Applied Attribute-based Encryption Schemes

Sebastian Zickau, Dirk Thatmann, Artjom Butyrtschik,
Iwailo Denisow, and Axel Küpper

Technische Universität Berlin

TELEKOM INNOVATION LABORATORIES

Sebastian Zickau

Service-centric NETWORKING

Motivation

- IoT gaining rapid popularity
- Security must be essential part of initial process
- Cloud Computing Security
- IoT Security
- Public / Subscribe (pub/sub)
- Message Oriented Middleware (MOM)
- Message Queue Telemetry Transport (MQTT)
- Previous work (Thatmann et al.)

Functional Encryption

- Cryptographic Schemes
- Symmetric Key
- Asymmetric Keys
- Homomorphic Encryption
- Functional Encryption (FE)
- Subset of FE is asymmetric Attribute-based Encryption (ABE)
- Cloud Computing and IoT

Attribute-based Encryption

- Sahai and Waters published in 2006
- Implementation by John Bethencourt
- Key authority
  - Generates public keys
  - Holds secret master key
  - Can generate private keys
- Secret master key
  - Used to generate keys
- Private key
  - Encrypt data with a given policy
- Public key
  - Decrypt data when attributes correspond

ABE Basics

- Attribute-based fine-grained access policy
- Boolean formula
- Ciphertext-Policy (CP) and Key-Policy (KP) ABE
- Ciphertext-Policy-ABE (CP-ABE)
  - Mostly used
- Keypolicy-ABE (KP-ABE)
  - DRM use cases
- *((student and enrollment < 2012) or professor)*

ABE Basics

- Attribute types: strings, numericals
- Dynamic attributes: time, date, location
- Operators: *and*, *or*, *of*, <, >, =
- Example policy 1:
  - *((student and enrollment < 2012) or professor)*
- Example policy 2:
  - (hiringdate <= 2012 and employee) or

  (birthyear=1990 and accesslevel > 5) or boss
- An important characteristic of ABE is the prevention of collusion attacks. As an example, a file is encrypted with the policy *(X and Y)* and sent to two users.

ABE Functions

- **Setup** - Generates a *public key* and an associated *secret master key*.
- **Encrypt** - Encrypts a file with a *public key* and an annotated *policy*.
- **Keygen** - Creates a *private key* with *attributes*. To do this, a *secret master key* is needed. This *private key* is associated with the *secret master key* and its *public key*.
- **Decrypt** - Needs a *ciphertext* and a *private key*. Decrypts the *ciphertext* only if the *attributes* in the *private key* satisfy the *policy* and the *private key* is associated with the *public key* that has been used initially for encryption.

Use Cases

Within the IOT world, there are certain characteristics that can be seen as fundamental:

- Involving a large amount of sensors and devices, which are attached to the Internet
- There exist one-to-many
- Many-to-many communications
- Human-to-machine
- Machine-to-machine

Related Work

- Singh et al. provide an approach combining MQTT and ABE. They introduce an ABE-secured MQTT and MQTT for sensor networks protocol
- There are use cases within the healthcare data domain that are based on ABE ciphertext-policies to protect electronic health records (EHR), Wang et al., Alshehri et al. and Akinyele et al.
- In the related work from Picazo-Sanchez et al. ABE is utilized to access medical sensor and devices data and to change the settings of sensors

Related Work

- In Yang et al. an overall encryption via ABE for private data in a pub/sub environment is discussed. The work introduces an ABE variant called bi-policy attribute-based encryption (BP-ABE)
- Cachet is a ’Decentralized Architecture for Privacy Preserving Social Networking with Caching’. Cachet aims to enable confidentiality, integrity and availability of user content, as well as the privacy of user relationships in online social networks (OSN)

Related Work

- In EASiER, an access control architecture for OSNs is described. Based on Bethencourt's CP-ABE implementation, Jahid et al. provides a revocation scheme by introducing a minimally trusted proxy and an integration of group communication schemes with ABE
- Thatmann et al. introduced the notion of ciphertext expiration, which supports temporal storage of cryptographic keys in a DHT in a secure manner

Implementations

A. *Cpabe*
B. *libfenc*
C. *Charm*
D. *cpabe (Java)*
E. *JCPABE*
F. *jTR-ABE*
G. *KPABE*
H. *DCPABE*
I. *DET-ABE*
J. *PIRATTE*
K. *arcanum*
L. *LSSS2*
M. *NEON*
N. *AndrABEn*

C/C++ Implementations

- Cpabe
  - First Implementation 2007 by J. Bethencourt
  - Pairing-based Cryptography
  - Only CP-ABE
  - And, or, of operators + numerical attributes
  - AES-128 in Cipher Block Chaining
- Libfenc
  - 2010
  - CP-ABE and KP-ABE
  - iOS
- KPABE, PIRATTE, LSSS2, NEON ABE

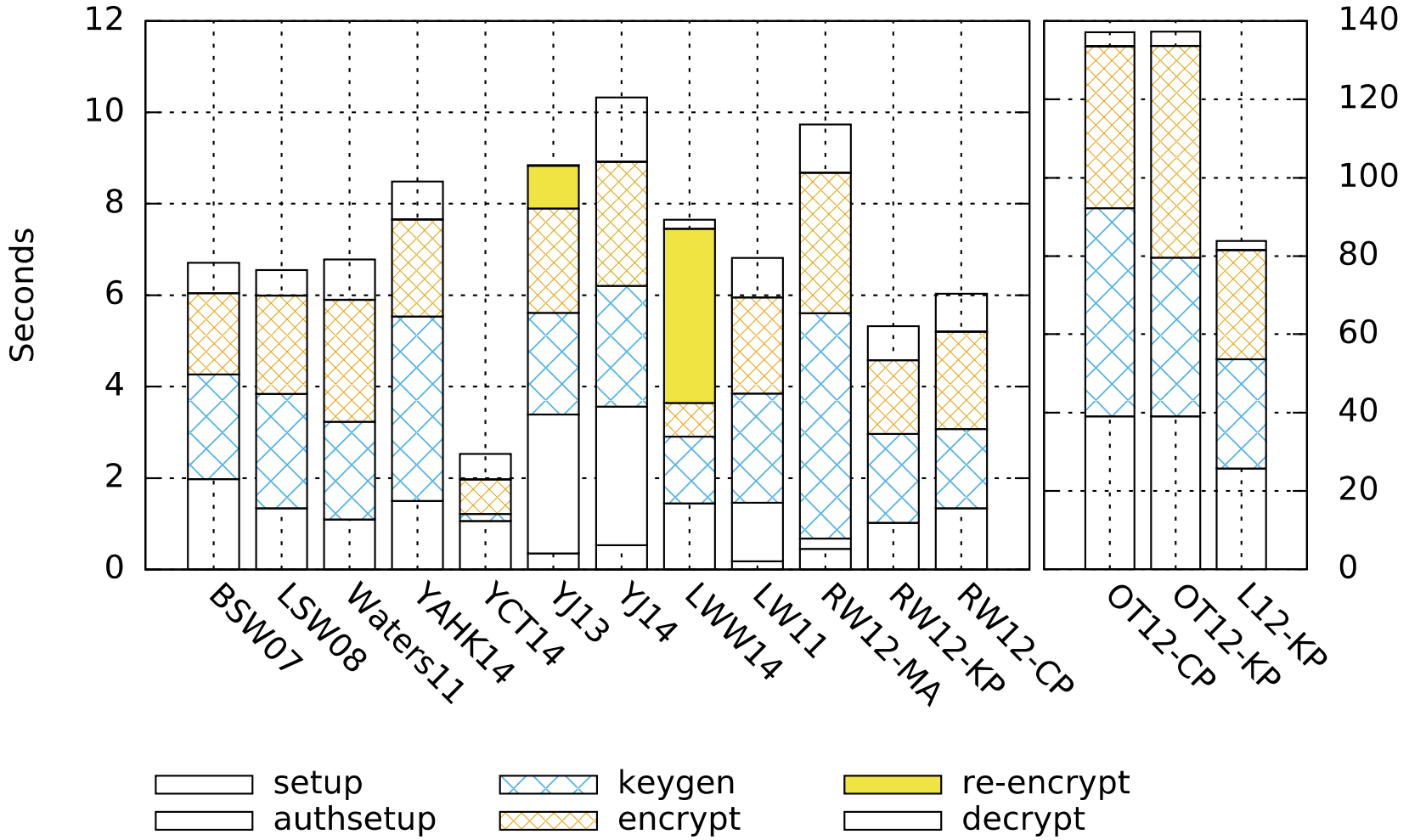
Java Implementations

- Cpabe (Java)
  - 2013
  - Adaptation of J. Bethencourt's cpabe
  - Policies in polish notation
  - Android support
- JCPABE (SNET)
  - Policy parser (JavaCC and JJTree)
  - Numerical attributes
  - Platform independency
  - Added feature: dynamic location information
- jTR-ABE (SNET)
  - Threshold gates
  - Public blackbox taritor tracing
- DCABE, DET-ABE, Arcanum, AndrABEn

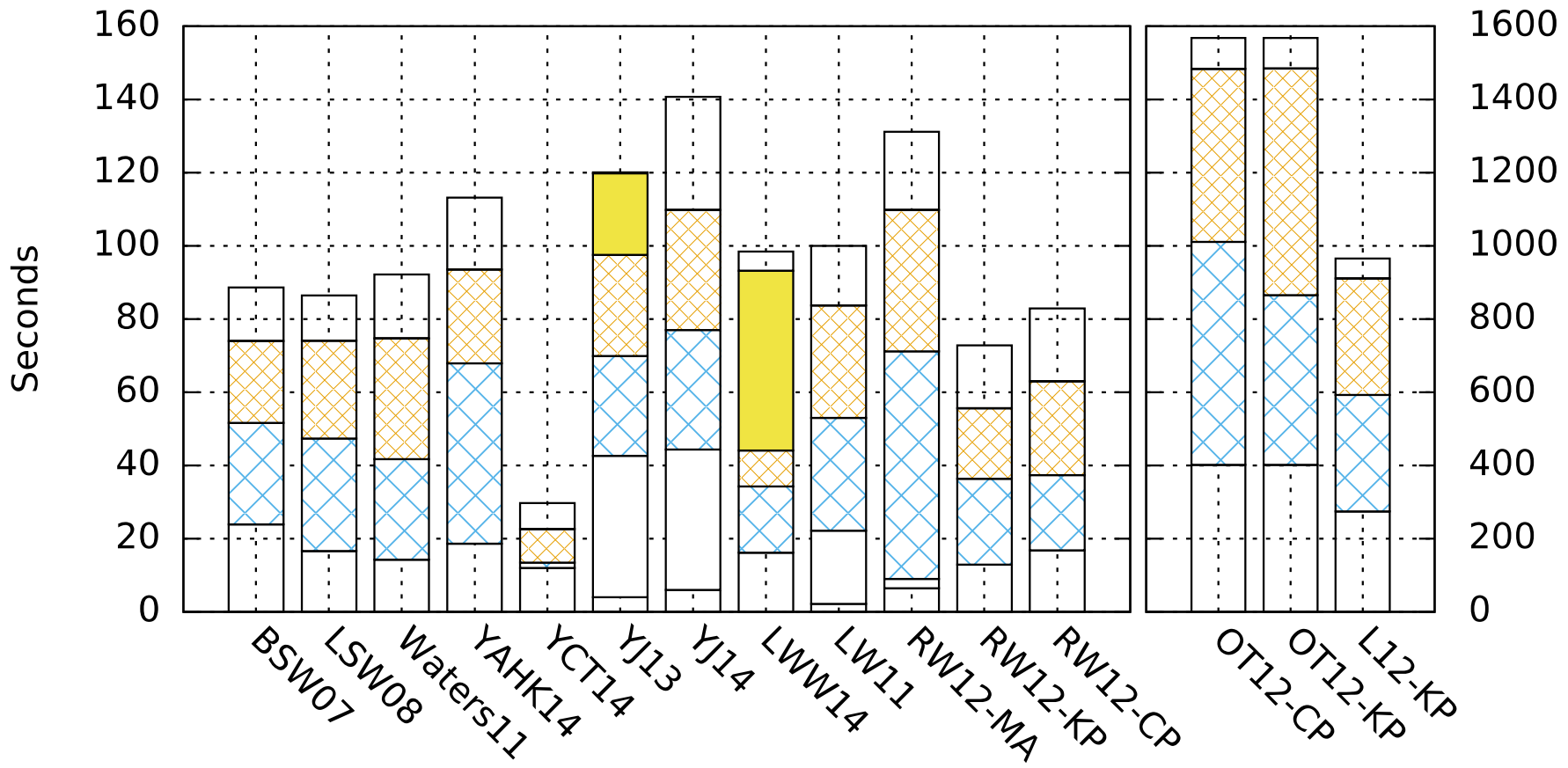
Python Implementation

- Charm (+ SNET schemes)
  - Since 2011
  - Various ABE schemes
  - Based on elliptic curve cryptography
  - Android support
  - Key encapsulation
  - ABE schemes
  - Multi-authority schemes
  - Proxy re-encryption schemes
  - User attribute revocation
  - No central authority

Core-i7 Benchmark



Raspberry2 Benchmark



Overview

Section	Library Name / Implementation	Implementation Author(s)	Scheme(s)	Language	Based on Library	License	Updated
V-A	cpabe [21]	John Bethencourt	BSW07 [5]	C	PBC	GPLv2	03/2011
V-B	libfenc [22]	Matthew Green, Joseph Ayo Akinyele	LSW08 [23], Waters11 [24], GPSW07 [4]	C++	PBC	GPLv2	02/2011
V-C	Charm [25]	Joseph Ayo Akinyele	BSW07 [5], LSW08 [23], Waters11 [24]	Python	PBC, MIRACL or RELIC	LGPLv3	07/2013
		Gary Belvin	LW11 [26]			LGPLv3	11/2013
		Artjom Butyrtschik	LWW14 [27], YCT14 [28], YJ13 [29], YJ14b [30]			LGPLv3	07/2015
		Alexander Förster	YAHK14 [31]			LGPLv3	07/2015
		Yannis Rouselakis	RW15 [32], LW12 ([33]) (KP), OT12 [34] (KP+CP), RW12 [35] (KP+CP)			Unlicensed	11/2012
V-D	cpabe (Java) [36]	Junwei Wang	BSW07 [5]	Java	JPBC	GPLv2	03/2015
V-E	JCPABE [37]	Iwailo Denisow	BSW07 [5]	Java	JPBC	GPLv2	06/2015
V-F	jTR-ABE [38]	Artjom Butyrtschik	LW14 [39]	Java	JPBC	GPLv2	09/2015
V-G	KPABE [40]	Yao Zheng	GPSW07 [4]	C	PBC	GPLv2	11/2014
V-H	DCPABE [41]	Stefano Braghin	LW11 [26]	Java	JPBC	Unlicensed	11/2012
V-I	DET-ABE [42]	Miguel Morales-Sandoval	BSW07 [5]	Java	JPBC	Public Domain	06/2015
V-J	PIRATTE [43]	Sonia Jahid	JB12 [6]	C	PBC	GPLv2	04/2013
V-K	arcanum [44]	Angelo De Caro	GVW13 [45], GGHVV13 [46], GGHSW13 [47], BNS13 [48]	Java	arcanum-pbc	LGPL v3	04/2015
V-L	LSSS2 [49]	Eric Zavattoni et al.	Waters11 [24]	C++	ate-pairing	3-clause BSD	10/2013
V-M	NEON ABE [50]	Ana Helena Sánchez	Waters11 [24]	C++	-	Public domain	02/2013
V-N	AndrABEn [51]	Moreno Ambrosin, Mauro Conti, Tooska Dargahi	BSW07 [5], GPSW07 [4]	Java	PBC	GPLv2	10/2014

Thank you!

#ICIN2016

Technische Universität Berlin

TELEKOM INNOVATION LABORATORIES

Service-centric NETWORKING

Contact Information

sebastian.zickau@tu-berlin.de

curcuma
Cloud Computing Location Metadata

http://curcuma-project.net/

http://entrance.snet.tu-berlin.de/

Service-centric NETWORKING

http://www.snet.tu-berlin.de/

https://github.com/TU-Berlin-SNET/