Non-monotonic practical Attribute-based Encryption

(Version 0.1, Oct 16th, 2016)

Dirk Thatmann*
Service-centric Networking, Technische Universität Berlin and Telekom Innovation Laboratories
Email: *d.thatmann@tu-berlin.de

***Abstract*—We introduce an extended version of Liu et al.'s "Practical Attribute-Based Encryption: Traitor Tracing, Revocation and Large Universe" cryptography scheme. Our extension adds the non-monotonic property for access structures to the scheme which is not supported by the original one. We implemented the scheme and our extension presented here. In addition, we describe further software components that were developed within the research project Entrance to enable an Attribute-Based Encryption secured data exchange between our system participates.**

I. Introduction

Data encryption is used today in many areas. Encryption technologies contribute, among other things, to achieving compliance with legal regulations or to preventing a fundamental misuse of data. This is particularly critical in an age in which data is seen as new gold and large industries intend to maximize profits. Practice shows that good encryption is not so easy to establish because usability is often difficult. Also new advanced cryptographic methods are not used by the market for various reasons. One reason is simply the lack of knowledge about the existence of these methods.

Many Attribute-Based Encryption (ABE) schemes exist. Most are based on bilinear mapping so on pairing-based cryptography, a few on lattice cryptography. A number of functionalities can be compiled, which should support an ideal and mature scheme. This includes support for a Large Attribute Universe, multi Attribute Authorities, attribute or user revocation and non-monotone access structures. A few schemes also offer functions such as rights delegation, malicious user/key tracing and more. There are also schemes dedicated to broadcast encryption or predicate encryption. The latter increases privacy, since attackers cannot learn from the readable access structure.

A. Contribution

In this work we describe the extension of an existing CP-ABE scheme [1] to support the property of non-monotonic access structures. Compared to monotonic access structures, non-monotonic access structures allow a more natural formulation on the one hand, and a reduction of their size on the other, which can have an effect on the computing time for encryption and decryption. An overview of all schemes and achievements, on which our selected scheme is based, shows Figure 1. We basically inherit all functions from Liu et al.'s CP-ABE scheme and extent it with the non-monotonic property. A brief introduction to the Entrance system is given beforehand.

B. Entrance goals

The Entrance Project wants to promote and evaluate the use of attribute-based encryption. Various existing ABE schemes were implemented [2]. In addition, software was developed which enables an easier use of ABE encryption [3]. Usability considerations have been carried out and e. g. published here [4].

C. remainder

The remainder of this paper is structured as follows. We describe the Entrance ecosystem in Section II. We describe the non-monotonic extension in Section III. First, we recapture Liu et al.'s PABE scheme and provide additional computations in order to achieve support for monotonic access structures. Afterwards we conclude in Section IV.

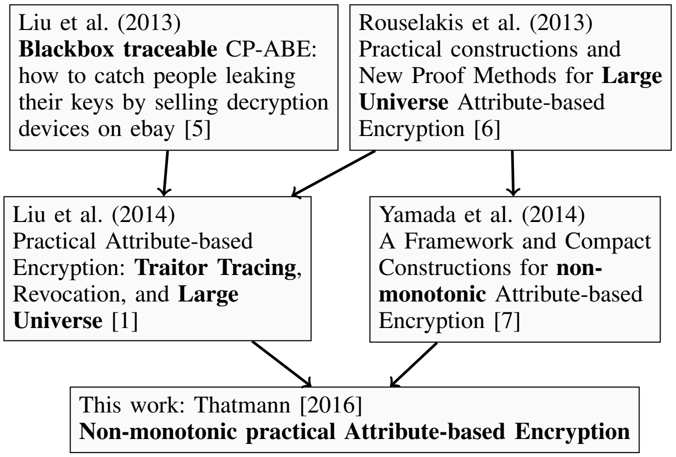

Liu et al. (2013)
Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay [5]
Rouselakis et al. (2013)
Practical constructions and New Proof Methods for **Large Universe** Attribute-based Encryption [6]
Liu et al. (2014)
Practical Attribute-based Encryption: **Traitor Tracing**, Revocation, and **Large Universe** [1]
Yamada et al. (2014)
A Framework and Compact Constructions for **non-monotonic** Attribute-based Encryption [7]
This work: Thatmann [2016]
Non-monotonic practical Attribute-based Encryption

Fig. 1. Scheme evolution - building on top of existing ABE schemes and constructions

II. The Entrance Ecosystem

Entrance is a research project which was first introduced by Thatmann et al. in [3]. It aims to enable a secure data exchange between participants of this system. The data owner should be able to share data with others in a self-determined way and keep control over his data. Since this requirement is very demanding, we reduce it to the use of modern encryption methods and the provision of functionalities such as rights revocation and traitor tracing. The crytographic sovereignty should always lie with the data owner. In the Entrance project, services and clients were implemented that enable the use of Attribute-based Encryption (ABE) for data exchange. The services implement Liu et al.'s Ciphertext-policy Attribute-based Encryption (CP-ABE) scheme [1] and further basic functions for key management, which enables the generation of private user keys and the assignment of user attributes to them. Besides the basic revocation mechanism provided in [1] the first generation of two new revocation mechanisms, namely "ciphertext expiration" and "attribute expiration" were developed and introduced in [3]. These expiration types led, among other things, to the integration with a Distributed Hash Table (DHT), whereby Kademilia [8] was integrated as an example.

During the project runtime, software clients were developed alongside the backend system, which enables data management, user and attribute management and encryption. The first Software Client was realized as Windows 10 App (c#). Further clients should be able to be operated via a web browser. Many browsers support W3C's Encrypted Media Extension (EME), which allows secure decryption of video in the browser (Netflix client). Unfortunately, the EME is very much focused on video streams, making it difficult to push other data through the browser and API. This led to other plugin solutions for web browsers being investigated. The first web browser client was a Google portable Native Client (pNaCl), which was later converted into a WebAssembly solution. A dashboard (Bootstrap.io and Python Flask) allows a graphical use of the Entrance System by the data owner. The application case "sport checkup" is implemented as an example. The aim here is to enable a long-distance runner to confidently share sensor data with a sports physician. Screenshots are depicted in the Annex A in Section V

III. Enhancing the scheme ”Practical Attribute-based Encryption”

Liu et al.'s Practical Attribute-based Encryption (PABE) [9] scheme supports monotonic access structures only. We will extend this scheme to support (unbounded) non-monotonic access structures. We borrow techniques from Yamada et al. presented in [7] which build on top of [10]. For our work we decided to use the notation applied by Liu et al. [9]. Next, we recapture the PABE's Augmented R-CP-ABE construction and emphasize the modifications required for achieving the non-monotonic and unbounded access structures property. The blue colored parts indicate the additional computations required to achieve the non-monotonic property. Black colored formulas indicate the original PABE construction.

A. Setup

$$Setup_A(\lambda, N = m^2) \rightarrow (PP, MSK) \tag{1}$$

Setup calls the group generator $G(\lambda)$ to get (e, p, G, G_T) where e is a bilinear map and p is the prime order of $\mathbb{G}$ and $\mathbb{G}_T$. The attribute universe is $\mathcal{U} = \mathbb{Z}_p$. The algorithm picks randomly

$g, h, f, f_1, ..., f_m, G, H \in \mathbb{G}, \{a_i, r_i, z_i \in \mathbb{Z}_p\}_{i \in [m]}$,
$\{c_j \in \mathbb{Z}_p\}_{j \in [m]}$

and returns the master secret key and the public parameters:

$$\begin{aligned} PP =& \Big((p, \mathbb{G}, \mathbb{G}_T, e), g, h, f, f_1, ..., f_m, G, H, \{E_i = e(g,g)^{\alpha_i}, \\ & G_i = g^{r_i}, Z_i = g^{z_i}\} i \in [m], \{H_j = g^{c_j}\} j \in [m]\Big) \\ MSK =& \Big(\alpha_1, ..., \alpha_m, r_1, ..., r_m, c_1, ..., c_m\Big) \\ MSK_{new} =& MSK \bigcup \{q \in \mathbb{Z}_p\} \\ PP_{new} =& PP \bigcup \{G' = H^q\} \end{aligned} \tag{2}$$

B. Keygen

$$KeyGen_A(PP, MSK, S \subseteq \mathbb{Z}_p) \rightarrow SK_{(i,j),S} \tag{3}$$

Choose $\{\delta'_{i,j,x} \in \mathbb{Z}_p\}_{\forall x \in S}$ such that $\delta'_{i,j,x_1} + \cdots + \delta'_{i,j,x_k} = \sigma_{i,j}$ with $k = |S|$.
Keygen then outputs the private key (conform to [9]) as

$SK_{(i,j),S} = ((i,j), S, K_{i,j}, K'_{i,j}, K''_{i,j}, \{\bar{K}_{i,j,j'}\}_{j' \in [m] \setminus \{j\}}$,

$\{K_{i,j,x}, K'_{i,j,x}\}_{\forall x \in S})$ where $K_{i,j} = g^{\alpha_i} g^{r_i c_j} (f f_j)^{\sigma_{i,j}}$,

$K'_{i,j} = g^{\sigma_{i,j}}, K''_{i,j} = Z_i^{\sigma_{i,j}}, \{\bar{K}_{i,j,j'} = f_{j'}^{\sigma_{i,j}}\}_{j' \in [m] \setminus \{j\}}$,

$\{K_{i,j,x} = g^{\delta_{i,j,x}}, K'_{i,j,x} = (H^x h)^{\delta_{i,j,x}} G^{-\delta_{i,j}}\}_{x \in S}$.

Now we extend the SK with additional computations in order to achieve support for attribute negations:

$SK_n = SK \bigcup \left\{\widetilde{K}_{i,j,x}, \widetilde{K}'_{i,j,x}\right\}_{\forall x \in S}$
with $\widetilde{K}_{i,j,x} = g^{q\delta'_{i,j,x}}$ and $\widetilde{K}'_{i,j,x} = \left(H^{qx} h^q\right)^{\delta'_{i,j,x}}$.

C. Encrypt

$$Encrypt_A(PP, M, R, \mathbb{A} = (A, \rho), (\bar{i}, \bar{j})) \rightarrow CT_{R,(A,\rho)} \tag{4}$$

For every attribute $x \in S$, check if x is primed (negated) and set P_k accordingly with $\rho(k) = x$:

$$P_k = \begin{cases} f^{A_k \cdot \mathbf{u}} G^{\xi_k} & \text{if } \rho(k) = x \\ f^{A_k \cdot \mathbf{u}} (G')^{\xi_k} & \text{if } \rho(k) = x' \end{cases}$$

D. Decrypt

$$Decrypt_A(PP, CT_{R,(\mathbb{A}=A,\rho)}, SK_{(i,j),S}) \rightarrow M \quad or \quad \perp \tag{5}$$

Compute d_k for all k with $\rho(k) \in S$.

$$D_P = \prod_{\rho(k) \in S} d_k^{\omega_k}, \omega_k \in \mathbb{Z}_p$$

$$d_k = \begin{cases} e\left(K'_{i,j}, P_k\right) \cdot \\ e\left(K_{i,j,\rho(k)}, P'_k\right) \cdot e\left(K'_{i,j,\rho(k)}, P''_k\right) & \text{if } \rho\left(k\right) = x \\ \\ e\left(K'_{i,j}, P_k\right) \cdot \prod_{z \in [k]} (e\left(\widetilde{K}_{i,j,\rho(z)}, P'_k\right) \cdot \\ e\left(\widetilde{K}'_{i,j,\rho(z)}, P''_k\right))^{\frac{1}{\rho(k)-\rho(z)}} & \text{if } \rho\left(k\right) = x' \end{cases}$$

Using non-monotonic access structures breaks with the malicious user traceability property. A new blackbox traceability solution must be researched.

The correctness of the scheme is proven under the Extended source group q-parallel BDHE assumption, as introduced in [9] and for the unbound non-monotonic computation under n-(B) assumption [7]. Both are closely related to the q-1 assumption in [6].

IV. Conclusion

We summarize our contribution next.

- We gave a overview of the Entrance system and its components.
- We apply the findings of Yamada et al. [7] to enhance Liu et al.'s ABE scheme [9] in order to support non-monotonic access structures.
- We implemented a basic version (without including the computations of Liu's revocation approach) in Java using jPBC.

A. outlook

Future work could be to provide the calculations for consideration of the revocation list.

Acknowledgment

The work presented in this paper was performed in the context of the *Entrance* project. *Entrance* is a Software Campus project and is funded by the German Federal Ministry of Education and Research (BMBF) [11] (Grant Number 01IS12056). The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the BMBF. Responsibility for the information and views expressed here lies entirely with the authors. Special thanks go to Artjom Butyrtschik for his implementation work on the monotonic scheme and his initial reference to the work of Yamada et al.

References

[1] Z. Liu and D. S. Wong, "Practical Attribute Based Encryption: Traitor Tracing, Revocation, and Large Universe," *IACR Cryptology ePrint Archive*, 2014, available at https://eprint.iacr.org/2014/616.

[2] S. Zickau, D. Thatmann, A. Butyrtschik, I. Denisow, and A. Küpper, "Applied Attribute-based Encryption Schemes," in *Proceedings of the 19th IEEE International Conference Innovation in Clouds, Internet and Networks (ICIN 2016)*. Paris, France: IEEE Computer Society, March 2016, pp. 88–95.

[3] D. Thatmann, A. Butyrtschik, and A. Küpper, "A secure DHT-based key distribution system for attribute-based encryption and decryption," in *Signal Processing and Communication Systems (ICSPCS), 2015 9th International Conference on*, Dec 2015, pp. 1–9.

[4] D. Thatmann, P. Raschke, and A. Küpper, ""Please, no more GUIs!": A user study, prototype development and evaluation on the integration of Attribute-based Encryption in a hospital environment," in *40th IEEE Computer Society International Conference on Computers, Software and Applications (Compsac 2016) - User Centered Design and Adaptive Systems (UCDAS)*. Atlanta, USA: IEEE Computer Society, June 2016.

[5] Z. Liu, Z. Cao, and D. S. Wong, "Blackbox Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on Ebay," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 475–486.

[6] Y. Rouselakis and B. Waters, "Practical Constructions and New Proof Methods for Large Universe Attribute-based Encryption," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 463–474.

[7] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption," Cryptology ePrint Archive, Report 2014/181, 2014, http://eprint.iacr.org/.

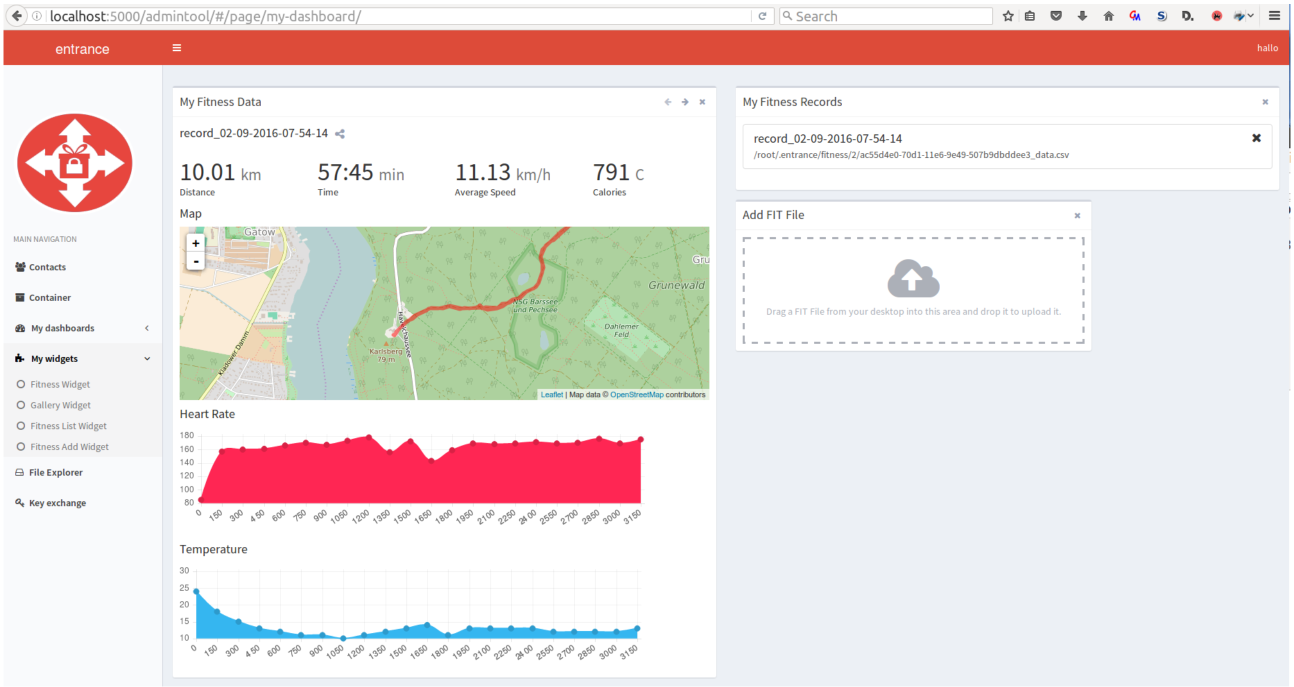
[8] P. Maymounkov and D. Mazières, "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01. London, UK, UK: Springer-Verlag, 2002, pp. 53–65.

[9] Z. Liu and D. S. Wong, "Practical Attribute Based Encryption: Traitor Tracing, Revocation, and Large Universe," *IACR Cryptology ePrint Archive*, 2014.

[10] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based Encryption with Non-monotonic Access Structures," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 195–203.

[11] "Federal Ministry of Education and Research (BMBF)." [Online]. Available: http://www.bmbf.de/en/

V. Annex A



My Fitness Data

record_02-09-2016-07-54-14

10.01 km	57:45 min	11.13 km/h	791 C
Distance	Time	Average Speed	Calories

Map

Heart Rate

Temperature

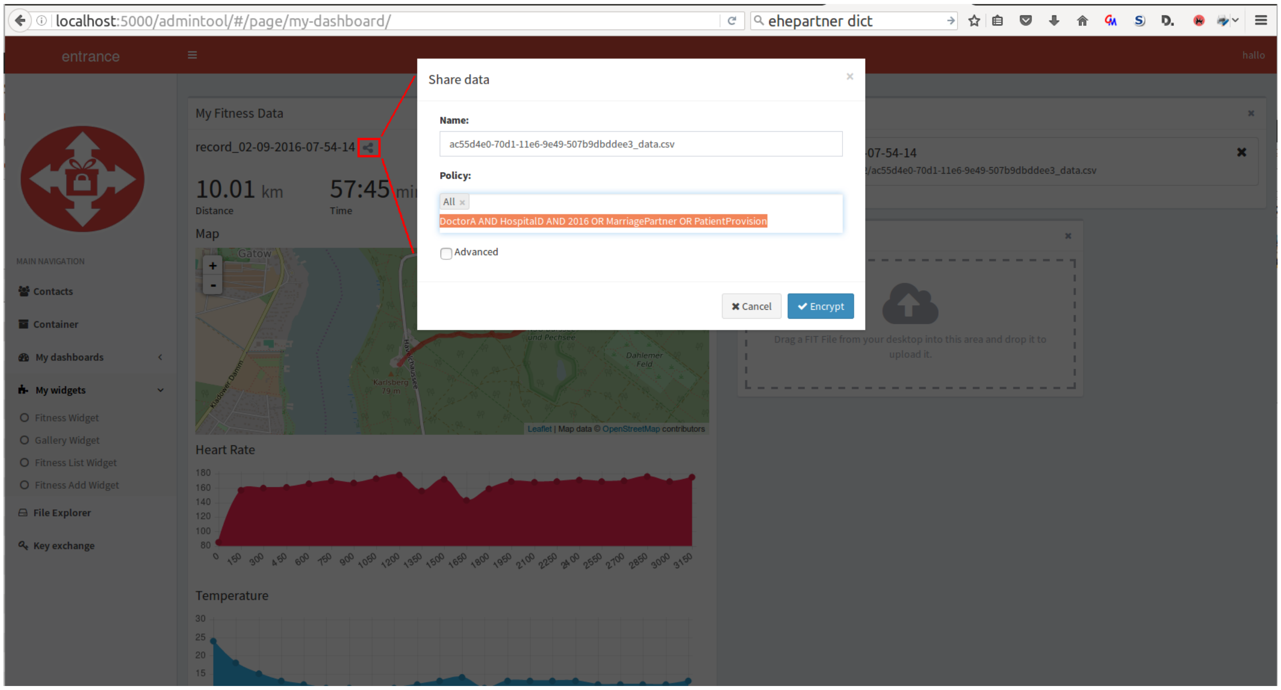
My Fitness Records

record_02-09-2016-07-54-14
/root/.entrance/fitness/2/ac55d4e0-70d1-11e6-9e49-507b9dbddee3_data.csv

Add FIT File

Drag a FIT File from your desktop into this area and drop it to upload it.

Fig. 2. Entrance-Dashboard: Representation of a training unit with details on running distance, speed, heart rate and outside temperature



Share data

Name:

ac55d4e0-70d1-11e6-9e49-507b9dbddee3_data.csv

Policy:

All ×

DoctorA AND HospitalD AND 2016 OR MarriagePartner OR PatientProvision

□ Advanced

✖ Cancel ✔ Encrypt

Fig. 3. Entrance-Dashboard: Creating an access structure