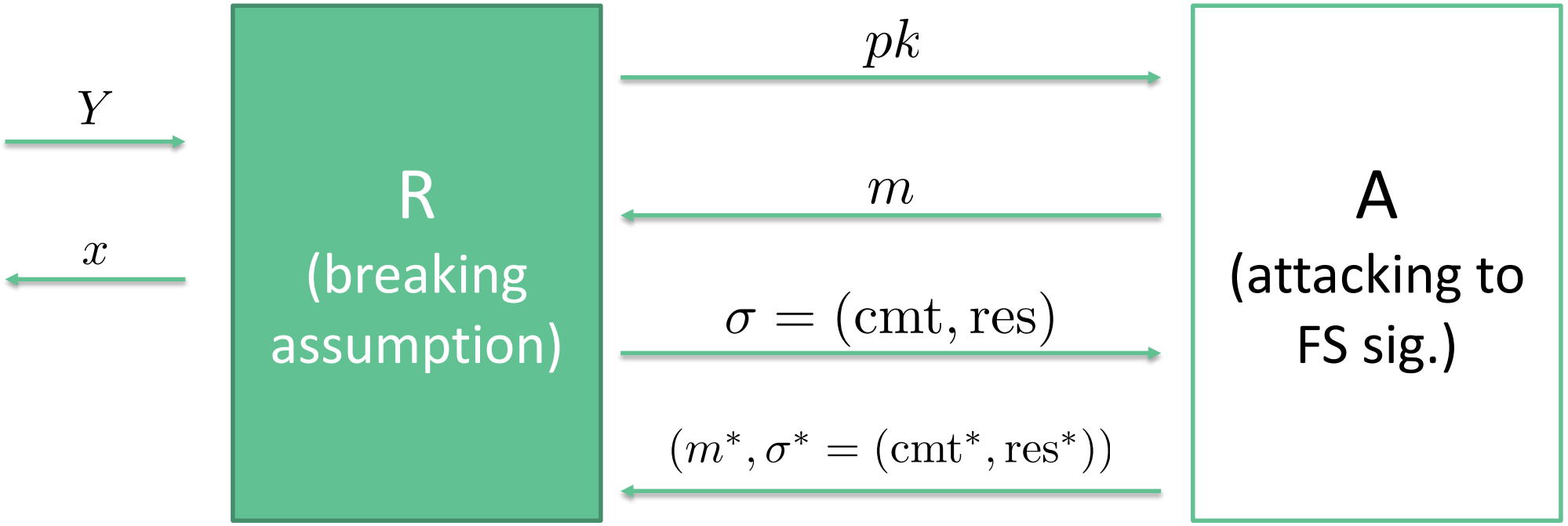
	Assumption on Underlying ID		Provable Security Of its FS-type sig.
[PS00]	HVZKPoK	⇒	seuf-cma
[AABN08]	imp-pa secure	⇔	seuf-cma

Instantiations:

- Schnorr signature scheme is secure under the discrete log (DL) assumption
- GQ signature scheme is secure under the RSA assumption

What Does Mean FS-type Signature Is Secure?

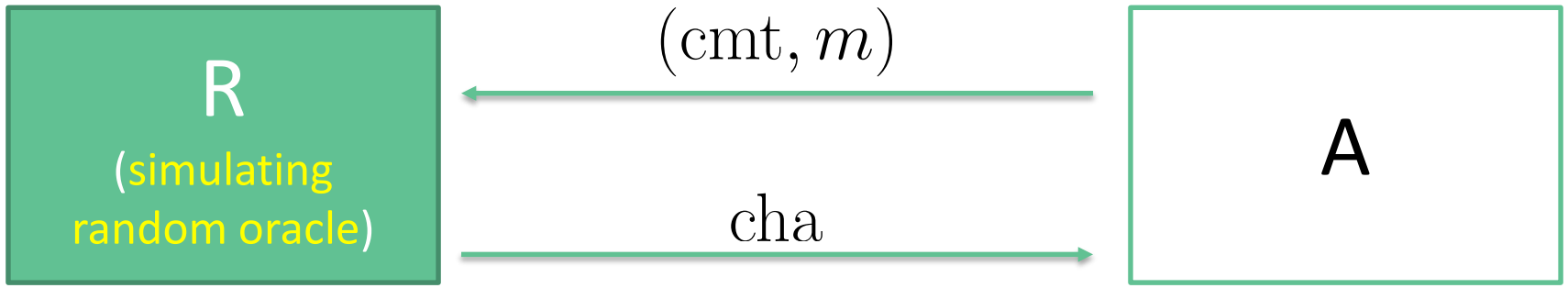
There is a polytime reduction algorithm R which breaks an underlying cryptographic assumption by accessing an adversary algorithm A against a designated FS-type signature scheme.



Proof Techniques

The results [PS00, AABN08] rely on the followings:

- Forking Lemma
- Random Oracle Model
  - Is a.k.a. Ideal security model
  - Restricts any party to obtain any hash value from the random oracle
  - Is applied to prove the security of many cryptographic schemes



Impossibility Result: Security Proof in Standard Model

The security of FS-type signature schemes
is known to be unprovable in standard model [PV05].

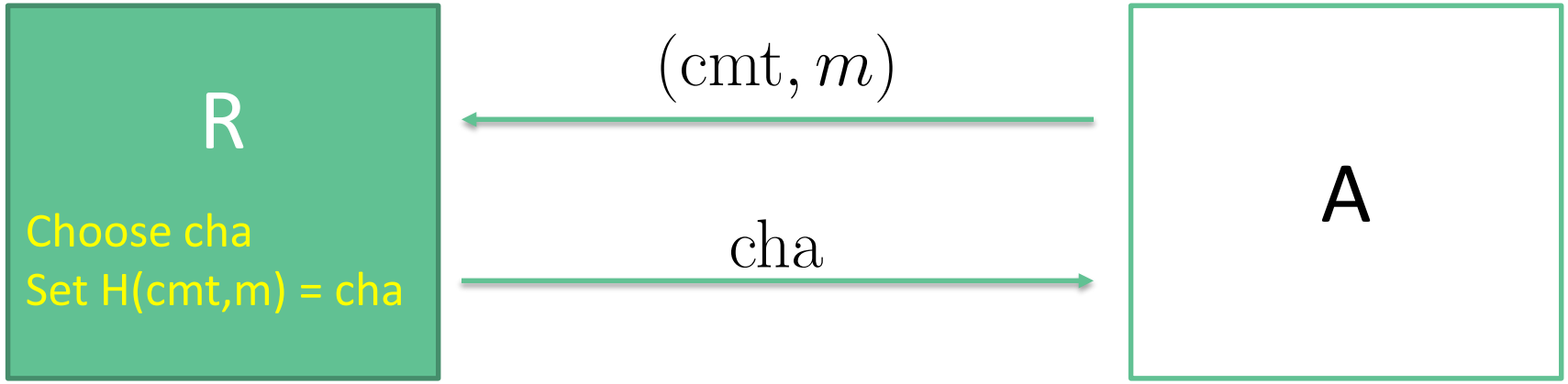
As far as some restricted reductions are concerned,

- OM-DL assumption holds ⇒
  Schnorr signature scheme cannot be proven from the DL assumption.
- OM-RSA assumption holds ⇒
  GQ signature scheme cannot be proven from the RSA assumption.

Why is ROM Strong?

A reduction R in ROM utilize the following ideal properties:

- Observing Property
  - R can observe all pairs of a query and its response on the random oracle.
- Programming Property
  - R can arbitrarily set a hash value of any query.



Intermediate Model between Standard Model and ROM

	Computing Hash	Programming	
ROM	By Random Oracle	Allowed	Ideal
NPROM	By Random Oracle	Not Allowed	⇳
Standard Model	Self	Not Allowed	real

Non-Programmable ROM [FLRSST10] is a security model in which a random oracle;

- outputs a hash value as in the ROM; but
- is dealt with an independent party.

Impossibility Result: Security Proof in NPROM

- Fischlin-Fleischhacker [FF13]
  OM-DL assumption holds ⇒
  Schnorr signature is unprovable to be secure in NPROM from the DL assumption via single-instance reductions.
- Fukumitsu-Hasegawa [FH16, FH18]
  Extend Fischlin-Fleischhacker result to cover many FS-type signature schemes

These results only consider the security from non-interactive assumptions.

Impossibility results from interactive assumptions

There are impossibility results on the provable security of only Schnorr signature from interactive assumptions:

- Fukumitsu-Hasegawa [FH17]
  - in NPROM
  - from the OM-DL assumption
- Fleischhacker-Jager-Schröder [FJS19]
  - even in ROM
  - from specific interactive assumptions
  - but, only for tight and generic reduction

Remained Question

Can one prove that FS-type signatures are secure from interactive assumptions in NPROM via a reasonable reduction?

- Can one expand a result for many types?
  - GQ, KW, Okamoto, Lyubashevsky, …
- Reasonable reductions
  - non-restriction on the tightness and internal operations

RSAConference2020

Our Contribution

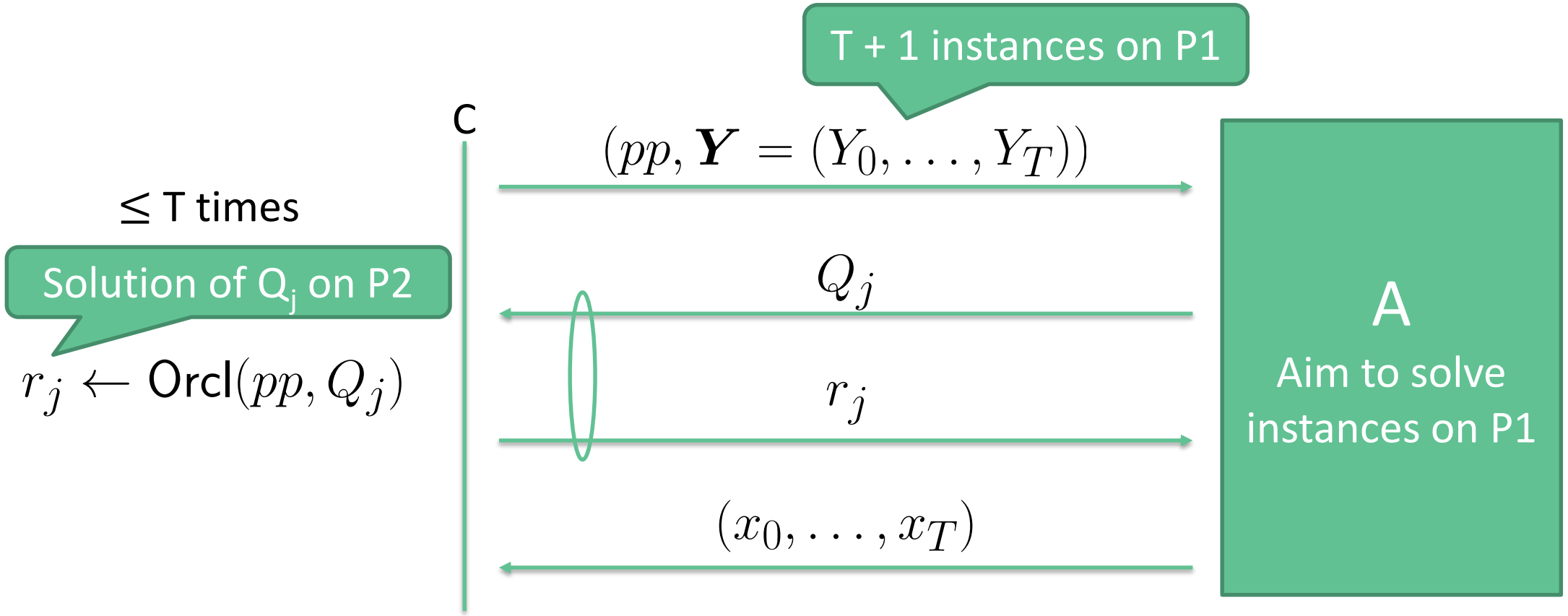
Informal Statement

We give a negative circumstantial evidence on the remained question by the following theorem.

Some FS-type signatures are unprovable to be secure in NPROM from the generalized One-More cryptographic assumptions.

Generalized One-More Cryptographic Assumption[ZZCGZ14]: T-(P1,P2) Assumption

Any PPT adversary A cannot win the following game.



Scope of Type on Underlying ID Schemes

- Special Soundness
  - (cmt, cha, res) and (cmt, cha', res') have been found, then a secret key of pk can be extracted in polytime.
    - s.t. cha ≠ cha' and V(pk, cmt, cha, res) = V(pk, cmt, cha', res') = 1
- Unique Key
  - Any public key pk has only one secret key sk.
- Certified (proposed)
  - One can check whether pk has a secret key.
  - DL-based ID schemes [Hes03, Sch91] have this property.
  - This is inspired by [KK13].

Type of Reductions I: Vanilla Reductions

Our result only considers vanilla reductions

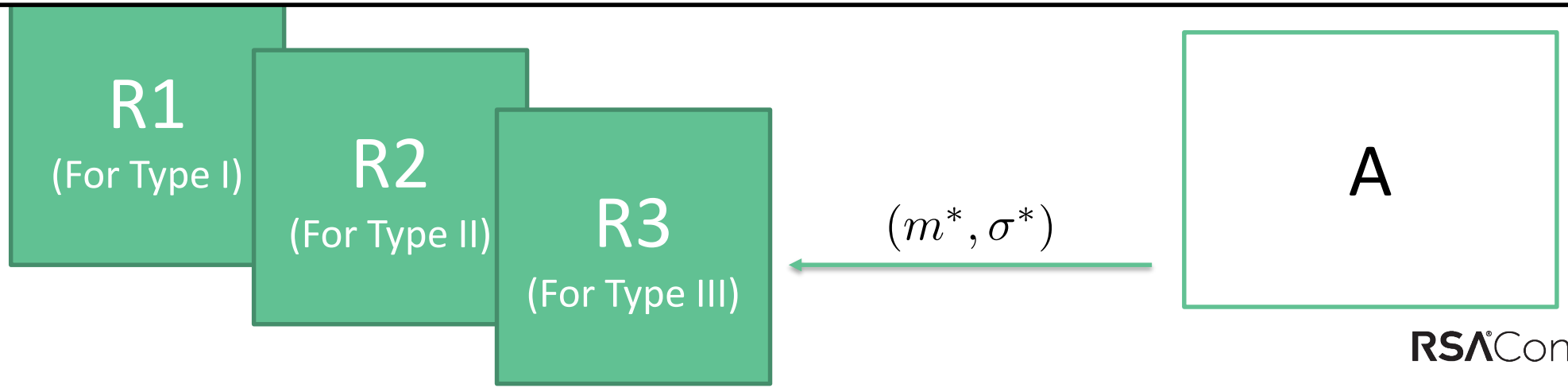
- Definition: A reduction R
  - can invoke an adversary A only once.
  - cannot rewind A
- Feature:
  - No restriction on the tightness, internal operations in R and pk queried to A

Type of Reductions II: Only for Specific Type of Forgery

A reduction works if
the forgery (cmt*,res*) satisfies that a $\mathrm{cmt}*$ part differs from all cmt which appear in the signing oracle phase.

By this restriction, the type guess reduction technique is avoided.

Type Guess Reduction Technique
A reduction is constructed by separating the forged signature by A into several types
e.g. Cramer-Shoup signature [CS00]



Suggestions

- This is a generalization of [FF13, FH17, FH18].
  - Can apply our result to the case on Schnorr signature from the DL assumption and the OM-DL assumption.
- There is a possibility to prove the security of FS-type signatures from non-certified ID schemes:
  - RSA-based ID schemes
  - Lossy ID schemes [AFLT16]
- Other type of reductions has potential

Comparisons: Target Security Reductions

	Model	Security	Tight	Assumption	Type
[Thm8, PV05]	ROM	uuf-cma	only	Non-interact	Algebraic
[FF13]	NPROM	euf-cma		Non-interact	Single-inst.
[FH16]	NPROM	suf-sma		imp-pa of ID	SMI
[Thm.1 FH18]	NPROM	euf-koa		imp-pa of ID	Key-pres.
[Thm2. FH18]	NPROM	euf-cma		Non-interact	Single-inst. key-pres.
[Thm2. PV05]	Standard	uuf-cma		Non-interact	Algebraic
[ours]	NPROM	euf-cma		Generalized OM	Vanilla

RSAConference2020

Concluding Remarks

Summary of Our Result

Some Fiat-Shamir-type signatures are unprovable to be secure in NPROM from T-(P1,P2) assumptions via a vanilla reduction.

- Restriction
  - ID scheme: special soundness, unique key and certified.
  - Reduction: only work when it is given (cmt*,res*) s.t. a cmt$*$ part differs from all cmt which appear in the signing oracle phase.
- Suggestion
  - Our result is a generalization of [FF13, FH17, FH18].
  - At least DL-based FS-type signatures may be unprovable to be secure only by the programming technique.
  - Other type of reductions has potential to prove the security proof.

References (1/3)

[FS87] Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. CRYPTO 1986.

[Sch91] Schnorr, C.P.: Efficient signature generation by smart cards. JoC. 4(3), 161–174 (1991).

[GQ88] Guillou, L.C., Quisquater, J.J.: A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. EUROCRYPT 1988.

[Oka93] Okamoto, T.: Provably secure and practical identification schemes and corresponding signature schemes. CRYPTO 1992.

[Lyu08] Lyubashevsky, V.: Lattice-based identification schemes secure under active attacks. PKC 2008.

[PS00] Pointcheval, D., Stern, J.: Provably secure blind signature schemes. ASIACRYPT 1996.

[AABN08] Abdalla, M., An, J.H., Bellare, M., Namprempre, C.: From identification to signatures via the Fiat-Shamir transform: necessary and sufficient conditions for security and forward-security. IEEE Trans. Inf. Theory 54(8), 3631–3646 (2008).

References (2/3)

[PV05] Paillier, P., Vergnaud, D.: Discrete-log-based signatures may not be equivalent to discrete log. ASIACRYPT 2005.

[FLRSST10] Fischlin, M., Lehmann, A., Ristenpart, T., Shrimpton, T., Stam, M., Tessaro, S.: Random oracles with(out) programmability. ASIACRYPT 2010.

[FF13] Fischlin, M., Fleischhacker, N.: Limitations of the meta-reduction technique: the case of schnorr signatures. EUROCRYPT 2013.

[FH16] Fukumitsu, M., Hasegawa, S.: Impossibility on the provable security of the Fiat-Shamir-type signatures in the nonprogrammable random oracle model. ISC 2016.

[FH18] Fukumitsu, M., Hasegawa, S.: Black-box separations on Fiat-Shamir-type signatures in the non-programmable random oracle model. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E101.A(1), 77–87 (2018).

[FH17] Fukumitsu, M., Hasegawa, S.: Impossibility of the provable security of the Schnorr signature from the one-more DL assumption in the non-programmable random oracle model. ProvSec 2017.

References (3/3)

[FJS19] Fleischhacker, N., Jager, T., Schr¨ oder, D.: On tight security proofs for Schnorr signatures. J. Cryptol. 32(2), 566–599 (2019).

[ZZCGZ14] Zhang, Z., Chen, Y., Chow, S.S.M., Hanaoka, G., Cao, Z., Zhao, Y.: Black-box separations of hash-and-sign signatures in the non-programmable random oracle model. ProvSec 2015.

[KK13] Kakvi, S.A., Kiltz, E.: Optimal security proofs for full domain hash, revisited. EUROCRYPT 2012.

[CS00] Cramer, R., Shoup, V.: Signature schemes based on the strong RSA assumption. ACM Trans. Inf. Syst. Secur. 3(3), 161–185 (2000).

[AFLT16] Abdalla, M., Fouque, P.A., Lyubashevsky, V., Tibouchi, M.: Tightly secure signatures from lossy identification schemes. J. Cryptol. 29(3), 597–631 (2016).