Unique Aggregate Signatures with Applications to Distributed Verifiable Random Functions

Veronika Kuchta and Mark Manulis

CANS 2013, Paraty, Brazil

November 21, 2013

Overview

Unique Signature Schemes

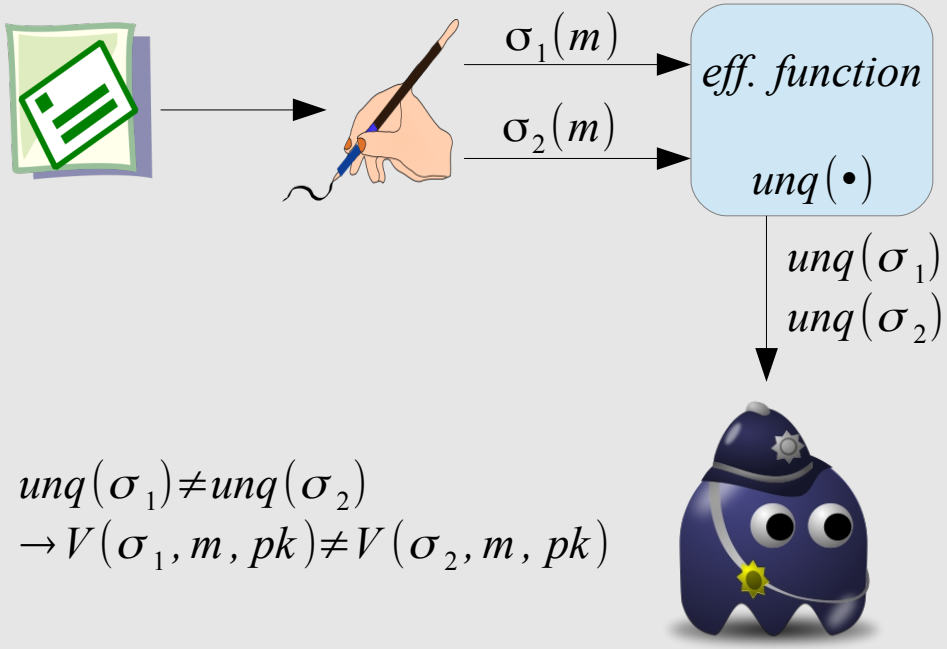
- Verifiable Random Functions

Unique Aggregate Signature Schemes

- Distributed Verifiable Random Functions

Unique Signature Scheme

Definition: **Unique** signature scheme



$unq(\sigma_1) \neq unq(\sigma_2)$
$\rightarrow V(\sigma_1, m, pk) \neq V(\sigma_2, m, pk)$

$\rightarrow$ σ is unique, if $unq(\sigma_1) = unq(\sigma_2)$

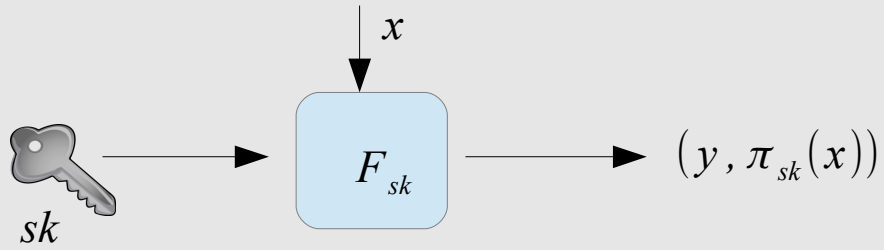
- Introduced by Goldwasser and Ostrovsky [CRYPTO'92]
- Existence of efficient function: $unq(.)$
- For deterministic signatures: $unq(\sigma) = \sigma$
- For probabilistic signatures: $unq(\sigma) = \tilde{\sigma}$

  $\rightarrow$ $\tilde{\sigma}$ unique component

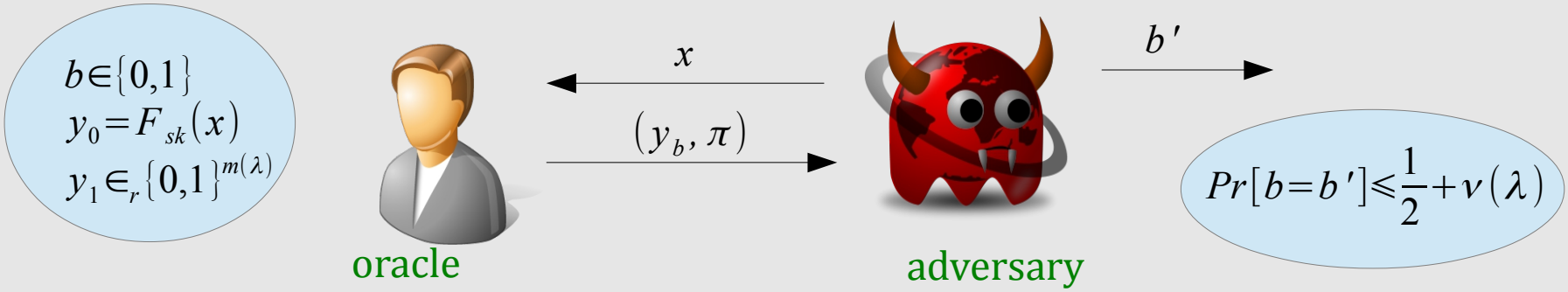
Main application: Construction of Verifiable Random Functions (VRF)

Verifiable Random Functions (VRF)

- First introduced by Micali-Rabin-Vadhan [FOCS'99]
- **Definition:**

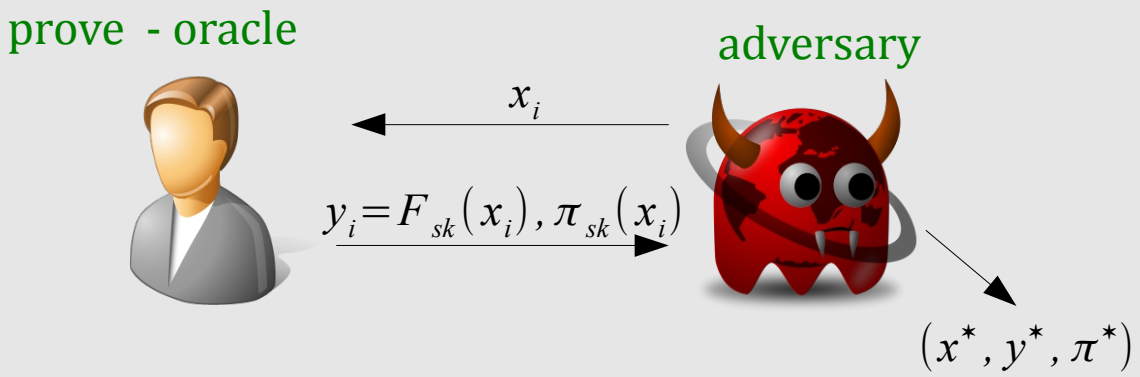


- π_{sk} proves correctness of computation $y = F_{sk}(x)$
- Uniqueness $y_1 \neq y_2, \pi_1 \neq \pi_2 \rightarrow V(x, y_1, \pi_1) \neq V(x, y_2, \pi_2)$
- Pseudorandomness:



VRF from Unique Signature Scheme

- Construction of VUF with the following properties:
  - Uniqueness: $y_1 \neq y_2, \pi_1 \neq \pi_2 \rightarrow V(x, y_1, \pi_1) \neq V(x, y_2, \pi_2)$
  - Provability: $y = F_{sk}(x)$
  - Unpredictability: Secure against adaptive queries



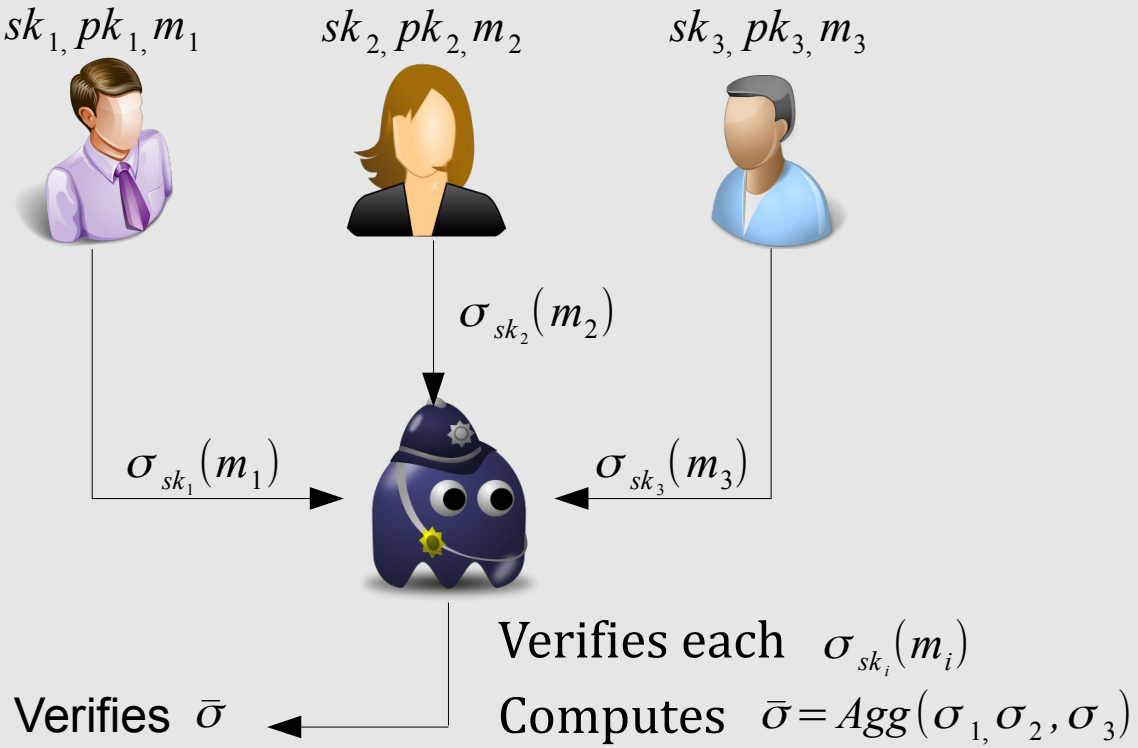
Secure if:
$Pr[Vrfy(pk^*, x^*, y^*, \pi^*) = 1] \leqslant \epsilon$
and x^* was never queried to prove-oracle

- Consider signer's sk as secret seed.
  - $\rightarrow unq(\sigma) = F_{sk}(x_i)$
  - $\rightarrow \sigma = \pi_{sk}(x_i)$
- Apply Goldreich-Levin hardcore bit to convert VUF into VRF [MRV99]

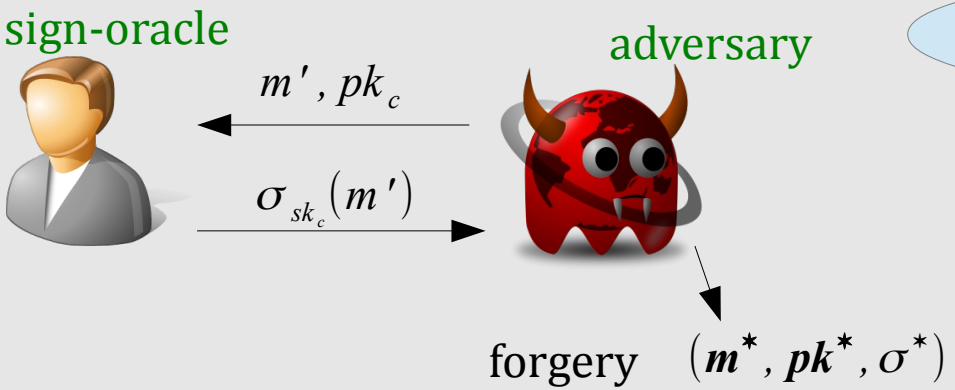
Application of VRF: Implication of random oracle (Goldreich et al. [1987])

Unique Aggregate Signature Scheme (UAS)

Definition:



Security:



m_c never queried to sign

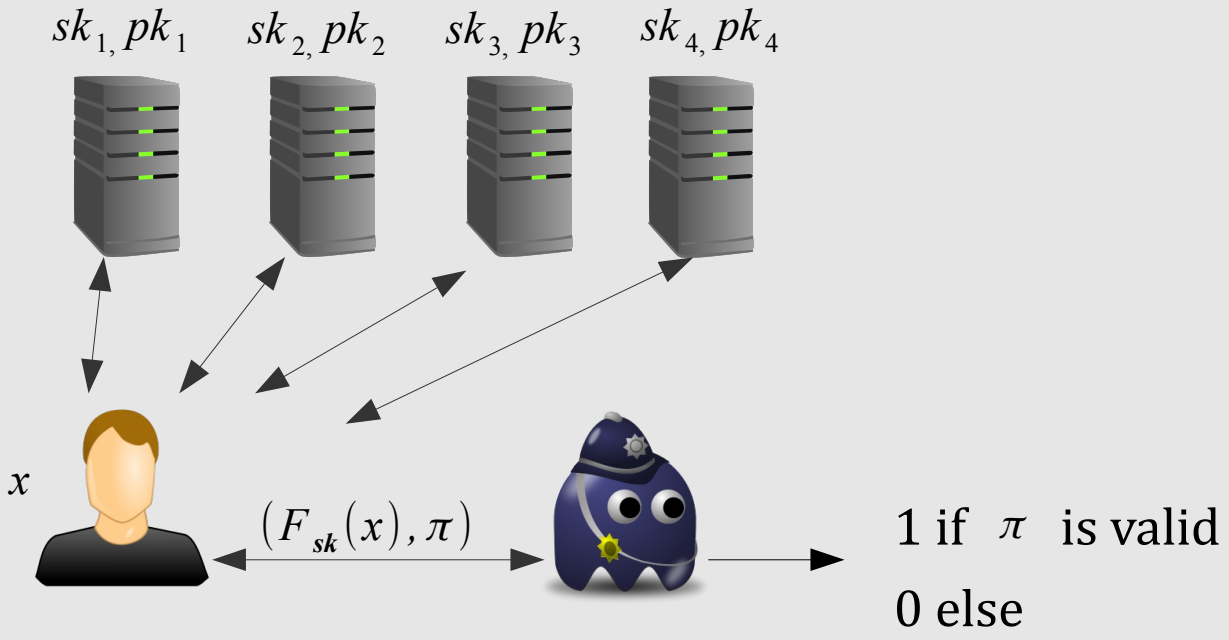
Secure if:

$Pr[Vrfy(\boldsymbol{m}^*, \boldsymbol{pk}^*, \sigma^*)=1] \leqslant \epsilon$

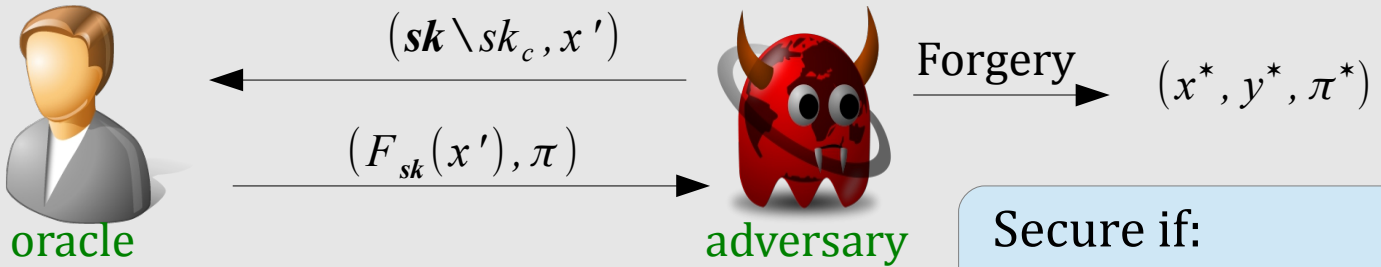
Unique UAS Schemes and DVRF

- We proved unqueness for Boneh-Gentry-Lynn-Shacham AS scheme [EUROCRYPT'03]
- We defined uniqueness for sequential aggregate signatures (USAS)
- Proof of uniqueness for Lu-Ostrovsky-Sahai-Shacham-Waters SAS scheme [EUROCRYPT'06]
- Construction of Distributed VUF (DVUF) from UAS/USAS
- Advantages in contrast to Dodis [PKC'03]:
  - Uniqueness+Unforgeability of UAS/USAS
    → Pseudorandomness of DVUF
  - No trusted setup for distribution of secret keys
    → Shared random string

DVUF from UAS



- Uniqueness: $y_1 \neq y_2, \pi_1 \neq \pi_2 \rightarrow V(x, y_1, \pi_1) \neq V(x, y_2, \pi_2)$
- Provability: $y = F_{sk}(x)$
- Unpredictability:



Secure if:

$Pr[Vrfy(x^*, y^*, \pi^*) = 1] \leq \epsilon$

From DVUF to DVRF

- Apply Goldreich-Levin technique → DVRF in shared random string model

- Efficient construction of DVRF presented by Dodis [PKC'03]

  VRF → DVRF using $(t+1, n)$- secret sharing technique

  ⇒ t+1 servers must be honest!!

  Trusted setup for secret key distribution

- Our construction: from UAS/USAS
  - No trust assumption on secret key generation
  - No threshold on the number of honest servers

Applications of DVRF

- Goldreich, Goldwasser, Micali [1987] showed a simulation of random oracle.

- Practical realization of random oracle (Bellare and Rogaway [ACM'93])

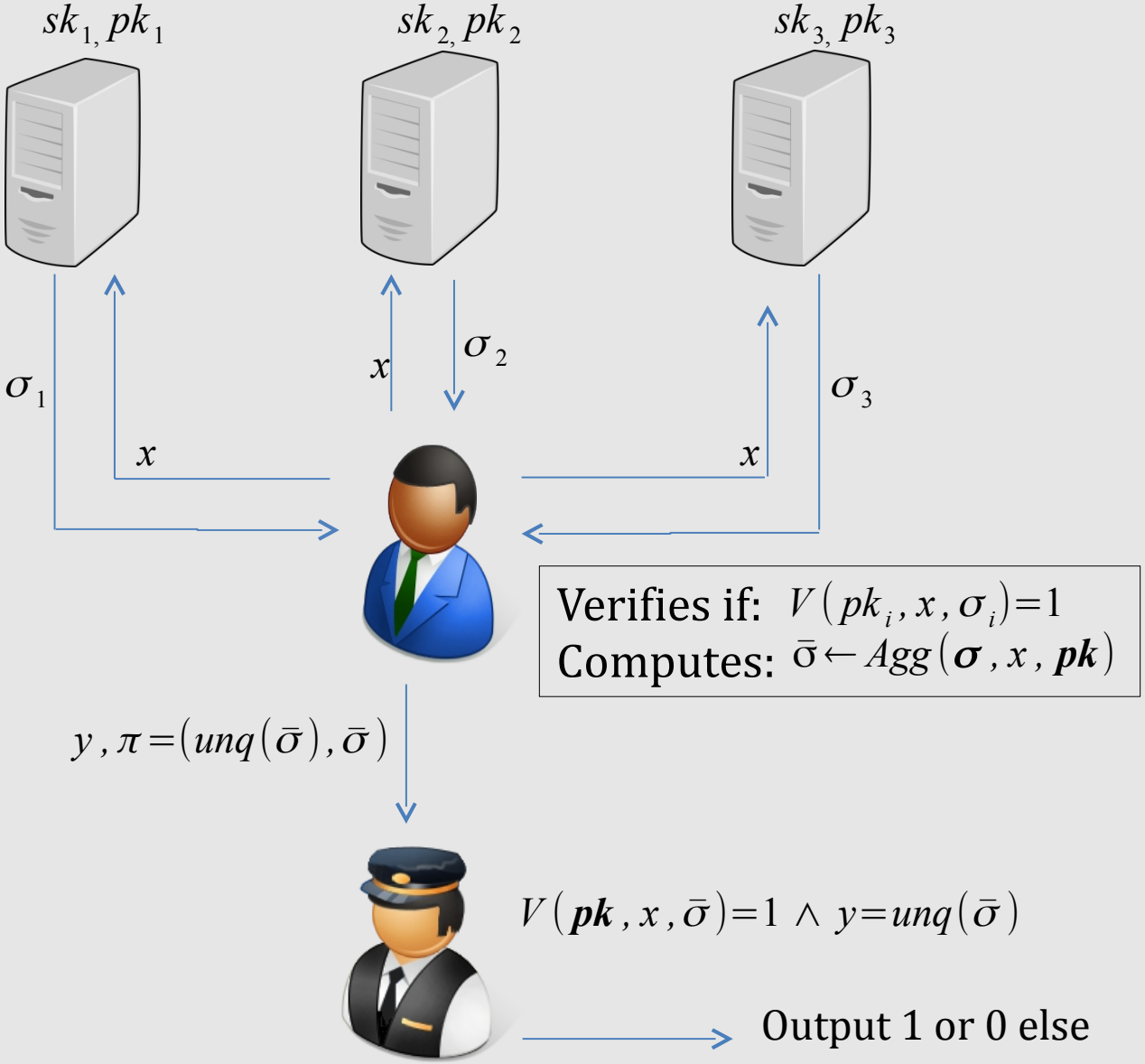
  → Usefull for security proofs in cryptographic schemes.

- Micali et al. [FOCS'99] suggested a realization of random oracle using VRF.

- Distributed version of VRF (Dodis [PKC'03])

  → He distributed the trust of VRF amongst independent parties.

Generic Construction of DVUF from UAS



Conclusions

- Generic Construction of DVUF from USAS

- DVUF construction possible from a special case of aggregate signatures
  ⟶Multisignatures [Boldyreva, PKC'03]

  - Interactive multisignatures: Micali-Ohta-Reyzin [ACM CCS'01], Bagherzandi-Cheon-Jarecki [ACM CCS'08], Bellare-Neven [ACM CCS'06]

  - Non-interactive multisignatures: [Boldyreva, PKC'03], Lu-Ostrovsky-Sahai-Schacham-Waters [EUROCRYPT'06], Zhou-Quian-Li [ISC'11]

BUT:

- All aggregate signatures are non-interactive.

Thank you for your attention!