Selective End-To-End Data-Sharing in the Cloud

Felix Hörandner
Graz University of Technology
Graz, Austria

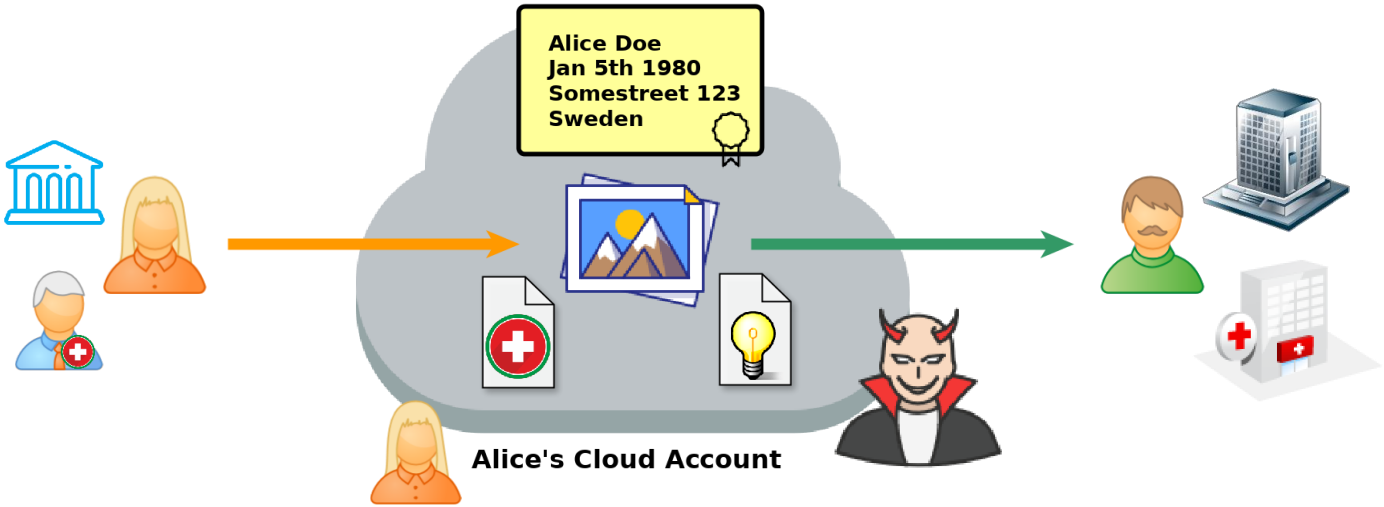
Sebastian Ramacher
Austrian Institute of Technology
Vienna, Austria

Simon Roth
Graz University of Technology
Graz, Austria

December 19, 2019

Data Sharing in the Cloud: Confidentiality

Cloud: Very convenient to share data (in plain)

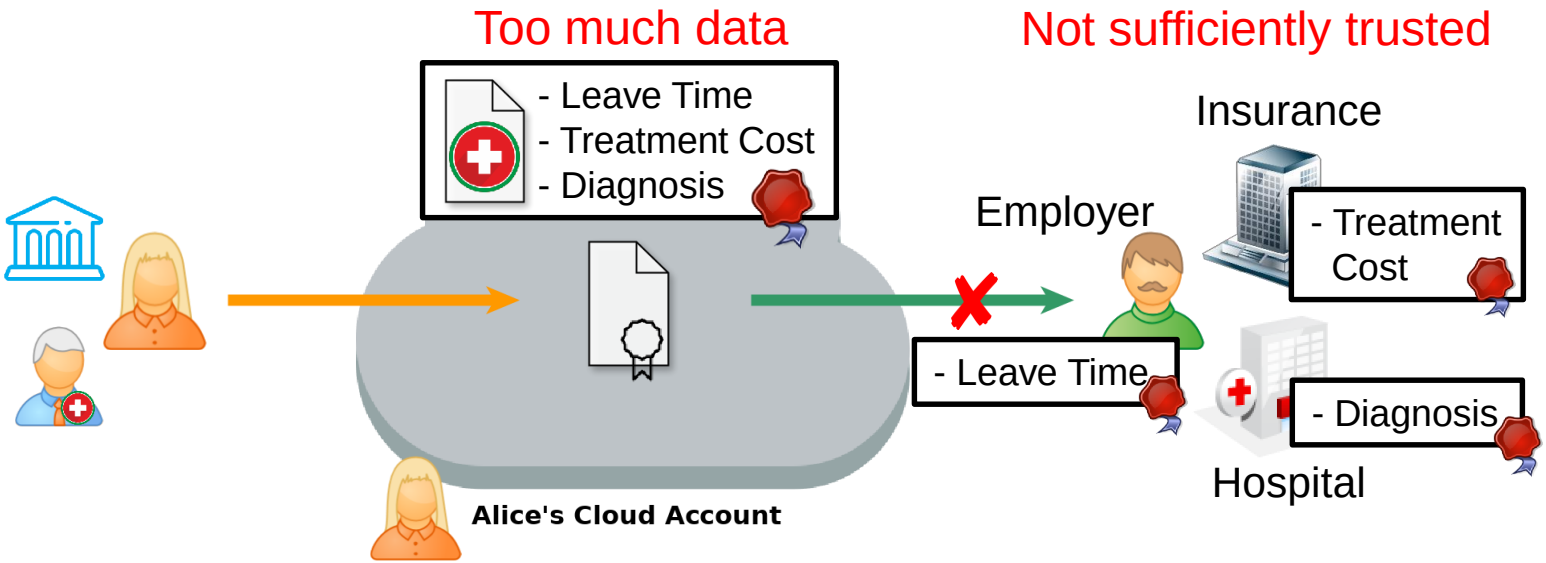


Cloud service

- Learns private data
- Trusted to not violate privacy?

➢ Need for end-to-end confidentiality

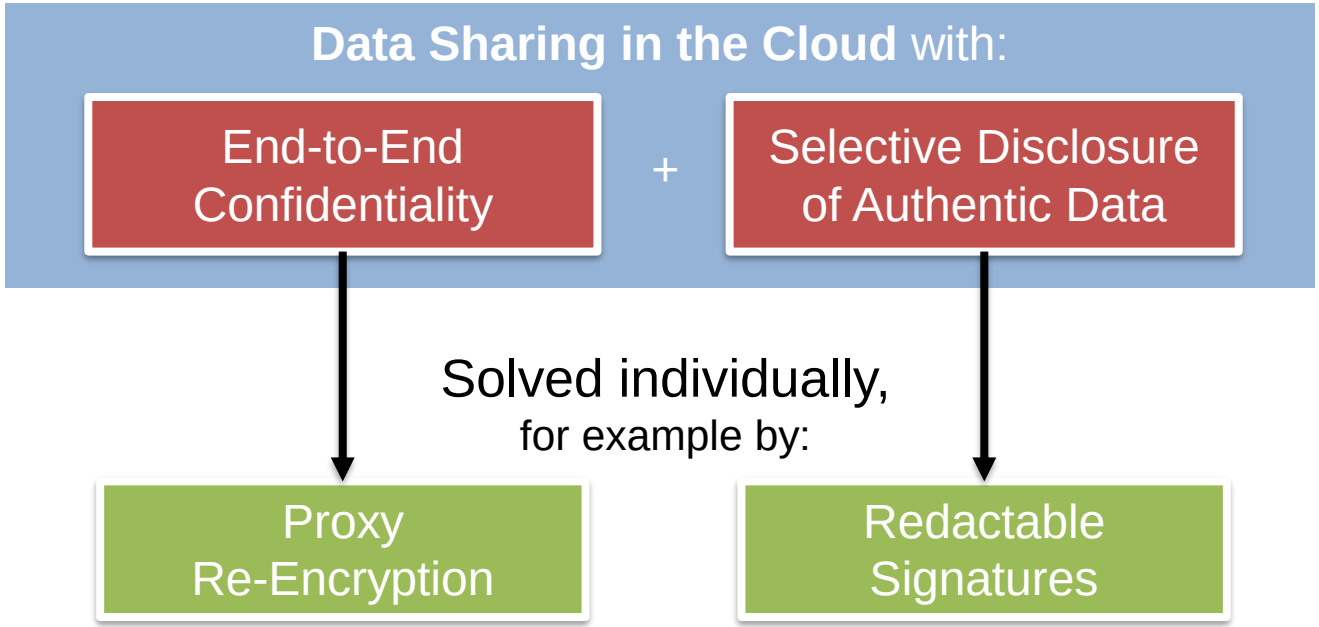
Data Sharing in the Cloud: Authenticity



- E.g. Digital signatures
- All or nothing

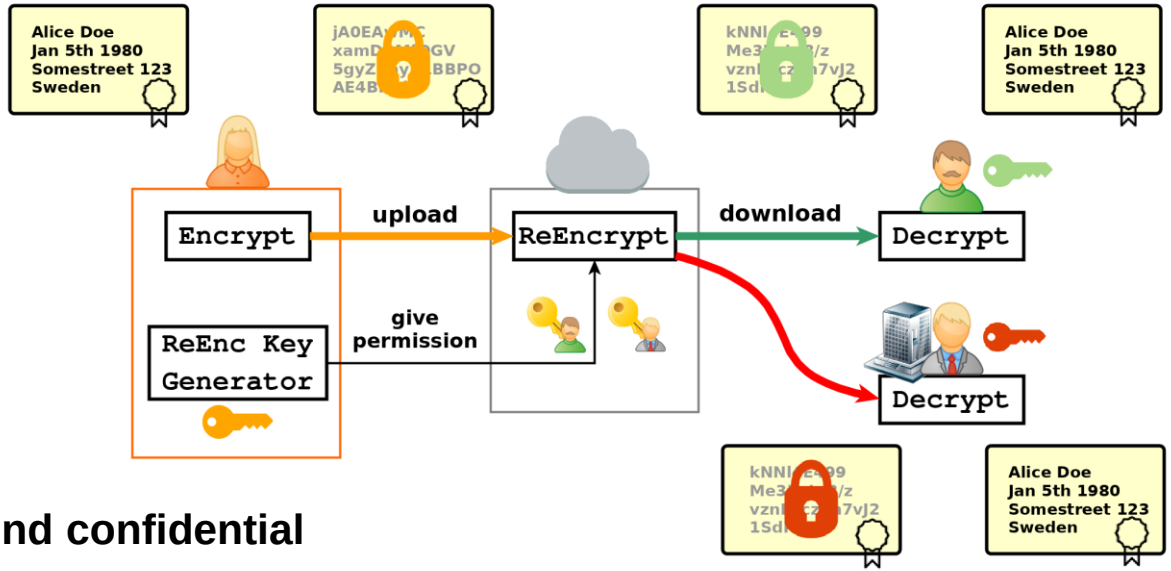
➢ Need for selective disclosure:
adapt data for each receiver

Ambition



➢ But **not trivial to combine**

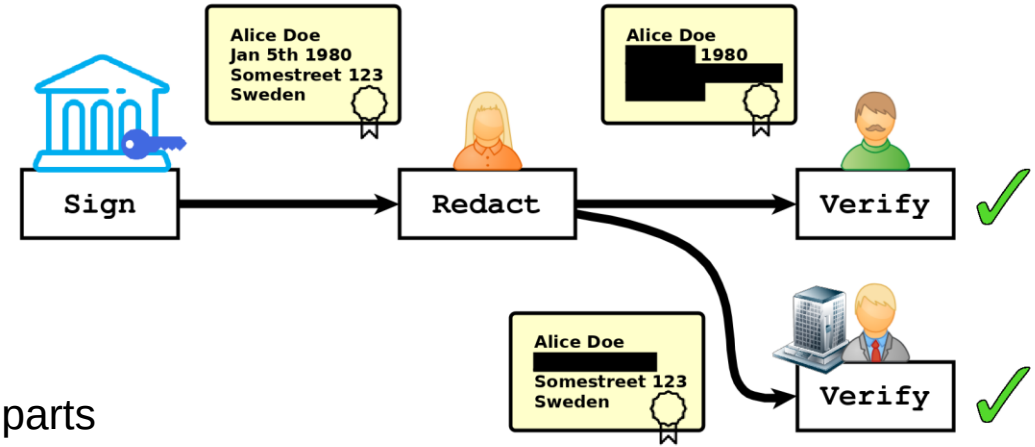
Background: Proxy Re-Encryption (PRE) [AFGH06]



- **End-to-end confidential**
- User: **no need to fully trust proxy**
- **User-centric:** Control through re-encryption key
- No duplicate data

[AFGH06] Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger:
Improved proxy re-encryption schemes with applications to secure distributed storage.
ACM Trans. Inf. Syst. Secur. 2006

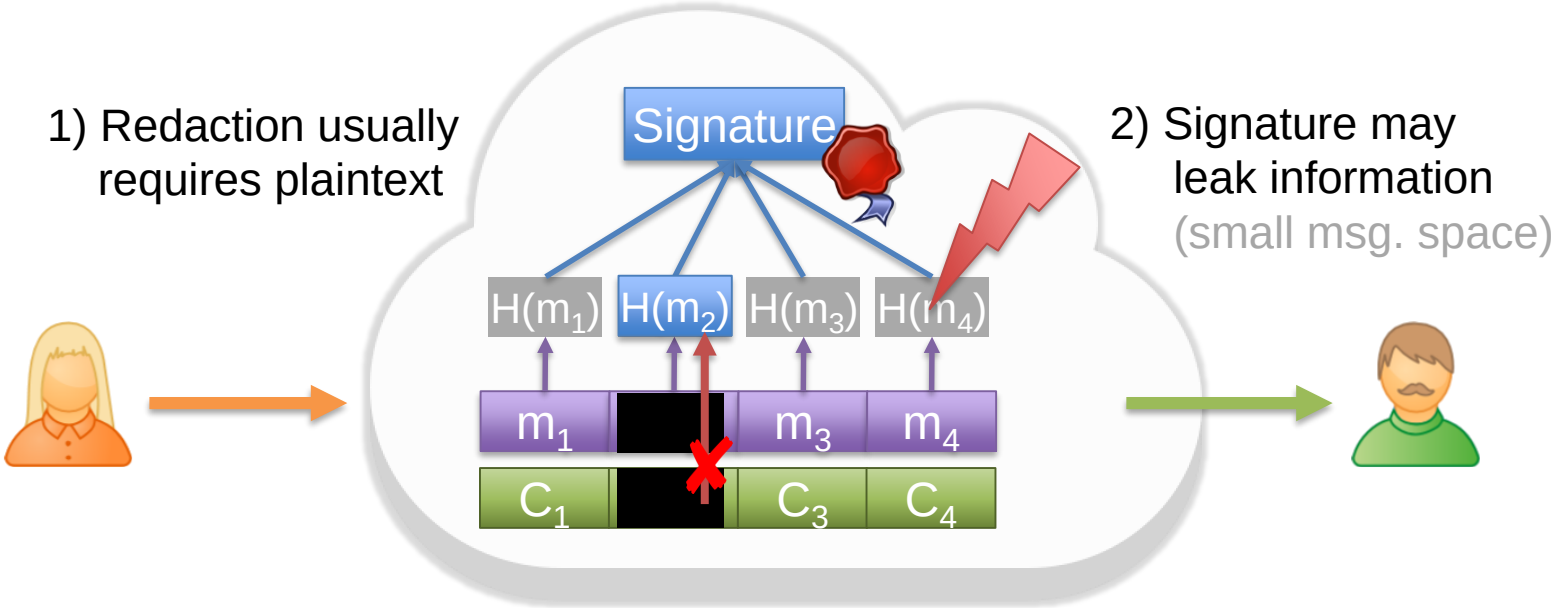
Background: Redactable Signatures (RS) [JMSW02]



- Black-out parts
- Signature stays valid for rest
- ➢ Selective disclosure

[JMSW02] Robert Johnson, David Molnar, Dawn Xiaodong Song, David A. Wagner: Homomorphic Signature Schemes. CT-RSA 2002

Combining: Naive Challenges



- **ReEncrypt and Redact conflict**
- **Privacy hard to get right**

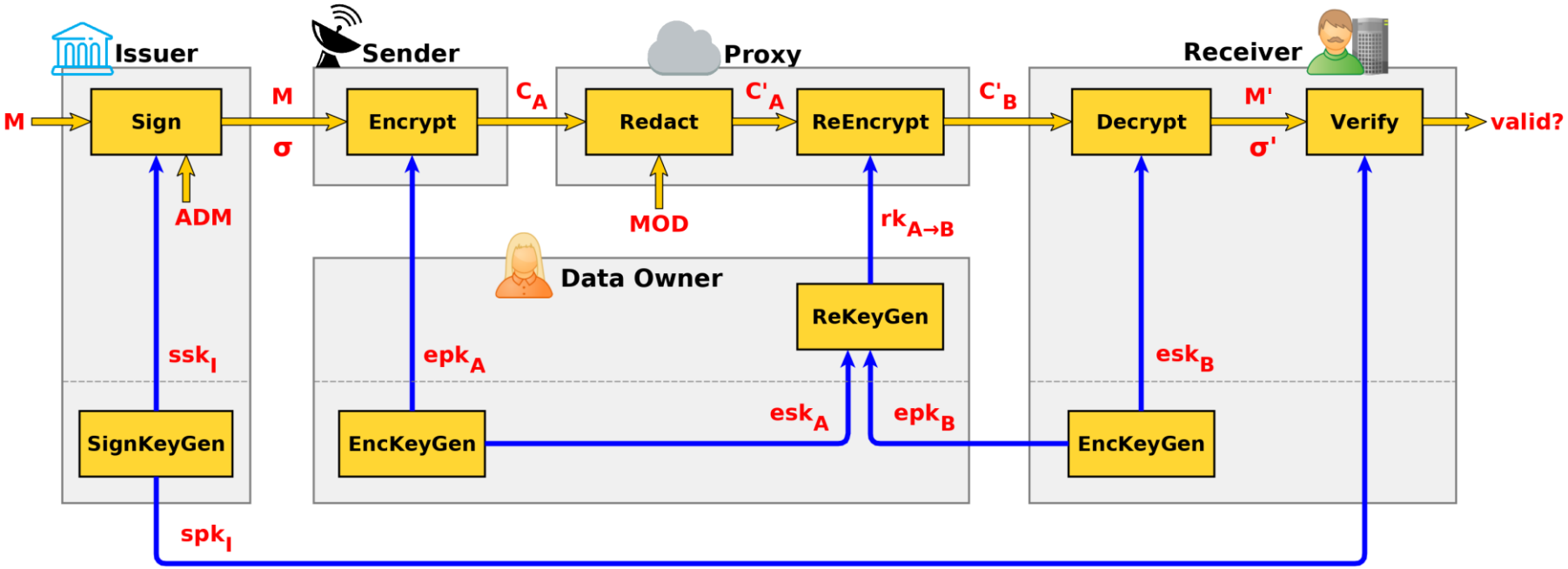
Our Contribution

Selective End-To-End Data Sharing (in the Cloud)

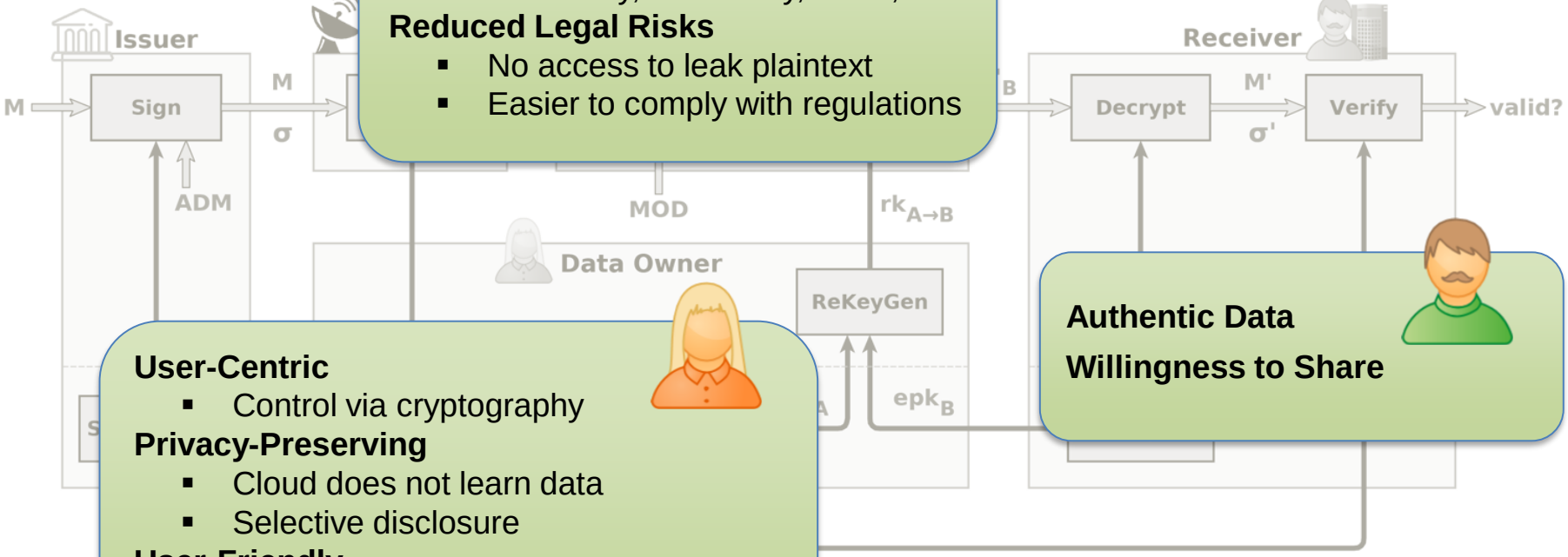
End-to-End Confidentiality + Selective Disclosure of Authentic Data

Model + Security Notions → Modular Instantiation → Three Implementations → Performance Evaluation

Model


Issuer
Sender
Proxy
Receiver
M
Sign
M
σ
Encrypt
C_A
Redact
C'_A
ReEncrypt
C'_B
Decrypt
M'
σ'
Verify
valid?
ADM
MOD
rk_A→B
Data Owner
ReKeyGen
ssk_I
epk_A
esk_B
esk_A
epk_B
SignKeyGen
EncKeyGen
EncKeyGen
spk_I

Benefits



Cloud-Benefits
- Scalability, availability, costs, ...

Reduced Legal Risks
- No access to leak plaintext
- Easier to comply with regulations

User-Centric
- Control via cryptography

Privacy-Preserving
- Cloud does not learn data
- Selective disclosure

User-Friendly
- Cloud: available, less maintenance, ...
- Single place to manage data/access

Authentic Data

Willingness to Share

Security Notions

- **Challenge**: Different/more data flows through system
  - E.g.: distinguish based on signature added to ciphertext
  - ➢ Adapt and combine notions from PRE and RSS

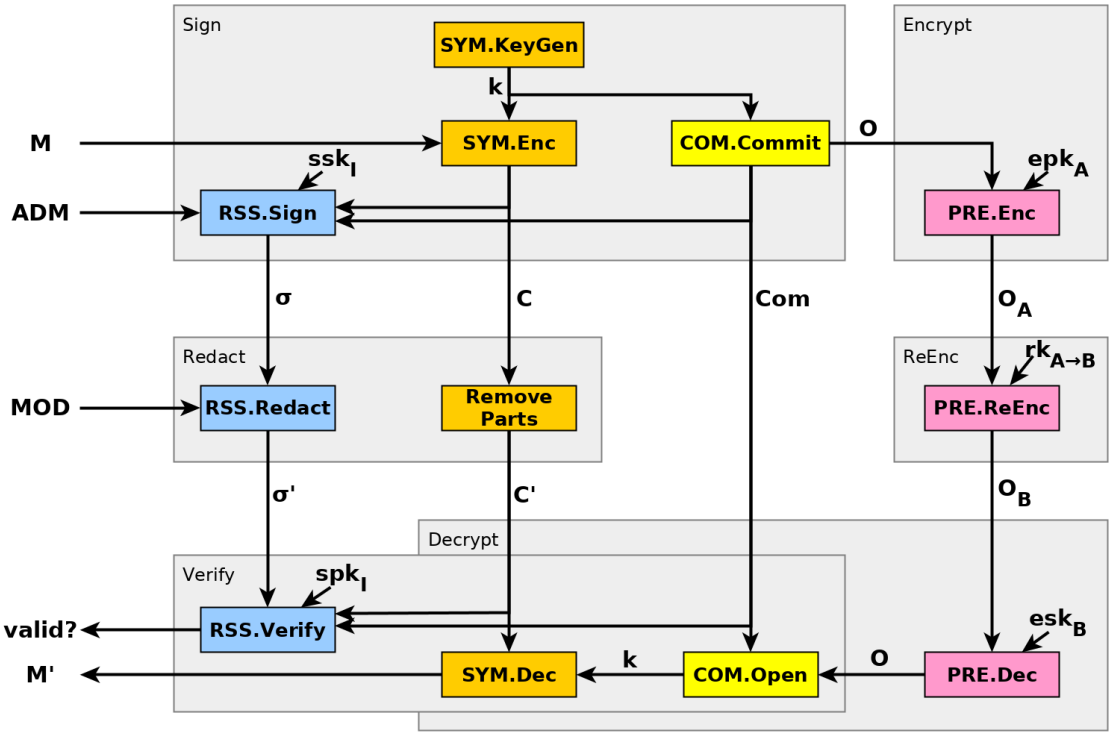
- **Unforgeability**
  Infeasible to create valid signature for given message without signing key

- **Receiver-Privacy**
  Receivers should not learn information on parts that were redacted

- **Proxy-Privacy**
  Proxy should not learn anything about plain data

- **Transparency**
  Infeasible to decide if parts of message were redacted

Modular Instantiation



- Sym. encrypt then sign
- Redact on sym. ciphertexts
- Commit to sym. key
- Share sym. key via PRE

- **Enables tailoring**: Choose underlying crypto according to app. needs

➢ **Proven secure**

Security Assumptions

- **Unforgeability**
  Infeasible to create valid signature for given message without signing key

  If: **COM** binding
  RSS unforgeable

- **Receiver-Privacy**
  Receivers should not learn information on parts that were redacted

  If: **RSS** private

- **Proxy-Privacy**
  Proxy should not learn anything about plain data

  If: **RSS** unforgeable
  PRE IND-RCCA secure
  COM hiding
  SYM IND-CPA secure

- **Transparency**
  Infeasible to decide if parts of message were redacted

  If: **RSS** transparent

➢ Only relies on std. notions of underlying schemes

Three Implementations

Common	PRE	Chow et al. [CWYD10]	3072bit
	SYM	AES	128bit
	COM	Hash Commitment (SHA3)	256bit
	Hash	SHA3	256bit
Impl. 1: Sets, CL	RSS	Derler et al. [DPSS15, Scheme 1]	
	Accu.	CL [CL02] (RSA)	3072bit
	DSS	RSA	3072bit
Impl. 2: Sets, DHS	RSS	Derler et al. [DPSS15, Scheme 1]	
	Accu.	DHS [DHS15] (ECC)	384bit
	DSS	ECDSA	256bit
Impl. 3: Lists, CL	RSS	Derler et al. [DPSS15, Scheme 2]	
	Accu.	CL [CL02] (RSA)	3072bit
	DSS	RSA	3072bit

128bit security

Different data structures
- Sets
- Lists

Different accumulators
- CL (RSA)
- DHS (ECC)

[CWYD10] Sherman S. M. Chow, Jian Weng, Yanjiang Yang, and Robert H. Deng. AFRICACRYPT 2010

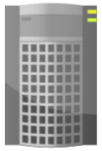
[DPSS15] David Derler, Henrich C. Pöhls, Kai Samelin, and Daniel Slamanig. ICISC 2015

[CL02] Jan Camenisch, Anna Lysyanskaya. CRYPTO 2002

[DHS15] David Derler, Christian Hanser, and Daniel Slamanig. CT-RSA 2015

Performance Evaluation

- **Platforms**



PC: Intel i7-4790 3.6 GHz (2014)

Mobile phone: Pixel 2 (2017)

- **Methodology**
  - Different number of parts & size per part
  - Redact half of parts before re-encrypting
  - For each of three implementations

- **Examples**:

Impl 1.: for sets with CL accumulator

		Sign	Enc	Redact	ReEnc	Dec	Verify
5 pages, each 200kB	PC	23	1	6	1	3	16
	Phone	177	12	73	6	28	106
50 x-rays, each 10MB	PC	1871	1	393	1	749	1100

(in milliseconds)

➢ Practical efficiency

Summary: Key Messages

- **Selective End-to-End Data-Sharing**
  - End-to-end confidentiality and
  - Selective disclosure of authentic data
  - ➢ New model and security notions
- **Modular Instantiation**
  - Combines proxy re-encryption and redactable signatures
  - ➢ Proven secure
- **Performance Evaluation** of three implementations
  - ➢ Practical efficiency

Thank you! Any Questions?