Generic Double-Authentication Preventing Signatures and a Post-Quantum Instantiation

David Derler[†,1], **Sebastian Ramacher**[‡], Daniel Slamanig[§]

ProvSec'18, October 27, 2018

[1] work done while at Graz University of Technology

† ‡ §

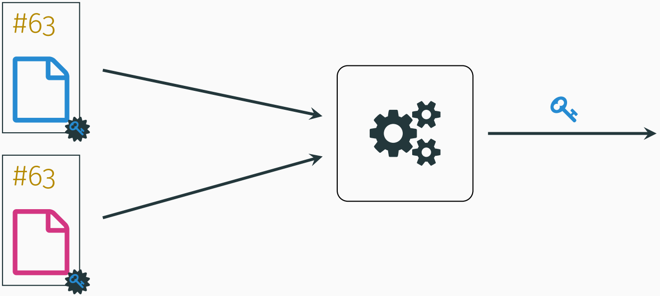
Introduction

Digital Signatures

Applications

- Signing transactions in cryptocurrencies
- Certificate and software signing
- And many more

Double-Authentication Preventing Signatures [PS14]



- Same context (address), different content

» Extract secret key

- Extraction from honest or malicious keys

Double-Authentication Preventing Signatures [PS14] (cont.)

Applications

- Deterring certificate subversion
- Double-spending prevention in offline payment channels
- Non-equivocation contracts

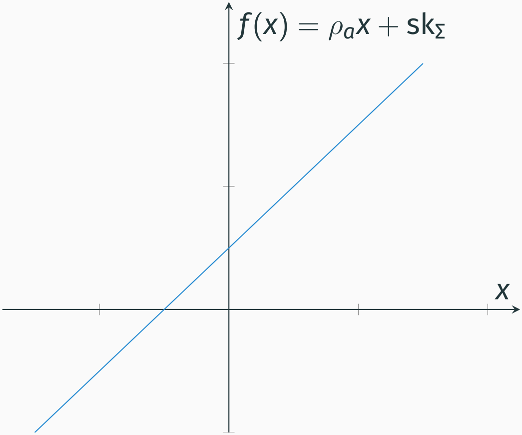
Existing DAPS

Approach	Address space	Extraction	Setting	Generic
[PS14]	exponential	**DSE**	factoring	×
[RKS15]	exponential	**DSE**	DLOG	×
[BPS17]	exponential	**DSE**	factoring	×
[BKN17]	exponential	**DSE**	SIS+LWE	×
[DRS18]	small	wDSE*	DLOG	✓
[Poe18]	small	**DSE**	DLOG	×

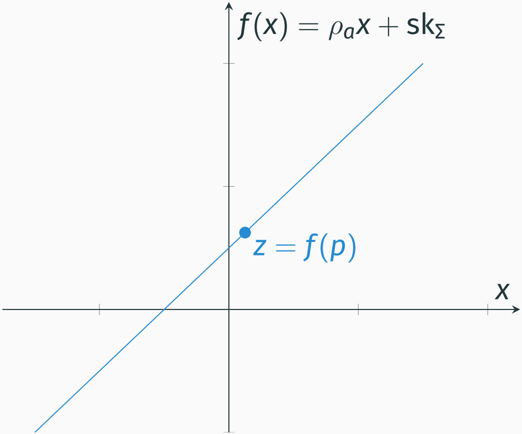
Can we build efficient DAPS without address space limitation from existing signature schemes in a black-box way?

DAPS without Structured Hardness Assumptions

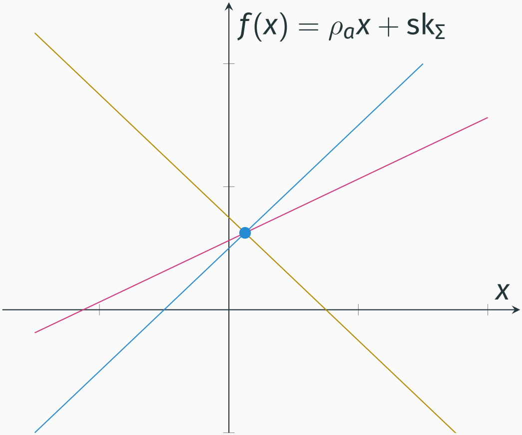
Shamir Secret Sharing



Shamir Secret Sharing

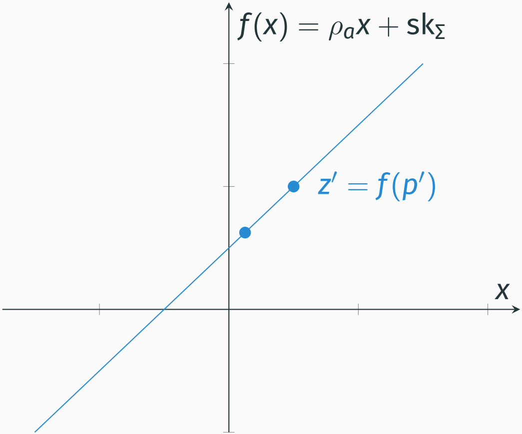


Shamir Secret Sharing



- One point reveals nothing about sk_Σ

Shamir Secret Sharing



- Two points allow to recover sk_Σ

The [DRS18] Approach

- DLOG-based signature scheme Σ

The [DRS18] Approach

- DLOG-based signature scheme Σ

+ Extend signature with secret share of private key
  Sharing polynomial is address dependent

» Extraction of Σ key

The [DRS18] Approach

- DLOG-based signature scheme Σ
- \+ Extend signature with secret share of private key
  Sharing polynomial is address dependent
- » Extraction of Σ key
- \+ Add consistency proof of share
- » Store encrypted coefficients in public key

The [DRS18] Approach

- DLOG-based signature scheme Σ
- + Extend signature with secret share of private key
  Sharing polynomial is address dependent
- » Extraction of Σ key
- + Add consistency proof of share
- » Store encrypted coefficients in public key
- » Polynomially sized address space

Resolving the Address Space Limitation

- Derive coefficients of sharing polynomial using PRF $\mathcal{F}$

Resolving the Address Space Limitation

- Derive coefficients of sharing polynomial using PRF $\mathcal{F}$
- “Commit” to the PRF secret key

» Fixed-value key-binding PRF [CMR98, Fis99]

Resolving the Address Space Limitation

- Derive coefficients of sharing polynomial using PRF $\mathcal{F}$
- “Commit” to the PRF secret key

» Fixed-value key-binding PRF [CMR98, Fis99]

- Signatures: secret share and consistency proof

» Signature-of-knowledge style signature

Resolving the Address Space Limitation

- Derive coefficients of sharing polynomial using PRF $\mathcal{F}$
- “Commit” to the PRF secret key

» Fixed-value key-binding PRF [CMR98, Fis99]

- Signatures: secret share and consistency proof

» Signature-of-knowledge style signature

+ Only requirement: Σ public key image of one-way function

Construction

sk_Σ

pk_Σ

Construction

sk_Σ $\mathsf{sk}_\mathcal{F}$

pk_Σ β c

Construction

sk_Σ $\mathsf{sk}_\mathcal{F}$

pk_Σ $\beta \longrightarrow c$

commit to $\mathsf{sk}_\mathcal{F}$

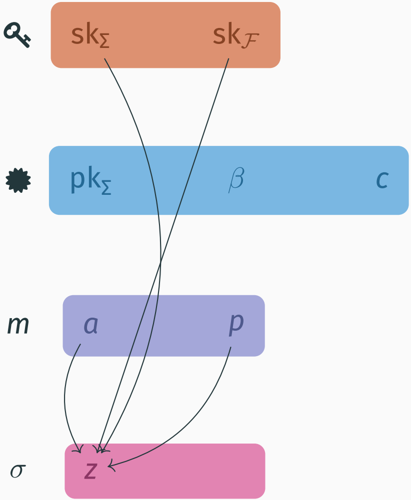
Construction

🔑 sk_Σ $\mathsf{sk}_\mathcal{F}$

✹ pk_Σ β c

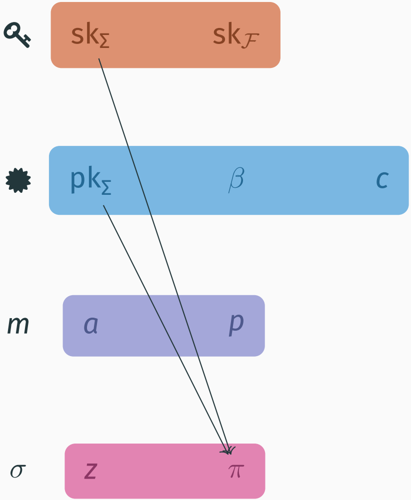
m a p

Construction



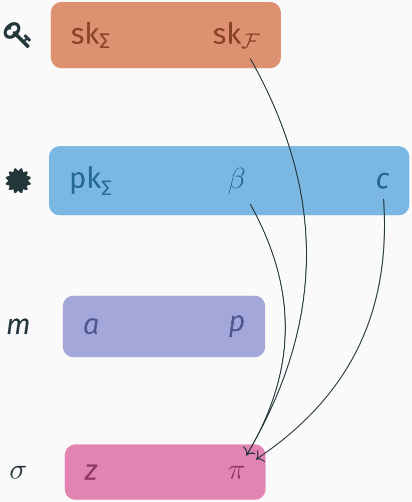
secret sharing of $\mathbf{sk}_\Sigma$

Construction



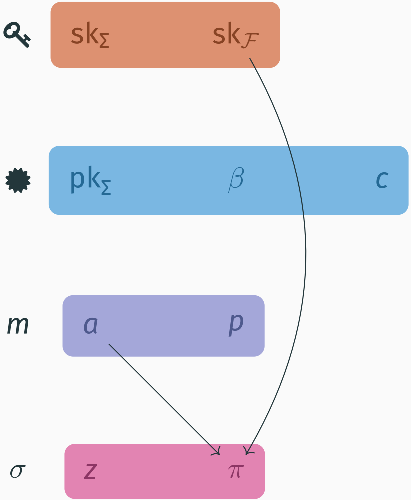
consistency proof of Σ keys

Construction



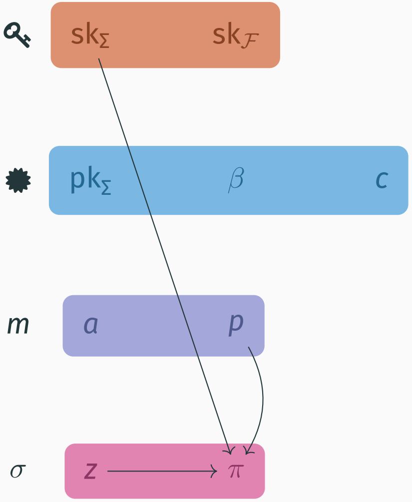
consistency proof of PRF commitment

Construction



consistency proof of sharing polynomial computation

Construction



consistency proof of secret sharing

Wrap Up

Generic approach:

- Σ with OWF relation between secret and public key
- **+** Verifiable Shamir secret sharing of Σ secret key
- **+** Sharing polynomial determined by address

$$f_a(x) = \mathcal{F}(\mathsf{sk}_{\mathcal{F}}, a) \cdot x + \mathsf{sk}_{\Sigma}$$

Wrap Up

Generic approach:

- Σ with OWF relation between secret and public key
+ Verifiable Shamir secret sharing of Σ secret key
+ Sharing polynomial determined by address

$$f_a(x) = \mathcal{F}(\mathsf{sk}_{\mathcal{F}}, a) \cdot x + \mathsf{sk}_{\Sigma}$$

- Zero-knowledge proof of consistency

Wrap Up (cont.)

Security (informal)

- Unforgeability from simulation-sound extractability, PRF and OWF properties
- Extraction from fixed-value-key-binding of PRF

Wrap Up (cont.)

Security (informal)

- Unforgeability from simulation-sound extractability, PRF and OWF properties
- Extraction from fixed-value-key-binding of PRF

Extension

+ Extendable to N-authentication preventing signatures

» Use degree $N - 1$ sharing polynomial

Instantiation

From Picnic:

- + OWF built from block cipher LowMC
- » Use LowMC also for PRF
- » Estimated signature size: 408 KB

Instantiation

From Picnic:

- + OWF built from block cipher LowMC
- » Use LowMC also for PRF
- » Estimated signature size: 408 KB

From SPHINCS:

- Secret-key-to-public-key relation more expensive
- Multiple evaluations of hash functions for consistency proof

Instantiation

From Picnic:

- + OWF built from block cipher LowMC
- » Use LowMC also for PRF
- » Estimated signature size: 408 KB

From SPHINCS:

- Secret-key-to-public-key relation more expensive
- Multiple evaluations of hash functions for consistency proof

From stuctured hardness assumptions:

- + Fulfill secret-key-to-public-key relation requirement
- ? Suitable proof system
- » Recent progress [AGM18]

Extending Any Signature Scheme

Black-box Extension

Signature scheme **Σ**

Sign(-Σ, ...) Verify(-Σ, ...)

Black-box Extension

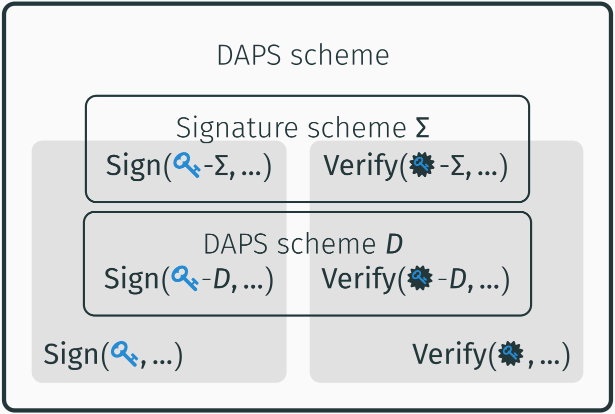
Signature scheme Σ

Sign(-Σ, ...) Verify(-Σ, ...)

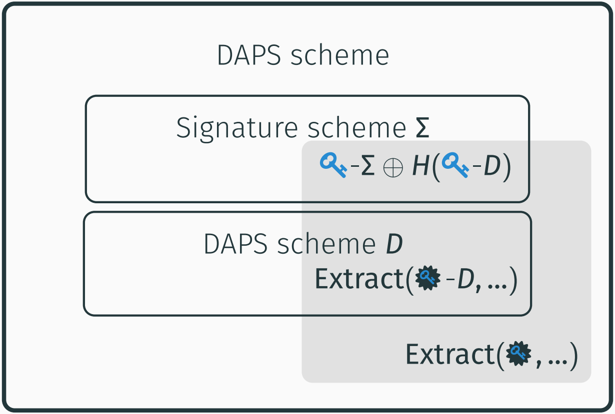
DAPS scheme D

Sign(-D, ...) Verify(-D, ...)

Black-box Extension



Black-box Extension



Black-box Extension (cont.)

- Extend any signature scheme to DAPS

+ From any other DAPS

» DAPS from standard signatures like EdDSA, ECDSA

Black-box Extension (cont.)

- Extend any signature scheme to DAPS

\+ From any other DAPS

» DAPS from standard signatures like EdDSA, ECDSA

Security (informal)

- Unforgeability from unforgeability of signature scheme
- Extraction from extraction of DAPS

Conclusion

DAPS Constructions

Approach	Address space	Extraction	Setting	Generic
[PS14]	exponential	DSE	factoring	$\times$
[RKS15]	exponential	DSE	DLOG	$\times$
[BPS17]	exponential	DSE	factoring	$\times$
[BKN17]	exponential	DSE	lattices	$\times$
[DRS18]	small	wDSE*	DLOG	✓
[Poe18]	small	DSE	DLOG	$\times$
Constr. 1	exponential	wDSE	symmetric	✓
Constr. 2	exponential	DSE	any	✓

Conclusion

Contribution

- ✔ Generic constructions of DAPS
- ✔ Construction 1: DAPS from symmetric-key primitives
- ✔ Construction 2: Extension of any signature scheme to DAPS

Questions?

Full version: `https://ia.cr/2018/790`

Supported by: prisma cloud

References i

[AGM18] Shashank Agrawal, Chaya Ganesh, and Payman Mohassel. **Non-interactive zero-knowledge proofs for composite statements.** In *CRYPTO (3)*, volume 10993 of *Lecture Notes in Computer Science*, pages 643–673. Springer, 2018.

[BKN17] Dan Boneh, Sam Kim, and Valeria Nikolaenko. **Lattice-based DAPS and generalizations: Self-enforcement in signature schemes.** In *ACNS*, volume 10355 of *Lecture Notes in Computer Science*, pages 457–477. Springer, 2017.

[BPS17] Mihir Bellare, Bertram Poettering, and Douglas Stebila. **Deterring certificate subversion: Efficient double-authentication-preventing signatures.** In *Public Key Cryptography (2)*, volume 10175 of *Lecture Notes in Computer Science*, pages 121–151. Springer, 2017.

[CMR98] Ran Canetti, Daniele Micciancio, and Omer Reingold. **Perfectly one-way probabilistic hash functions (preliminary version).** In *STOC*, pages 131–140. ACM, 1998.

[DRS18] David Derler, Sebastian Ramacher, and Daniel Slamanig. **Short double- and n-times-authentication-preventing signatures from ECDSA and more.** In *EuroS&P*, pages 273–287. IEEE, 2018.

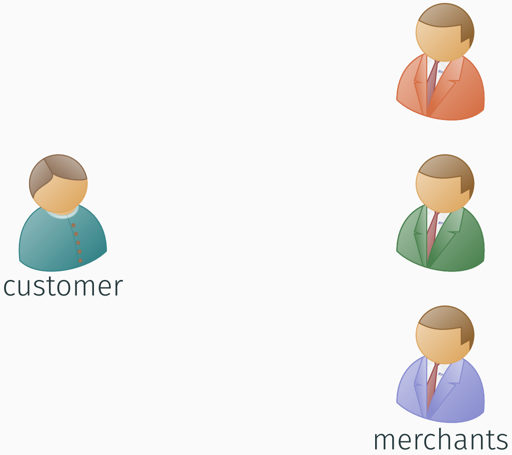
[Fis99] Marc Fischlin. **Pseudorandom function tribe ensembles based on one-way permutations: Improvements and applications.** In *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 432–445. Springer, 1999.

[Poe18] Bertram Poettering. **Shorter double-authentication preventing signatures for small address spaces.** In *AFRICACRYPT*, volume 10831 of *Lecture Notes in Computer Science*, pages 344–361. Springer, 2018.

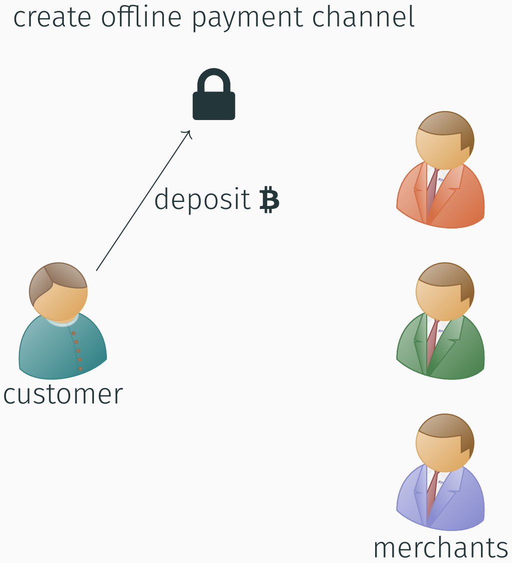
[PS14] Bertram Poettering and Douglas Stebila. **Double-authentication-preventing signatures.** In *ESORICS (1)*, volume 8712 of *Lecture Notes in Computer Science*, pages 436–453. Springer, 2014.

[RKS15] Tim Ruffing, Aniket Kate, and Dominique Schröder. **Liar, liar, coins on fire!: Penalizing equivocation by loss of bitcoins.** In *ACM Conference on Computer and Communications Security*, pages 219–230. ACM, 2015.

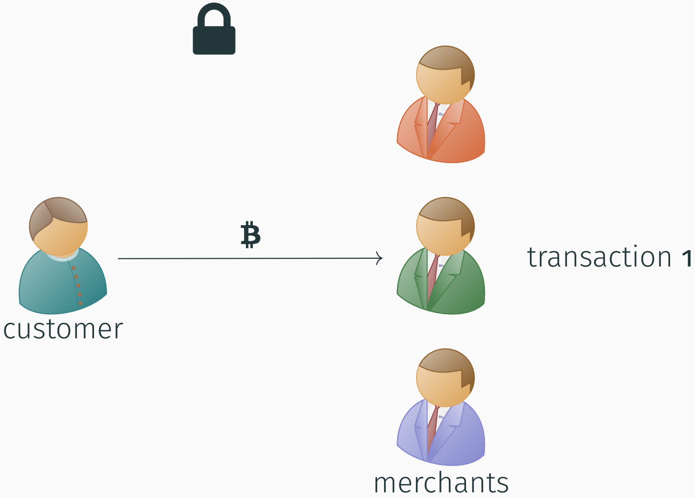
Penalize Double-Spending



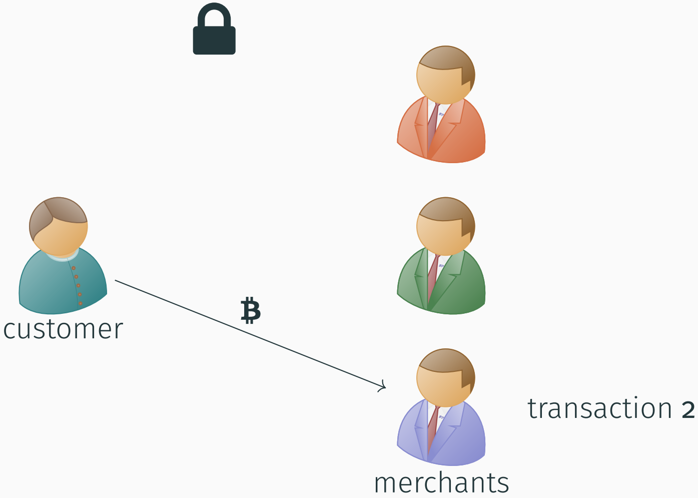
Penalize Double-Spending



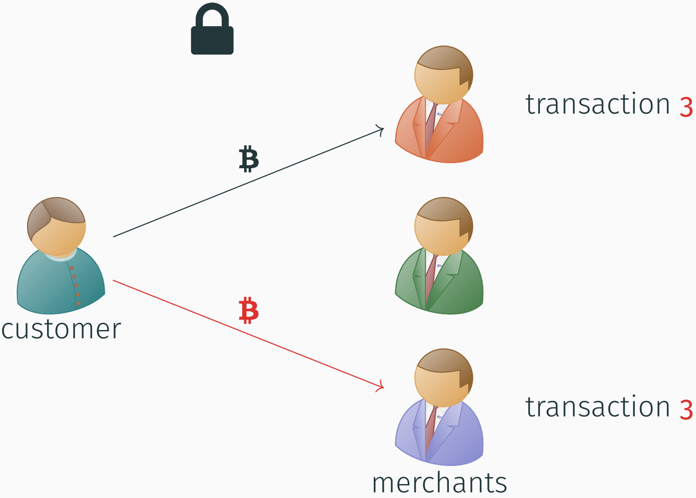
Penalize Double-Spending



Penalize Double-Spending



Penalize Double-Spending



Penalize Double-Spending