Pseudorandom Signatures

Relations among Privacy Notions for Digital Signatures

TECHNISCHE UNIVERSITÄT DARMSTADT

Felix Günther

Technische Universität Darmstadt

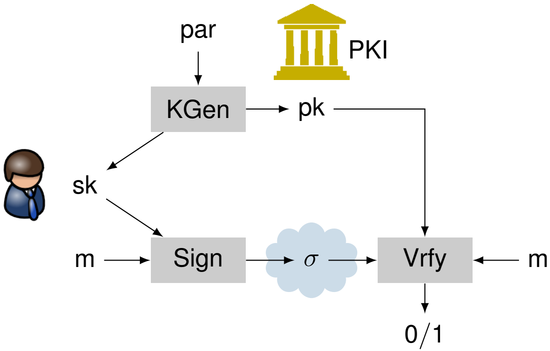
joint work with

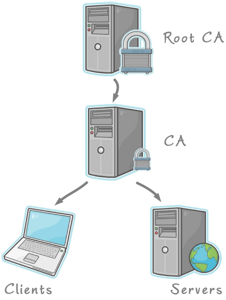
Nils Fleischhacker, Franziskus Kiefer, Mark Manulis, Bertram Poettering

Saarland University (Germany), University of Surrey (UK), Royal Holloway University of London (UK)

Digital Signatures

TECHNISCHE UNIVERSITÄT DARMSTADT





Digital signatures do not offer privacy!

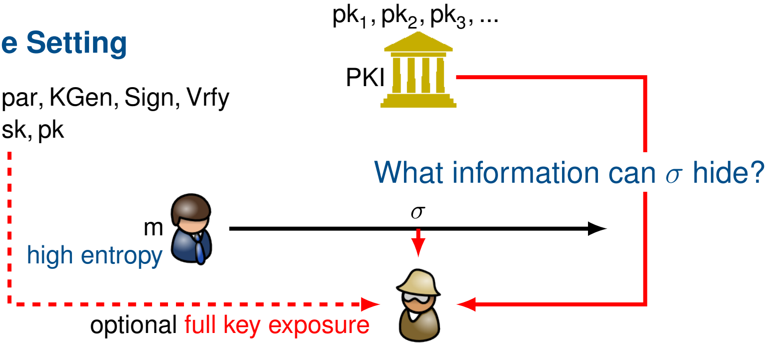
. . . due to public verification.

Privacy for Digital Signatures

Is privacy for digital signatures thus hopeless?

Not quite!

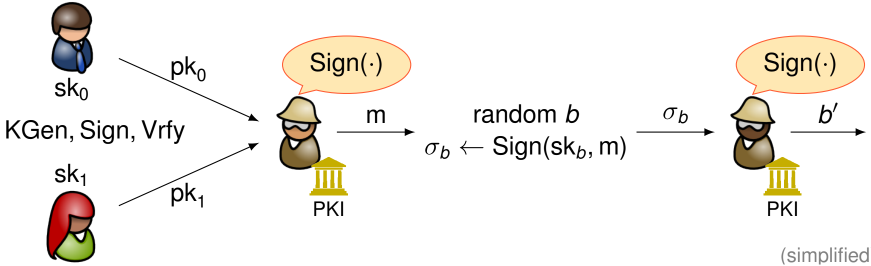
The Setting



Anonymous Signatures

Anonymous Signatures (ANON)

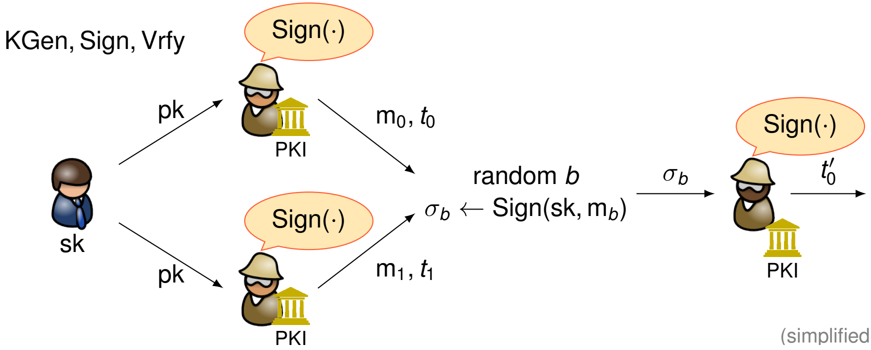
- Yang, Wong, Deng, Wang @ PKC 2006
- Fischlin @ PKC 2007
- Bellare, Duan @ eprint 2009 (non-standard signatures)
- Saraswat, Yun @ ProvSec 2009 (non-standard signatures)
- Zhang, Imai @ IEICE Trans. 92-A 2009 (non-standard signatures)



(simplified)

Confidential Signatures (CONF)

- Dent, Fischlin, Manulis, Stam, Schröder @ PKC 2010 (strong, mezzo, weak)
- Canetti @ CRYPTO 1997 (preliminary ideas)



(simplified)

Applications and Theoretical Aspects of Privacy-Friendly Signatures

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Signatures are often sent together with signed message.

However, anonymous/confidential signatures are useful in

- anonymous auctions (where bid is revealed later)
- anonymous key exchange
- output signing of secure multi-party computation

But signatures (e.g., in European passports [Bringer et al. @ ACNS 2010]) might already be distinguishable by the signing algorithm and parameters used

Existence of anonymous/confidential signatures also raises theoretical questions:

- How are ANON and CONF related?
- Can signature schemes achieve both ANON and CONF?
- Is there a limit on the information that can be hidden?

Relationship between ANON and CONF

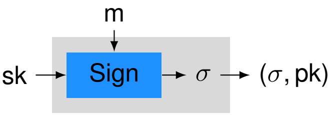
ANON

CONF

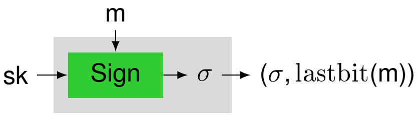
We have two privacy notions, but the work isn't complete. . .

ANON and CONF are independent privacy notions:

- existance of non-private signature schemes (e.g., FDH-RSA)
- black-box separation of ANON and CONF



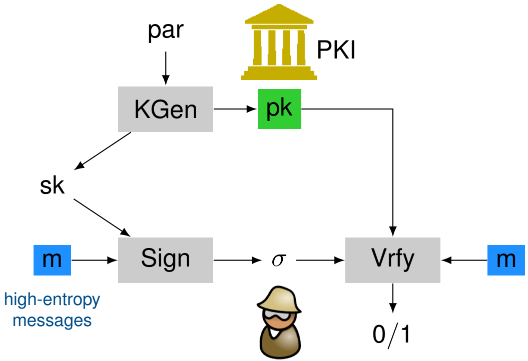
confidential but not anonymous

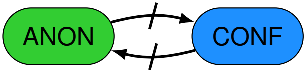


anonymous but not confidential

“State-of-the-Art” Privacy Snapshot

TECHNISCHE UNIVERSITÄT DARMSTADT





Can we achive ANON and CONF at the same time?

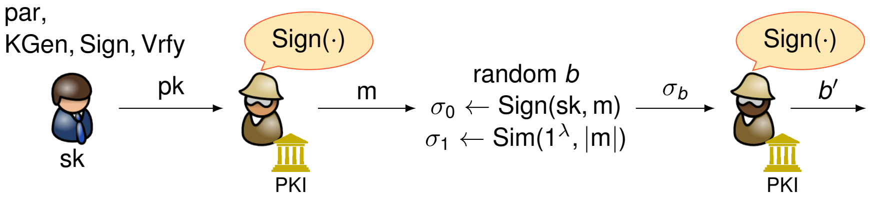
Indistinguishable Signatures

Intuition

Sign(sk, m) $\approx$ Sim(1^λ, |m|) — Sim implicitly knows (par, KGen, Sign, Vrfy)

Indistinguishable Signatures (IND)

There exists a simulator Sim s.t. for all adversaries



(simplified)

Examples of IND Signatures

TECHNISCHE UNIVERSITÄT DARMSTADT

IND signature schemes exist in different crypto settings, e.g.,

- Probabilistic FDH-RSA with padding $\sigma = (H_N(m, r)^d + kN, r)$

  where $H_N\colon \{0,1\}^* \to \mathbb{Z}_N$, $k \in_R [0, \lfloor Z_\lambda / N \rfloor - 1]$, $Z_\lambda \in \mathbb{N}$ of 2λ bits.

- Schnorr scheme (shared $\mathbb{G} = \langle g \rangle$) $\sigma = (c = H(g^r, m), s = sk \cdot c + r \bmod q)$

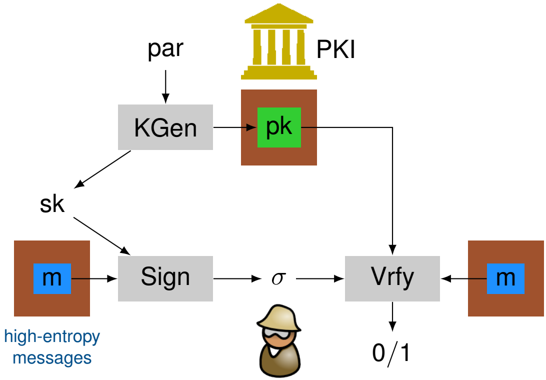
  where $H\colon \{0,1\}^* \to \mathbb{Z}_q$ and $sk \in_R \mathbb{Z}_q$ is the secret key.

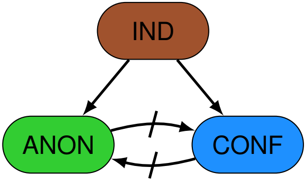
- Boneh-Boyen scheme (shared $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$) $\sigma = (g_1^{1/(x+m+yr)}, r)$

  for uniform $m \in_R \mathbb{Z}_q$ — can be dropped with “hash-then-sign” in ROM.

“So-Far” Privacy Snapshot

TECHNISCHE UNIVERSITÄT DARMSTADT





- IND signatures may still leak par!
  possible to distinguish between security parameters, groups
- IND signatures may still leak specification of (KGen, Sign, Vrfy)!
  possible to distinguish between the (instantiations of) schemes

Pseudorandom Signatures

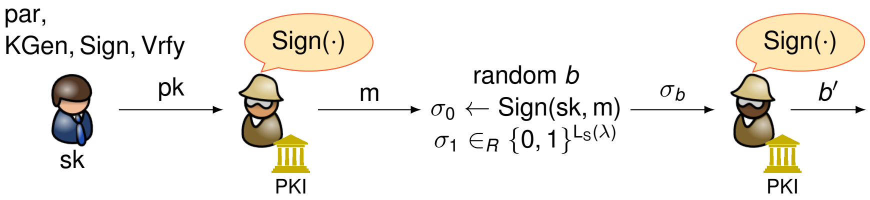
TECHNISCHE UNIVERSITÄT DARMSTADT

Intuition

Sign(sk, m) $\approx$ random string from $\{0,1\}^{L_S(\lambda)}$

where $L_S(\lambda)$ is the length of signatures output by a scheme S on security parameter λ

Pseudorandom Signatures (PR)

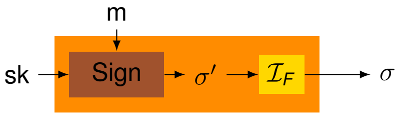


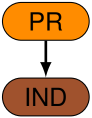
(simplified)

Note: Multiple PR signatures can always be extended to some common length L

IND-to-PR Compiler

- converts IND signatures into PR signatures — in the standard model
- uses admissible encoding $F \colon \{0,1\}^{L_S(\lambda)} \to R$ (Brier et al. @ CRYPTO 2010)
  - F is efficient and invertible by $\mathcal{I}_F$, which maps to uniform distribution in $\{0,1\}^{L_S(\lambda)}$
  - admissible encodings exist for elliptic curves, $\mathbb{Z}_N$, $QR(p)$ and are aggregatable





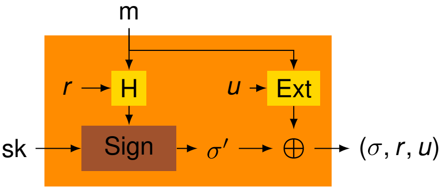
- suitable for IND schemes with regular Sim (uniform output)
- aggregation of encodings helps if σ contains elements from various sets
- very efficient

Direct PR Compiler

TECHNISCHE UNIVERSITÄT DARMSTADT

- works for arbitrary (incl. non-private) signatures — in the standard model
- bases on construction of ANON signature scheme by Fischlin @ PKC 2007
- implies that Fischlin's scheme achieves PR $\Rightarrow$ IND $\Rightarrow$ CONF

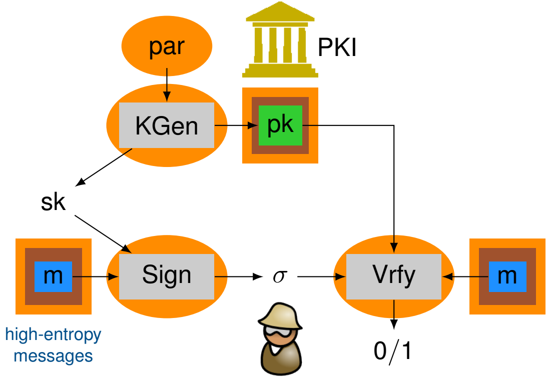
Idea: PR compiler extracts randomness from m to encrypt the signature

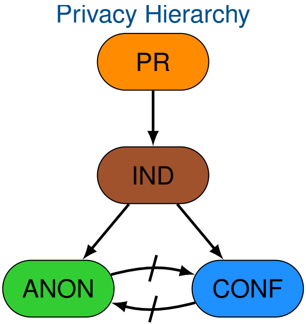


uses associated randomness extractor and hash function

$r, u, \mathrm{H}(\mathrm{m}, r), \mathrm{Ext}(\mathrm{m}, u) \approx r, u, \mathrm{H}(\mathrm{m}, r), v$

Final Privacy Snapshot





many of our results also hold in case of full key exposure

Summary

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy **is** possible for digital signatures!

- complete privacy hierarchy for signatures (PR $\Rightarrow$ IND $\Rightarrow$ $\{$ANON, CONF$\}$)
- constructions for IND-variants of FDH-RSA, Schnorr, Boneh-Boyen
- two generic compilers (IND-to-PR, direct PR) in the standard model

- pseudorandom (PR) signatures hide all information about the signing process — including parameters, instantiations, schemes

All results in our full paper @ **http://eprint.iacr.org/2011/673**, including

- details on full key exposure
- impossibility results for
  - information recovering signatures (generalization of message recovery)
  - deterministic signatures

References I

TECHNISCHE UNIVERSITÄT DARMSTADT

[Brier et al., 2010] Brier, E., Coron, J.-S., Icart, T., Madore, D., Randriam, H., and Tibouchi, M. (2010).
Efficient Indifferentiable Hashing into Ordinary Elliptic Curves.
In *CRYPTO 2010*, volume 6223 of *LNCS*, pages 237–254. Springer.

[Bringer et al., 2010] Bringer, J., Chabanne, H., and Icart, T. (2010).
Password Based Key Exchange Protocols on Elliptic Curves Which Conceal the Public Parameters.
In *ACNS 2010*, volume 6123 of *LNCS*, pages 291–308. Springer.

[Dent et al., 2010] Dent, A. W., Fischlin, M., Manulis, M., Stam, M., and Schröder, D. (2010).
Confidential Signatures and Deterministic Signcryption.
In *PKC 2010*, volume 6056 of *LNCS*, pages 462–479. Springer.

References II

[Fischlin, 2007] Fischlin, M. (2007).
Anonymous Signatures Made Easy.
In *PKC 2007*, volume 4450 of *LNCS*, pages 31–42. Springer.

[Yang et al., 2006] Yang, G., Wong, D. S., Deng, X., and Wang, H. (2006).
Anonymous Signature Schemes.
In *PKC 2006*, volume 3958 of *LNCS*, pages 347–363. Springer.