DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Implementation of Attribute-Based Encryption in Rust on ARM Cortex M Processors

Daniel Bücheler

DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Implementation of Attribute-Based Encryption in Rust on ARM Cortex M Processors

Implementierung von Attributbasierter Verschlüsselung in Rust auf ARM Cortex M Prozessoren

Author:	Daniel Bücheler
Supervisor:	Prof. Dr. Claudia Eckert
Advisor:	Stefan Hristozov
Submission Date:	15.04.2021

I confirm that this bachelor's thesis in informatics is my own work and I have documented all sources and material used.

Munich, 15.04.2021 Daniel Bücheler

Acknowledgments

Abstract

Contents

1 Introduction

2 Preliminaries

This chapter introduces Attribute-Based Encryption and the relevant mathematical background for implementing it.

2.1 Confidentiality with Classic Symmetric and Asymmetric Cryptography

Today's conventional cryptography knows two main classes of cryptosystems: symmetric encryption schemes and asymmetric encryption schemes. See Figure 2.1 for an illustration of the differences.

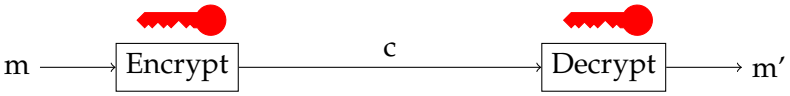
Consider n participants wanting to communicate securely (i.e. no user can read encrypted messages between two other users). Using a symmetric encryption scheme, each participant would need to agree on a unique key with every other participant, resulting in a total number of $\frac{n(n-1)}{2}$ keys. Using a asymmetric encryption scheme reduces the number of keys to only n, because each participant could obtain everyone else's public key and then send messages to them securely.

Another problem remains, however: Encrypting a single message to a large number of participants requires encrypting it with everyone's public key separately. For a large number of recipients, this is inefficient. So, for example, to encrypt a message for all students of a certain university, we'd need to obtain each student's public key and encrypt the message with each key separately.

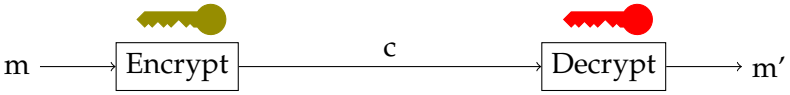
Even worse, what if we want to encrypt data for any student of said university, even if they *haven't joined the university yet*. In this case, our only option using classic asymmetric cryptography would be to have some trusted instance keep a plaintext copy and re-encrypt the data for any new student when they join the university. Attribute-Based encryption solves this problem.

2.2 Attribute-Based Encryption

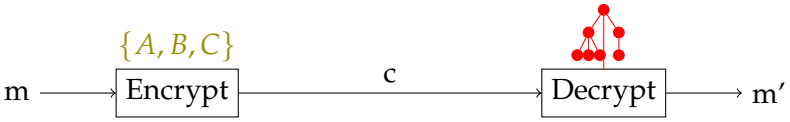
Attribute-Based Encryption (ABE) uses a combination of attributes to define a *group* of private keys that should be able to read encrypted data, instead of encrypting it for one



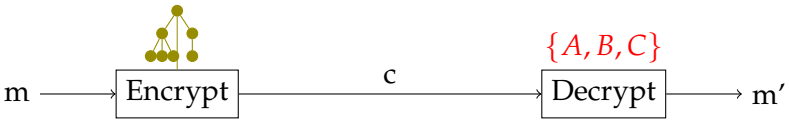
(a) Symmetric Encryption: Both keys are identical.



(b) Asymmetric Encryption: Different keys for encryption and decryption.



(c) Key-Policy Attribute-Based Encryption: Attributes for encryption, access structure for decryption. Note that the access structure of the decryption key may be public; the actual key consists of secret shares that allow the user to decrypt a ciphertext if the correct attributes are present.



(d) Ciphertex-Policy Attribute-Based Encryption: Access policy for encryption, attributes for decryption. Note that the attributes associated with the decryption key may be public; the actual key consists of corresponding secret shares.

Figure 2.1: Keys used for encryption and decryption in different classes of encryption schemes. Red information has to be kept secret, green information may be made publicly available. For the differences between the two types of ABE, see Section 2.2.3.

specific private key only (as in asymmetric encryption schemes). In Figure 2.1d, this is represented by a tree.

The combination of attributes may be as restrictive or permissive as needed. It is possible to create ciphertexts that can be read by almost all members of an ABE scheme, and ciphertexts that can be read by nobody except a few selected participants.

Figure 2.2 shows a small ABE system with the KGC initializing the system and issuing keys, and two users sharing an encrypted message.

2.2.1 Attributes and the Key Generation Center

In essence, attributes are strings describing certain characteristics or features of actors and objects. For example, a typical freshman student of informatics at TUM could be described by the attributes `"semester count 1"`, `"computer science"`, `"tum"`, `"is young"`, `"started degree in 2017"`.

These attributes themselves don't contain any information to which users or object they apply; instead this is a matter of interpretation. Some attributes may be very clearly defined, e.g. `"started degree in 2017"` from above. For others, it may be more difficult to decide whether they apply, e.g. the attribute `"is young"`: Until what age is a student young?

In any instance of ABE, there needs to exist an arbiter who decides whether an attribute applies to a certain user or object. This role is assumed by a trusted third party, the Key Generation Center (KGC). It has two main responsibilities: First, the KGC decides which attribute applies to which user. Second, it issues private keys corresponding to these attributes, and hands these to the users.

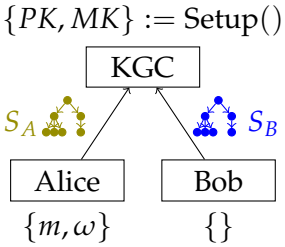
Without this KGC, there is no ABE. This differs from traditional public-key encryption schemes, where any user can independently create their own keypair.

Regarding the set of possible attributes (called the *attribute universe*), there are two possibilities: In a large universe construction, all possible strings can be used as attributes [1]. In a small universe construction, the universe of attributes is explicitly fixed when the system is instantiated, i.e. when the KGC runs the *Setup* algorithm (see below, section 2.2.2) [1]. With a small universe construction, the size of the public parameters usually grows with the size of the attribute universe [1].

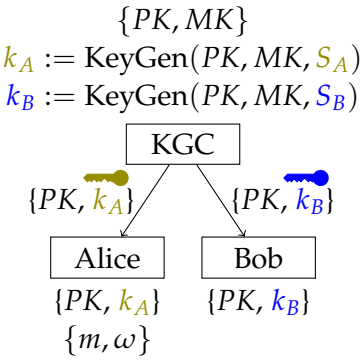
2.2.2 Formal definition of an ABE Scheme

We will define a KP-ABE scheme here, for the difference between CP-ABE and KP-ABE and formal definitions of Access Trees, see the next sections.

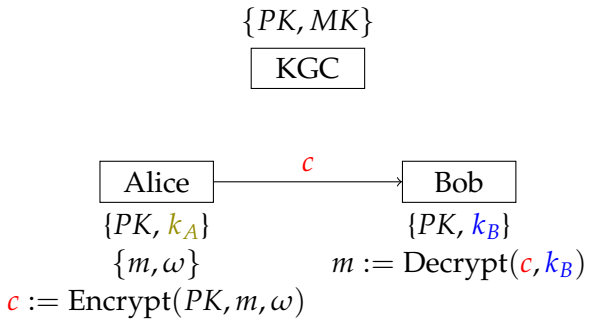
Definition 2.1. A (Key-Policy) Attribute-Based Encryption scheme consists of the following four algorithms: [1]



(a) The KGC sets up the system and obtains Alice's and Bob's desired access policies.



(b) If S_A and S_B are allowed access policies for Alice and Bob, respectively, the KGC creates their private keys and transmits them via a secure channel.



(c) Alice can now use the public parameters PK and ω to encrypt a message for Bob, which he can decrypt only if his access policy S_B is satisfied by ω. Note that the KGC plays no role in this step

Figure 2.2: Alice wants to send an KP-ABE encrypted message m to Bob. She wants to encrypt the message under a set of attributes ω. Both Alice and Bob create a desired access policy, S_A and S_B, respectively. Note that the KGC will only issue a corresponding key if it deems that they should be allowed to obtain a key under the given access policy.

- *Setup*. Run once by the Key Generation Center (KGC). Sets up the system by generating public parameters PK and a private master key MK. The public parameters are shared with all participants, while the master key remains only known to the KGC.
- *KeyGen(PK, s, S)*. Input: public parameters PK, master secret s and access structure S.
  Run by the trusted authority once for each user to generate their private key. Returns a private key k corresponding to S.
- *Encrypt(PK, m, ω)*. Input: public parameters PK, plaintext message m and set of attributes ω.
  Run by any participant of the system. Encrypts m under ω and returns the ciphertext c.
- *Decrypt(c, k)*. Input: ciphertext c (output of *Encrypt*) and key k (output of *KeyGen*).
  Run by any participant holding a private key generated by *KeyGen*. Outputs the correctly decrypted message m' if and only if the set of attributes under which m was encrypted satisfies the access structure under which k was created.

The definition of a CP-ABE scheme is identical, except that *Encrypt(PK, m, S)* takes an access structure S and *KeyGen(PK, s, ω)* takes a set of attributes.

How exactly these algorithms work in concrete ABE schemes will be discussed in Section 4.

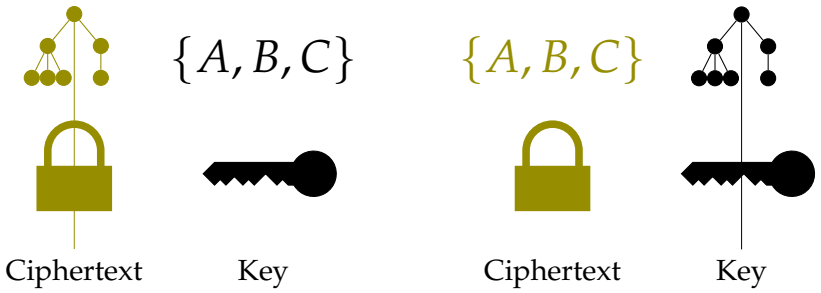
2.2.3 KP-ABE and CP-ABE

Two components are necessary to specify a group of keys that shall be able to decrypt a ciphertext: A number of attributes that are present, and a policy that defines a combination of required attributes. Each of these can either be associated with the ciphertext, or with the decryption key:

In Ciphertext-Policy ABE (CP-ABE), so the key is associated with a set of attributes and the ciphertext is encrypted under an access policy. Key-Policy ABE (KP-ABE) works the other way around, so the ciphertext is associated with a set of attributes, and the key is associated with an access policy. See Figure 2.3 for illustration.

In both cases, a ciphertext can be decrypted if and only if the set of attributes specified in one part satisfy the access policy associated with the other part.

CP-ABE tends to be more intuitive because, when encrypting a plaintext, the encryptor controls rather explicitly who can decrypt their ciphertext: They set the access policy that defines which combinations of attributes are required from the users to successfully decrypt the ciphertext [2].



(a) CP-ABE (b) KP-ABE

Figure 2.3: CP-ABE vs. KP-ABE: Association of key and ciphertext with Access Policy and set of attributes.

With KP-ABE, on the other hand, the encryptor doesn't have any control over who will be able to access the data, except for the choice of attributes under which they encrypt the plaintext [2]. Instead, the Key Generation Center must be trusted with intelligently deciding which key to give to the decrypting party [2]. For example, imagine a KP-ABE system in which it is common practice to label all ciphertexts with an attribute corresponding to the version number of the encryption software used. If the KGC were to give out a key containing a monotone access structure satisfied by just a single attribute corresponding to a commonly-used version of this software, this key could be used to decrypt any ciphertext - completely disregarding any other attributes that might be associated with it.

An example use case for CP-ABE in a hospital setting would be sending an encrypted note about problems with a specific treatment to all doctors, patients that received that treatment and nurses of the department that administered the treatment. This could be specified by an access policy as (`hospital-name` AND (`doctor` OR (`patient` AND `received-treatment-x`) OR (`nurse` AND `department-y`)).

In the same hospital setting, KP-ABE could be employed in a different use case: When storing medical data about a patient, CP-ABE would require re-encrypting the data under a new access policy whenever a patient needs to see a different doctor. With KP-ABE, the data could instead be associated with the patient's name as an attribute, and the hospital's IT department could extend the new doctor's key's policy to allow decrypting the new patient's data.

2.2.4 Access Structures

Access structures formally determine which sets of attributes are required to reconstruct the ciphertext under ABE. This definition is adapted from [3] for our setting of allowed

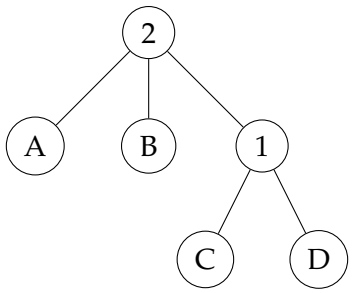


Figure 2.4: Sample Access Tree over the attributes `A`, `B`, `C`, `D`.

attribute sets, instead of allowed parties.

Definition 2.2. Access Structure [3].
Let $U = \{A_1, \ldots, A_n\}$ be the universe of attributes. A set $\mathcal{A} \subseteq 2^U$ is monotone if for all $B \in \mathcal{A}$ and $C \supseteq B$, $C \in \mathcal{A}$. An access structure $\mathcal{A}$ is a non-empty subset of 2^U, i.e. $\mathcal{A} \in 2^U \backslash \{\emptyset\}$. A monotone access structure is an access structure that is monotone. The sets in $\mathcal{A}$ are called the *authorized sets*, those not in $\mathcal{A}$ are called the *unauthorized sets*.

Intuitively, the monotonicity of an access structure means that adding an attribute to an authorized set cannot result in an unauthorized set.

2.2.5 Access Trees

Explicitly specifying an access structure is not feasible, as its size may be exponential in the size of the attribute universe. Therefore, we will use the construction of *Access Trees* from Goyal et al. in [1]. Each leaf of this tree is labelled with an attribute, and each interior node is labelled with an integer, the threshold for it to be satisfied [1].

Figure 2.4 illustrates an example for an Access Tree. It is satisfied by any set of attributes that contains two of A, B and either C or D. That is, $\{A, B\}$ would satsify the tree, just as $\{B, D\}$ would, but $\{C, D\}$ would not be sufficient. For an attribute universe of $U = \{A, B, C, D\}$ this would realize the access structure $\mathcal{A} = \{\{A, B, C, D\}, \{A, B, C\}, \{A, B, D\}, \{A, C, D\}, \{B, C, D\}, \{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}\}$

Definition 2.3. Access Tree [1].
An interal node x of an access tree is defined by its children and a threshold value d_x. If x has num_x children, then its threshold value satisfies $0 < d_x \leq num_x$.
A leaf node x is defined by an attribute and a threshold value $k_x = 1$.

[1] also defines the following functions for working with access trees: The parent of a node x in the access tree is denoted by $\text{parent}(x)$. If x is a leaf node, $\text{att}(x)$ denotes the attribute associated with x; otherwise it is undefined. The children of a node x are

numbered from 1 to num_x. Then index(y) denotes the unique index of y among the children of its parent node.

Definition 2.4. Satisfying Access Trees [1].
Let $\mathcal{T}$ be an access tree with root r and $\mathcal{T}_x$ the subtree with x as its root. If a set of attributes γ satisfies the access tree $\mathcal{T}_x$, we write $\mathcal{T}_x(\gamma) = 1$; otherwise $\mathcal{T}_x(\gamma) = 0$.
If x is a leaf node, then $\mathcal{T}_x(\gamma) = 1$ if and only if attr$(x) \in \gamma$.
If x is an internal node, then $\mathcal{T}_x = 1$ if and only if d_x or more of the children x' of x return $\mathcal{T}_{x'}(\gamma) = 1$.

The set of attribute sets that satisfy a tree $\mathcal{T}$ is then the access structure it represents: $\mathcal{A} = \{\gamma \in 2^U | \mathcal{T}(\gamma) = 1\}$. Note that $\mathcal{A}$ has to be monotone. It is not possible to specify that the *absence* of an attribute in the tree.

Using the threshold-gate construction, we can express *A AND B* as a node with two children A and B and threshold 2, and express *A OR B* as a node with two children A and B and threshold 1 [4].

2.2.6 Linear Secret Sharing Schemes and Span Programs

Instead of the access tree construction, nowadays most ABE schemes use monotone monotone span programs (MSPs) to describe any access structure realizable by linear secret sharing scheme (LSSS). For a definition of LSSS see [3]. Also see there for a proof of the equivalence of LSSS and MSP.

It is conjectured, but not proven, that there are access structures that require secret shares of exponential size in any secret sharing scheme that realizes them [3]. This would especially mean that not all access structures can be realized by LSSS (as their shares are smaller than exponential). LSSS-realizable access structures seem to be the most general type of access structures supported by ABE schemes in literature.

Any access structure that can be described by an access tree can also be described by a MSP or LSSS. For an efficient conversion from Boolean Formulas (which are essentially access trees limited to two children per inner node) to monotone span programs, see the appendix of [5]. A more general construction for the threshold trees described in Section 2.2.5 is given in [6].

MSPs can realize more general access structures than access trees and better suited for the design of ABE schemes [7].

Definition 2.5. (Monotone) Span Program. Adapted from [1], [3].
Let $\mathbb{K}$ be a field and $\{x_1, \ldots, x_n, \}$ a set of variables.
A span program over $\mathbb{K}$ is a labelled matrix $\hat{M} = (M, \rho)$ where M is a matrix over $\mathbb{K}$. ρ is a function that labels every row of M by one literal from $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$.

Span programs reject or accept inputs as follows: For an input set $\gamma \subseteq \{x_1, \ldots, x_n\}$ let M_γ define the submatrix of M consisting only of those rows whose labels are contained in γ, and the rows labelled by a negated literal $\bar{x}_i$ that is not contained in γ. That means M_γ contains a row i if $\rho(i) = x_j$ and $x_j \in \gamma$ or $\rho(i) = \bar{x}_j$ and $x_j \notin \gamma$. The MSP accepts γ if and only if $\vec{1} \in \text{span}(M_\gamma)$, i.e. there exists a linear combination of the rows of M_γ that is the row vector consisting of only ones ($\vec{1} = (1, \ldots, 1)$).

A span program is called *monotone* if the rows are labelled using only the (positive) literals $\{x_1, \ldots, x_n\}$.

Note that the vector $\vec{1}$ can be replaced by any other fixed nonzero vector [3].

Intuitively, a row i labelled by the literal $\rho(i) = x$ is labelled with the *positive* of x; a row labelled by $\rho(i) = \bar{x}$ is labelled by the *negative* of x.

The linear combination yielding $\vec{1}$ may only consist of the rows labelled with positive attributes that are included in γ and those labelled with negative literals not included in γ. That means there are coefficients $\{\alpha_i\}_{\rho(i)\in\gamma \text{ or } \rho(i)=\bar{x}\wedge x\notin\gamma}$ such that $\sum \alpha_i \cdot M_i = \vec{1}$. M_i denotes the i-th row of the matrix M.

The role of the variables in the definition will be taken by attributes in our context, i.e. each row will be labelled by an attribute or the negation of an attribute [1].

2.3 Shamir's Secret Sharing

This secret sharing scheme based on polynomial interpolation was first introduced by Adi Shamir in 1979 [8]. It allows a secret s, which is generally just a number, to be shared among a number of n participants. The shares are computed such that s can be reconstructed if, and only if, at least k participants meet and combine their shares. Such a theme is then called a (k, n)-threshold scheme. [8]

2.3.1 Lagrange interpolation

Shamir's scheme makes use of a property of polynomials: A polynomial of degree d is unambiguously determined by $d + 1$ points (x_i, y_i). In other words, any polynomial of degree d can be unambiguously interpolated (reconstructed) from $d + 1$ distinct points.

To interpolate a polynomial of degree d from $d + 1$ given points $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, we can make use of the lagrange basis polynomials: [4]

Definition 2.6. Lagrange interpolation: Given a set of $d + 1$ points $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$.

Then the polynomial

$$L(x) = \sum_{k=0}^{d} \Delta_{\omega,x_k}(x) \cdot y_k \tag{2.1}$$

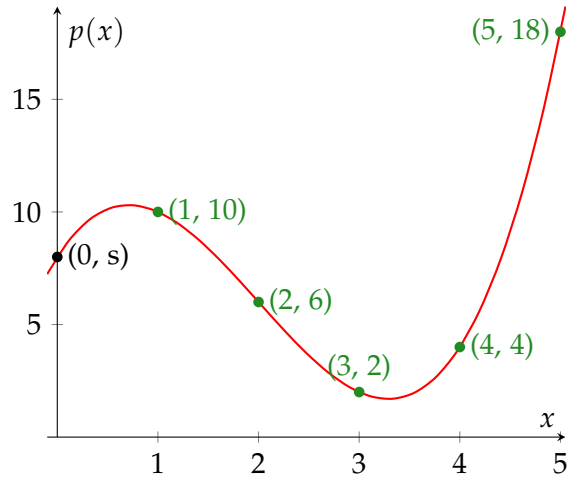


Figure 2.5: Example for a $(5,4)$-threshold scheme with $s = 8$ and $p(x) = 8 + 7x - 6x^2 + x^3$. The five green-colored points are distributed as the secret shares. As $p(x)$ has degree three, at least four shares are required to reconstruct s.

is the lagrange interpolation polynomial for that set of points, where $\omega = \{x_1, \ldots, x_{d+1}\}$ and $\Delta_{\omega,k}(x)$ are the Lagrange basis polynomials:

$$\Delta_{\omega,k}(x) = \prod_{\substack{i \in \omega \\ i \neq k}}^{d} \frac{x - i}{k - i} \tag{2.2}$$

This polynomial has degree d. If the points (x_i, y_i) lie on a d-degree polynomial, then the lagrange interpolation $L(x)$ is *exactly* that polynomial.

On the other hand, if there are less than $d + 1$ points of a d-degree polynomial known, there are infinitely many d-degree polynomials that pass through all given points. [8]

2.3.2 Secret sharing with polynomials

To share our secret, we now hide it in a polynomial and give out points on this polynomial as secret shares. Using the lagrange basis polynomials, we can then reconstruct $p(x)$ and thus the secret if we know enough shares [8].

Definition 2.7. Shamir's (k, n)-threshold secret sharing scheme [8]. To share a secret s among n participants such that s can be recovered if and only if k or more shares are combined, do:

1. Pick coefficients $a_1, ..., a_{k-1}$ at random

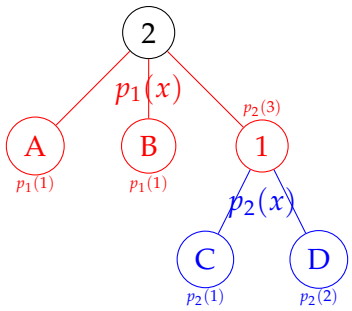


Figure 2.6: Access Tree from Figure 2.4 showing how Shamir's Secret Sharing is employed recursively. $p_1(x)$ is a the polynomial of a $(2,3)$-threshold scheme, $p_2(x)$ of a $(1,2)$-threshold scheme. Shown in small are the secret shares embedded into each node.

2. Set $a_0 = s$. This results in the polynomial $p(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$. Note that $p(0) = s$.
3. The secret shares are $(1, p(1)), (2, p(2)), \ldots, (n, p(n))$. Give one to each participant.

To reconstruct the secret from any subset of k shares, interpolate the polynomial $p(x)$ and evaluate $p(0) = s$.

See also Figure 2.5 for illustration. In practice, the numbers would be far bigger and calculations wouldn't be performed over the real numbers, but rather a finite field modulo a prime [8].

2.3.3 Secret Sharing in Attribute Based Encryption

To realize an Access Tree that „gives away" a secret if and only if it is satsified by a set of attributes, we can recursively use Shamir's Secret Sharing scheme:

We use a secret-sharing polynomial on each internal node of the Access Tree: For a node x with threshold d_x and num_x children, we define a (d_x, num_x)-threshold scheme and embed one share of the secret in each child. Begin in the root, and set s as the secret we want to embed in the tree. For all other nodes, set s as the secret share received from the parent node.

If the child is a leaf, we modify the share such that it can only be used if the relevant attribute is present (how exactly this is done differs between CP-ABE and KP-ABE).

Now, let ω be a set of attributes. We have built our tree in such a way that the share embedded in a leaf node u can be used only if $\text{attr}(u) \in \omega$. That means, a leaf node's secret share can be used if and only if the set of attributes satisfies this leaf node.

For the internal nodes x, the use of a (d_x, num_x)-threshold scheme ensures that the secret embedded in x can be reconstructed if and only if the secret shares of at least d_x child nodes can be used, i.e. at least d_x child nodes are satisfied. Following this recursive definition up to the root, we can see that our secret s embedded in the root can be reconstructed exactly if ω satisfies the Acess Tree.

See Figure 2.6 for an illustration with the tree from Figure 2.4: Two (k, n)-threshold schemes are employed, one for each internal node of the access tree. $p_1(x)$ is the polynomial of the root's $(2, 3)$-threshold scheme, sharing s, the secret to be embedded in the tree (i.e. $p_1(0) = s$). $p_2(x)$ is the polynomial for the $(1, 2)$-threshold scheme belonging to the node labelled "1" and shares the value $p_1(3)$ that it received from the $(2, 3)$-threshold scheme of the layer above (i.e. $p_2(0) = p_1(3)$).

2.3.4 Revocation

So far, it is not possible to take away privileges from a user: Once the private key has been issued, it can not be taken back.A user's capabilities can only be extended (e.g. by issuing a key with additional attributes or with a more permissive policy). This is is an problem, e.g. if their private key is compromised [9].

The simplest approach is to simply renew the keys of valid users from time to time [9]. When a user is revoked, their key will not be updated any longer. Thus any ciphertexts encrypted after the next key update will not be readable for the revoked user [9]

This approach requires the KGC to update or re-issue one key per valid user and requires a secure channel to the KGC [9].

Attrapadung and Imai [10] differentiate between *direct* and *indirect revocation*: With direct revocation, the list of revoked users is directly specified by the encrypting party (i.e. the encryption takes a "black list" of revoked users). Indirect revocation achieves revocation by means of updating the keys of valid users, as described in the naive approach above.

Direct revocation requires the encryptor to know the list of revoked users [10] (i.e. the encrypting party is responsible for correct revocation of the users on the revocation list). With indirect revocation, the encryptor does not need to do anything except use the most recent version of the public parameters [10].

Direct revocation also works instantly: As soon as an encryptor knows about the revocation of a user, they will include them on their revocation list for future encryptions. With indirect revocation, a revoked user can still use their key normally until the next key update is distributed by the KGC [10].

2.4 Elliptic Curves

The mathematics of modern cryptosystems (including, but not limited to ABE) work any group that satisfies the axioms (see below), and elliptic curves are just one of them. Because Elliptic Curves allow for shorter key lengths than, e.g. groups modulo a prime, they have become very popular for use in cryptography. Exact definitions and notations differ, these are taken from the textbook *Introduction to Modern Cryptography* by Katz and Lindell [11].

2.4.1 Group Axioms

Definition 2.8. [11]. A *Group* consists of a set $\mathbb{G}$ together with a binary operation $\circ$ for which these four conditions hold:

- Closure: For all $g, h \in \mathbb{G}$, $g \circ h \in \mathbb{G}$.
- Existence of identity: There is an element $e \in \mathbb{G}$, called the *identity*, such that for all $g \in \mathbb{G}$, $g \circ e = g = e \circ g$.
- Existence of inverse: For every $g \in \mathbb{G}$ there exists an *inverse* element $h \in \mathbb{G}$ such that $g \circ h = e = h \circ g$.
- Associativity: For all $g_1, g_2, g_3 \in \mathbb{G}$, $(g_1 \circ g_2) \circ g_3 = g_1(\circ g_2 \circ g_3)$.

When $\mathbb{G}$ has a finite number of elements, the group $\mathbb{G}$ is called finite and $|\mathbb{G}|$ denotes the order of the group.

A group $\mathbb{G}$ with operation $\circ$ is called *abelian* or commutative if, in addition, the following holds:

- Commutativity: For all $g, h \in \mathbb{G}, g \circ h = h \circ g$.

When the binary operation is clear from context, we simply use $\mathbb{G}$ to denote the group.

We also define *Group Exponentiation*: $g \in \mathbb{G}, m \in \mathbb{N}^+$, then $mg = \underbrace{g \circ \cdots \circ g}_{m \text{ times}}$.

Usually, the symbol used to denote the group operation is not the $\circ$ from above, but either $+$ or $\cdot$. These are called *additive* and *multiplicative* notation, respectively. It is important to remember, though, that the group operation might be defined completely differently!

In multiplicative notation, the group exponentiation of $g \in \mathbb{G}$ with $m \in \mathbb{N}^+$ is written as g^m, in additive groups it is written as $m \cdot g$.

2.4.2 Elliptic Curves

Definition 2.9. Given a prime $p \geq 5$ and $a, b \in \mathbb{Z}_p$ with $4a^2 + 27b^2 \neq 0 \bmod p$, the Elliptic Curve over $\mathbb{Z}_p$ is: [11]

$$E(\mathbb{Z}_p) := \{(x, y) \mid x, y \in \mathbb{Z}_p \text{ and } y^2 = x^3 + ax + b \bmod p\} \cup \{\mathcal{O}\} \tag{2.3}$$

a and b are called the curve parameters, and the requirement that $4a^2 + 27b^2 \neq 0 \bmod p$ makes sure that the curve has no repeated roots [11]. The curve is simply the set of points $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ that satisfy the curve equation $y^2 = x^3 + ax + b \bmod b$. One special point is added, the *point at infinity* denoted by $\mathcal{O}$. This will help define the point addition as a group operation in the next paragraph. [11]

2.4.3 Point Addition

Now, it is possible to show that every line intersecting a curve $E(\mathbb{Z}_p)$ intersects it in exactly three points, if you (1) count tangential intersections double and (2) count any vertical line as intersecting the curve in the point at infinity $\mathcal{O}$ [11]. Therefore, $\mathcal{O}$ can be thought of as sitting "above" the end of the y-axis [11]. Figure 2.7 shows all four different combinations, feel free to convince yourself that this statement indeed makes sense for the plotted curve.

Using this intersecting line, we can define an operation on curve points:

Definition 2.10. Given an Elliptic Curve $E(\mathbb{Z}_p)$, we define a binary operation called *(point) addition* and denoted by $+$: [11]
Let $P_1, P_2 \in E(\mathbb{Z}_p)$.

- For two points $P_1, P_2 \neq \mathcal{O}$ and $P_1 \neq P_2$, their sum $P_1 + P_2$ is evaluated by drawing the line through P_1 and P_2. This line will intersect the curve in a third point, $P_3 = (x_3, y_3)$. Then the result of the addition is $P_1 + P_2 = (x_3, -y_3)$, i.e. P_3 is reflected in the x-axis (Figure 2.7-1). If $P_3 = \mathcal{O}$, then the result of the addition is $\mathcal{O}$ (Figure 2.7-3).
- If $P_1, P_2 \neq \mathcal{O}$ and $P_1 = P_2$, as above but draw the line as tangent on the curve in P_1 (Figure 2.7-2 and -4).
- If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2$ and vice-versa.

We will be adding points to themselves a lot. Therefore, we define for ease of notation:

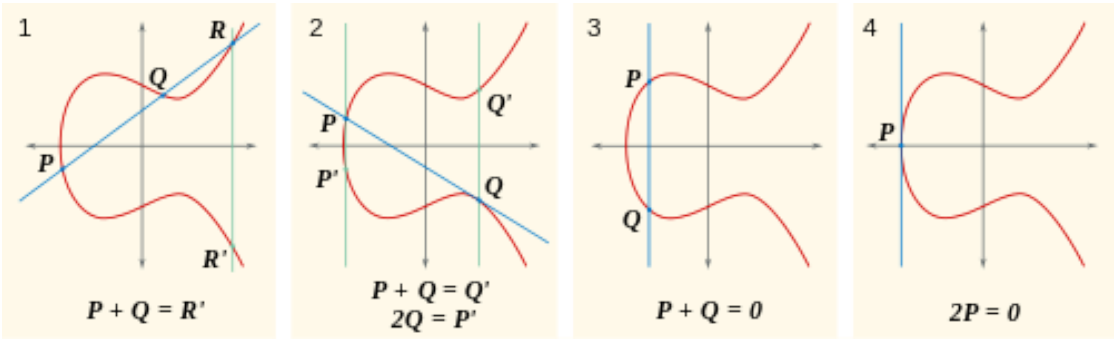


Figure 2.7: Elliptic Curve point addition
(Image by SuperManu, licensed under Creative Commons.)

Definition 2.11. Point-Scalar multiplication: Given a point $P \in E(\mathbb{Z}_p)$ and a scalar $d \in \mathbb{N}$:

$$d \cdot P = \underbrace{P + P + \cdots + P}_{d \text{ times}} \tag{2.4}$$

That is exactly the definition of group exponentiation, applied to our additive Elliptic Curve group. Note that the product of a scalar with a point is again a point on our curve.

2.4.4 Groups on Elliptic Curves

Theorem 2.1. *The points of an Elliptic Curve $E(\mathbb{Z}_p)$ plus the addition law as stated in Definition 2.10 forms an abelian (commutative group) [11], [12]:*

Proof. A formal proof is outside the scope of this thesis, but here's some informal reasoning about the group axioms:

- Existence of Identity: $P + \mathcal{O} = P$ (as per definition)
- Commutativity: For all $P_1, P_2 \in E(\mathbb{Z}_p)$, $P_1 + P_2 = P_2 + P_1$ (obvious, because the line through P_1 and P_2 will be the same)
- Unique inverse: For any point $P = (x, y) \in E(\mathbb{Z}_p)$, the unique inverse is $-P = (x, -y)$ (obvious).
- Associativity: For all $P_1, P_2, P_3 \in E(\mathbb{Z}_p)$, $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ (much less obvious, see e.g. [12, Chapter 2.4] for a proof).

□

Of particular interest to cryptography are *cyclic* groups on elliptic curves:

Definition 2.12. A (multiplicative) group $\mathbb{G}$ is cyclic if there is an element $g \in \mathbb{G}$ that generates $\mathbb{G}$, i.e. $\mathbb{G} = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}$.

Translated to our (additive) groups on elliptic curves, this means that there is a generator point $P \in E(\mathbb{Z}_p)$, such that every point $Q \in E(\mathbb{Z}_p)$ can be written as $Q = nP$ with some $n \in \mathbb{N}$.

Theorem 2.2. *[11] Let $\mathbb{G}$ be a finite group of order n, i.e. $|\mathbb{G}| = n$. Let $g \in \mathbb{G}$ be an element of $\mathbb{G}$ with order k, i.e. $k = |\langle g \rangle|$*
Then $k|n$, i.e. the order of g divides the group order n.

Proof. See [11, Proposition 8.54]. □

There is an important consequence to this fact: If a group has prime order, all points except the identity are generators. This stems from the fact that a prime number has exactly two divisors: One (the order of the identity) and itself (the order of all other points).
This follows from the fact that for any point $P \in E(\mathbb{Z}_p)$, its order $\text{ord}(P) = |\langle P \rangle|$ must divide the group order. A prime has exactly two divisors: One (the order of $\mathcal{O}$) and itself (the order of all other points).

Again, translated to Elliptic Curves this means that if the number of points $\#E(\mathbb{Z}_p)$ on a curve is prime, all points except $\mathcal{O}$ are generators. These cyclic elliptic curve groups (or, cyclic subgroups of non-cyclic elliptic curves) are exactly the groups we are interested in for doing actual cryptography. For a detailed description why, see [11, p. 321].

2.4.5 Bilinear Pairings

Definition 2.13. Bilinear pairing [13].
Let $\mathbb{G}_1$ and $\mathbb{G}_2$ denote cyclic groups with prime order n. Let $\mathbb{G}_T$ be another cyclic group of the same order n. $\mathbb{G}_1$ and $\mathbb{G}_2$ are written additively, $\mathbb{G}_T$ is written using multiplicative notation.
A *bilinear pairing* then is a function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ with the following properties:

- *Bilinearity.* For all $P_1, P_2 \in \mathbb{G}_1, Q_1, Q_2 \in \mathbb{G}_2$
  - $e(P_1 + P_2, Q_1) = e(P_1, Q_1) \cdot e(P_2, Q_1)$
  - $e(P_1, Q_1 + Q_2) = e(P_1, Q_1) \cdot e(P_1, Q_2)$
- *Non-Degeneracy.*

  - for each $P \in \mathbb{G}_1, P \neq 0$ there is a $Q \in \mathbb{G}_2$ with $e(P, Q) \neq 1$
  - for each $Q \in \mathbb{G}_2, Q \neq 0$ there is a $P \in \mathbb{G}_1$ with $e(P, Q) \neq 1$
- *Computability.* There is an algorithm that computes e efficiently.

If $\mathbb{G}_1 = \mathbb{G}_2$, the pairing is called a *symmetric pairing*, otherwise it is an *asymmetric pairing*.

There are a few different concrete pairing functions, e.g. the Weil pairing, Tate pairing and the Ate pairing [13]. Usually the source groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are subgroups of certain elliptic curves [13] and the target $\mathbb{G}_T$ is a finite field (*not* another point on a curve) [14].

3 Related Work

Attribute-Based Encryption was introduced by Sahai and Waters in 2005 [15]. They proposed a new type of identity-based encryption where identities are a set of attributes. Their so-called *fuzzy* identity-based encryption scheme allows a user to decrypt a ciphertext even if their identity doesn't exactly match the identity specified at the time of encryption [15]. Instead, an overlap larger than some threshold value between the attributes in the ciphertext's identity with the attributes of the key's identity is sufficient [15]. This property is realized by means of a (k, n)-threshold secret sharing scheme.

Sahai and Water's construction can already be seen as an ABE scheme with very limited expressiveness, i.e. it only works with "k-out-of-n" access structures [1].

In 2006, Goyal, Pandey, Sahai and Waters [1] extended this into the first expressive KP-ABE scheme using the access tree construction described in Chapter 2. Their main construction uses access trees and a small attribute universe, but they also give constructions with a large attribute universe and for linear secret sharing scheme (LSSS) access structures, respectively.

The first expressive CP-ABE scheme was proposed by Bethencourt, Sahai and Waters in [2]. It is also a large-universe construction and uses access trees. Waters [16] later also gives the first CP-ABE schemes with a security proof in the standard model, not only in the generic group model (the distinction is not relevant for this thesis).

Both the schemes in [1] and in [2] only support monotonic access structures.

In [1], an inefficient realization of general (non-monotonic) access structures is proposed, which is to simply represent the absence of an attribute as a separate attribute. This is inefficient because it doubles the total number of attributes in the system [1]. Non-monotonic access structures over a universe of n attributes are represented by monotonic access structures over a universe of $2n$ attributes. It also requires every ciphertext to be associated with n attributes (i.e. either with their positive or negated of a corresponding attribute). Note that the size of ciphertexts or keys is linear in the number of attributes in all expressive ABE schemes.

The first efficient construction for non-monotonic access structures was given in [17]. However, this construction leads to large private keys. More specifically, the size is $\mathcal{O}(t \log(n))$, where t is the number of leaf nodes in the key's access tree and n a system-wide bound on the number of attributes a ciphertext may have [18].

In [18] direct revocation is related to the realization non-monotone access structures and a scheme with efficient direct revocation is presented. The authors also present an efficient construction for non-monotone access structures with keys of size $\mathcal{O}(t)$ [18], where t is again the number of leaf nodes in the key's access tree.

The difference between direct and indirect revocation is introduced in [10], and a *Hybrid Revocable* ABE scheme is given. It allows the encryptor to choose the revocation mode separately for every message [10].

All of these schemes are built using a bilinear pairing as introduced in Section 2.4.5. A pairing-free KP-ABE scheme was proposed by Yao, Chen and Tian [4] in 2015. Their scheme only uses a single group and no bilinear pairing. Instead of encrypting a group element that encodes a message, their scheme yields a random group element which is then used as a key for a symmetric encryption algorithm [4].

In [19] a cryptanalysis of the scheme in [4] is performed. It is shown that the scheme is not secure, but the authors propose an effective fix and prove its security. They also extend the scheme to allow for key delegation (i.e. a hierarchical KP-ABE scheme) [19].

[20] presents a pairing-free ABE scheme with indirect revocation. It is an adaptation of the schemes in [4], [19], see also [21].

All three of these schemes were attacked by Herranz in [21] (one attack for all three schemes is given, as they are very similar). [21] argues that it is not possible to build secure ABE schemes in the (non-bilinear) discrete-logarithm setting (i.e. on elliptic curves without bilinear pairings). For this reason, the security of pairing-free schemes like [4], [19], [20] remains questionable, even if further improved.

One of the major factors for the performance of the implementation of an ABE scheme is the underlying pairing computation (except for [4] and its derivatives, of course). Not only ABE is based on bilinear pairings, but a large variety of cryptographic schemes, e.g. a three-party Diffie-Hellman Key Exchange [22] or short digital signature schemes [23]).

Therefore, a fast implementation of the bilinear pairing is vital. Comparing different pairing implementations is difficult because the performance greatly depends on the security level, the concrete pairing implemented, the choice of elliptic curves and of course the speed of the hardware and architecture used. Furthermore, many implementations are not portable due to hand-optimized assembly code or the use of architecture-specific instructions.

One of the first notable implementations was the *Pairing-Based Cryptography Library (PBC)*[1] [24]. The efficiency improvements implemented by the PBC library were first described by its author, Ben Lynn, in [24]. This implementation runs sufficiently fast

[1] `https://crypto.stanford.edu/pbc/`

on standard PC hardware, e.g. it takes 20.5ms to compute a pairing on a 224-bit MNT curve on a 2.4GHz Intel Core i5 processor [25].

On the other end of the hardware spectrum stands the assembly-optimized *TinyPBC* library[2]. It takes a minimum of 1.9s to compute a pairing on a 7MHz ATmega128L processor with optimized assembly code [26]. Their choice of elliptic curves, however, only provides a security level of 80 bit (the 224-bit MNT curve from the PBC library is closer to a 128-bit security level [25]).

Scott [27] provides a fast implementation of the 254-bit BN curve (the same as used in `rabe-bn`) in the *MIRACL Core Cryptographic Library*[3]. They also evaluate their library on the same SoC as used in this thesis (nRF52840, 64MHz ARM Cortex M4 CPU) and compute a pairing of the 254-bit BN curve in 439ms [27, Table 4].

Implementations of ABE on standard PC hardware are well-studied [2], [28], [29]; for an overview see [30].

In [25], a pairing-based ABE scheme is evaluated on a standard computer and an ARM-based smartphone (iPhone 4). On the smartphone, only decryption is implemented because encryption is not needed in their scenario. This implementation uses the PBC library and 224-bit MNT curve from [24]. They conclude that for policies with less than 30 leaves, decryption on a smartphone is feasible (taking around 2 to 7 seconds, depending on the scheme) [25].

In [31], a pairing library and ABE scheme is implemented using the NEON instructions, a set of SIMD vector instructions for ARM processors. They evaluate their implementations on several ARM Cortex A9 and A15 processors with clock frequencies between 1GHz and 1.7GHz. The use of NEON improves performance by 20-50%, depending on the chip. Note that the NEON instruction set is not available on our SoC.

In [32], CP- and KP-ABE are evaluated for different security levels on an Intel Atom-based smartphone using a Java implementation. They conclude that ABE on smartphones is not fast enough to be practical. This is subsequently challenged in [33], where a C implementation also using the PBC library from **lynn** is evaluated on another smartphone with a 1.2GHz ARM Cortex A9 CPU. This implementation is significantly faster than the one in [32] at comparable security levels. As such, the authors conclude that ABE is indeed feasible on smartphones.

The authors of [33] shortly thereafter consider the feasibility of ABE on Internet of Things (IoT) devices in [34]. They evaluate the performance of the same library on, among others, a Raspberry Pi Zero (1GHz ARM11 CPU) and conclude that ABE is feasible on these devices, too. However, they note that especially lower security levels

[2] `https://sites.google.com/site/tinypbc/`
[3] `https://github.com/miracl/core`

are suitable and that the penalty for increasing the security level is very high (e.g. increasing the security level from 80 to 128 bits without increasing the encryption time requires reduction of the number of attributes by a factor of 10) [34].

The setting in [35] is much closer to ours: ABE is implemented bare-metal (i.e. without operating system) on a sensor equipped with an STM32L151VCT6 SoC with a maximum clock frequency of 32MHz. They use the pairing library *RELIC Toolkit*[4] and evaluate a C implementation of the CP-ABE scheme in [16]. The author again concludes that ABE encryption on the sensor is feasible if the policy size is rather small and the runtime of several seconds is acceptable [35]. In this case, the encryption time is over 10s already for just six attributes [35].

[36] provides a similar analysis for the slightly faster ESP32 board (240MHz Xtensa LX6 processor). They also test the pairing-free YCT14 scheme [4] and evaluate the energy consumption of ABE operations.

[4] `https://github.com/relic-toolkit/relic`

4 Constructions

4.1 Goyal, Pandey, Sahai and Waters, 2006

This scheme was the first ABE scheme with expressive access policys. Policies are associated with the key (KP-ABE). It was described by Goyal, Pandey, Sahai and Waters [1] in 2006. This scheme will be referred to as GPSW.

Goyal *et. al.* extend the earlier work from Sahai and Waters [15] to allow arbitrary access structures expressed by access trees, not just a "k-out-of-n" attributes. They are the first to use Shamir's Secret Sharing hierarchically in the access tree as described in Section 2.3.3.

The GPSW scheme encrypts a message represented by a point of the bilinear pairing's target group $\mathbb{G}_T$. The main construction follows the small universe approach, but a construction allowing arbitrary attributes is also given. The construction described here ist the small universe construction.

The construction given here is exactly as implemented; it differs from the original construction in the use of an asymmetric pairing ($e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$) instead of a symmetric pairing ($e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$).
In the GPSW construction, the pairing is only evaluated during decryption phase for leaf nodes (see below). There, the curve point on one side comes from the ciphertext, and the point on the other side from the key. Originally, a symmetric pairing is used, so their order can be swapped freely. As we want to improve the speed of the encryption, we use the shorter elements of $\mathbb{G}_1$ for everything that has to do with the ciphertext, because that way only elements of $\mathbb{G}_1$ need to manipulated during encryption.

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be bilinear groups of prime order q. Let P be a generator of $\mathbb{G}_1$ and Q be a generator of $\mathbb{G}_2$. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ be a bilinear map. Note that $\mathbb{G}_1$ and $\mathbb{G}_2$ are written additively, but $\mathbb{G}_T$ is written using multiplicative notation.

Setup [1]. The attribute universe is defined as $\mathrm{U} = \{1, 2, \ldots, n\}$ and is fixed. For every attribute $i \in U$, choose uniformly at random a secret number $t_i \in \mathbb{Z}_q$. Then the public key of attribute i is $T_i = t_1 \cdot P$. Also, choose uniformly at random the master private key $y \in \mathbb{Z}_p$, from which the master public key $Y = e(P, Q)^y$ is derived.

Publish $Params = (Y, T_1, \ldots, T_n)$ as the public parameters, privately save $MK = (y, t_1, \ldots, t_n)$ as the master key.

KeyGen(Γ, *MK*) [1]. Input: access tree Γ and master key *MK*.

For each node u in the access tree Γ, recursively define polynomials $q_u(x)$ with degree $(d_u - 1)$, starting from the root.

For the root r, set $q_r(0) = s$ and randomly choose $d_r - 1$ other points to determine the polynomial $q_r(x)$. Then, for any other node u, including leaf nodes, set $q_u(0) = q_{\text{parent}(x)}(\text{index}(x))$ and choose $d_u - 1$ other points at random to define the polynomial. For all leaf nodes u, create a secret share $D_u = q_x(0) \cdot t_i^{-1} \cdot Q$ where $i = \text{att}(x)$.

The set of these secret shares is the decryption key $D = \{D_u | u \text{ leaf node of } \Gamma\}$.

Encrypt(M, ω, *Params*) [1]. Input: Message $M \in \mathbb{G}_T$, set of attributes ω and public parameters *Params*.

Choose $s \in \mathbb{Z}_q$ at random and compute $E' = M + s \cdot Y$. For each attribute $i \in \omega$ compute $E_i = s \cdot T_i$.

Return the ciphertext as $E = (\omega, E', \{E_i | i \in \omega\})$

Decrypt(E, D) [1]. Input: Ciphertext E and decryption key D.

First, define a recursive procedure $\text{DecryptNode}(E, D, u)$ which takes as inputs a ciphertext $E = (\omega, E', \{E_i | i \in \omega\})$, the decryption key D and a node x of the access tree associated with the decryption key. It outputs either en element of $\mathbb{G}_T$ or $\perp$.

If u is a leaf node, then $i = \text{att}(x)$ and

$$\text{DecryptNode}(E, D, u) = \begin{cases} e(E_i, D_u) = e(s \cdot t_i \cdot P, q_u(0) \cdot t_i^{-1} \cdot Q) = e(P, Q)^{s \cdot q_u(0)} & i \in \omega \\ \perp & i \notin \omega \end{cases} \tag{4.1}$$

If u is not a leaf node, instead call $\text{DecryptNode}(E, D, v)$ for all child nodes v of u and store the result in F_v. Let S_u be an arbitrary d_u-sized subset of child nodes v with $F_v \neq \perp$. If no such set exists, the node was not satisfied. In this case return $\perp$. Then compute with $i = \text{index}(z)$ and $S'_u = \{\text{index}(z) | z \in S_u\}$.

$$\begin{aligned} F_u &= \prod_{z \in S_u} F_z^{\Delta_{i, S'_u}(0)} \\ &= \prod_{z \in S_u} (e(P, Q)^{s \cdot q_z(0)})^{\Delta_{i, S'_u}(0)} \\ &= \prod_{z \in S_u} (e(P, Q)^{s \cdot q_{\text{parent}(z)}(\text{index}(z))})^{\Delta_{i, S'_u}(0)} \\ &= \prod_{z \in S_u} e(P, Q)^{s \cdot q_u(i) \cdot \Delta_{i, S'_u}(0)} \\ &\overset{(*)}{=} e(P, Q)^{s \cdot q_u(0)} \end{aligned} \tag{4.2}$$

The equality $(*)$ holds because, in the exponent, the product becomes a sum: $\sum_{i \in S'_u} s \cdot q_u(i) \cdot \Delta_{i,S'_u}(0)$ is exactly the lagrange interpolation of $s \cdot q_u(0)$.

Let the root of the access tree be r, then the decryption algorithm simply calls $\text{DecryptNode}(E, D, r) = e(P, Q)^{s \cdot y} = Y^s$, if the ciphertexts's attributes satisfy the access tree. If they don't, then $\text{DecryptNode}(E, D, r) = \perp$.

To retrieve the message from $E' = M \cdot Y^s$, simply calculate and return $M' = E' \cdot (Y^s)^{-1}$.

Of course, it is rather difficult (and slow) to encode the full plaintext as a group element of $\mathbb{G}_T$. Therefore, it is advisable to simply generate a random $K \in \mathbb{G}_T$ and encrypt the plaintext using a secure symmetric cipher with key $k = \text{KDF}(K)$, where KDF is a key derivation function. Then encrypt the point K using the GPSW scheme and attach its ciphertext to the symmetric ciphertext. Correct decryption of $K \in \mathbb{G}_T$ then allows a receiver to decrypt the actual payload.

4.2 Yao, Chen and Tian 2015

This scheme was described by Yao, Chen and Tian [4] in 2015. In 2019, Tan, Yeow and Hwang [19] proposed an enhancement, fixing a flaw in the scheme and extending it to be a hierarchical KP-ABE scheme.

Yao, Chen and Tian's ABE scheme (hereafter written just YCT) is a KP-ABE scheme that does not use any bilinear pairing operations. Instead, the only operation performed on Elliptic Curves are point-scalar multiplication [4]. This makes it especially useful for our resource-constrained context, as bilinear pairings are significantly more costly in terms of computation and memory.

As opposed to other ABE schemes based on pairings, YCT uses a hybrid approach similar to Elliptic Curve Integrated Encryption Standard (ECIES): The actual encryption of the plaintext is done by a symmetric cipher, for which the key is derived from a curve point determined by the YCT scheme [4]. If a key's access structure is satisfied by a certain ciphertext, this curve point and thus the symmetric encryption key can be reconstructed, allowing for decryption. [4]

The four algorithms of an ABE scheme are defined as follows:

Setup [4]. The attribute universe is defined as $\text{U} = \{1, 2, \ldots, n\}$ and is fixed.

For every attribute $i \in U$, choose uniformly at random a secret number $s_i \in \mathbb{Z}_q^*$. Then the public key of attribute i is $P_i = s_i \cdot G$ (i.e. a curve point).

Also, choose uniformly at random the master private key $s \in \mathbb{Z}_q^*$, from which the master public key $PK = s \cdot G$ is derived.

Publish $Params = (PK, P_1, \ldots, P_n)$ as the public parameters, privately save $MK = (s, s_1, \ldots, s_n)$ as the private master key.

KeyGen(Γ, MK) [4]. Input: access trees Γ and master key MK.

For each node u in the Access Tree Γ, recursively define polynomials $q_u(x)$ with degree $(d_u - 1)$, starting from the root.

For the root r, set $q_r(0) = s$ and randomly choose $(d_r - 1)$ other points to determine the polynomial $q_r(x)$. Then, for any other node u (including leafs), set $q_u(0) = q_{\text{parent}(u)}(\text{index(u)})$ and choose $(d_u - 1)$ other points for q_u, similar to above.

Whenever u is a leaf node, use $q_u(x)$ to define a secret share $D_u = \frac{q_u(0)}{s_i}$; where $i = \text{attr}(u)$, s_i the randomly chosen secret number from *Setup* and s_i^{-1} the inverse of s_i in $\mathbb{Z}_q^*$.

Return the generated key as $D = \{D_u | u \text{ leaf node of } \Gamma\}$.

Encrypt(m, ω, Params) [4]. Input: Message m, set of attributes ω and public parameters $Params$.

Randomly choose $k \in \mathbb{Z}_q^*$ and compute $C' = k \cdot PK$. If $C' = \mathcal{O}$, repeat until $C' \neq \mathcal{O}$. $C' = (k_x, k_y)$ are the coordinates of the point C'. k_x is used as the encryption key and k_y as the integrity key.

Then compute $C_i = k \cdot P_i$ for all attributes $i \in \omega$.

Encrypt the actual message as $c = \text{Enc}(m, k_x)$, generate a Message Authentication Code $\text{mac}_m = \text{HMAC}(m, k_y)$.

Return the ciphertext $CM = (\omega, c, \text{mac}_m, \{C_i | i \in \omega\})$

Decrypt(CM, D, Params) [4]. Input: Ciphertext CM, decryption key D and public parameters $Params$.

Decryption is split into two phases: Reconstructing the curve point C' to get the encryption and integrity keys, and actual decryption of the ciphertext.

First, define a recursive decryption procedure for a node u: $\text{DecryptNode}(CM, D, u)$. For leaf nodes with $i = \text{attr}(u)$:

$$\text{DecryptNode}(CM, D, u) = \begin{cases} D_u \cdot C_i \overset{(*)}{=} q_u(0) \cdot k \cdot G & i \in \omega \\ \perp & i \notin \omega \end{cases}$$

Where the equality $(*)$ holds because s_i and s_i^{-1} cancel out:

$$D_u \cdot C_i = q_u(0) \cdot s_i^{-1} \cdot k \cdot P_i = q_u(0) \cdot s_i^{-1} \cdot k \cdot s_i \cdot G = q_u(0) \cdot k \cdot G$$

For an internal node u, call DecryptNode(CM, D, v) for each of its childen v. If for less than d_u of the child nodes DecryptNode$(CM, D, v) \neq \perp$, return DecryptNode$(CM, D,) = \perp$. Then let ω_u be an arbitrary subset of d_u child nodes of u, where for all $v \in \omega_u$, DecryptNode$(CM, D, v) \neq \perp$. Then DecryptNode(CM, D, u) is defined as follows, where $i = \text{index}(v)$, $\omega'_u = \{\text{index}(v) | v \in \omega_u\}$.

$$\begin{aligned}
&\text{DecryptNode}(CM, D, u) \\
&= \sum_{v \in \omega_u} \Delta_{\omega'_u, i}(0) \cdot \text{DecryptNode}(CM, D, v) \\
&= \sum_{v \in \omega_u} \Delta_{\omega'_u, i}(0) \cdot q_v(0) \cdot k \cdot G \\
&= \sum_{v \in \omega_u} \Delta_{\omega'_u, i}(0) \cdot q_{\text{parent}(v)}(\text{index}(v)) \cdot k \cdot G \\
&= \sum_{v \in \omega_u} \Delta_{\omega'_u, i}(0) \cdot q_u(i) \cdot k \cdot G \\
&\overset{(*)}{=} q_u(0) \cdot k \cdot G
\end{aligned}$$

The equality $(*)$ holds because $\sum_{v \in \omega'_u} \Delta_{\omega'_u, i}(0) \cdot q_u(i) = q_u(0)$ is exactly the lagrange interpolation polynomial $q_u(x)$ at $x = 0$ with respect to the points $\{(index(v), q_v(0)) | v \in \omega_u\}$.

This means for the root r of the access tree Γ, we have

$$\text{DecryptNode}(CM, D, r) = q_r(0) \cdot k \cdot G = s \cdot k \cdot G = (k'_x, k'_y)$$

With k'_x the decryption key for m and k'_y the integrity key. Therefore now decrypt $m' = \text{Dec}(c, k'_x)$.

Now check if $\text{HMAC}(m', k'_y) = \text{mac}_m$. If yes, the ciphertext has been correctly decrypted and was not tampered with. Return m', otherwise return $\perp$.

5 Implementation

The implementation of ABE on the SoC in Rust posed three main challenges:

- The availability of pairing libraries in Rust is very limited.
- Due to the lack of an operating system, there is no standard library, no dynamic memory allocation and no easy access to a CSPRNG.
- The low speed of computation compared to PCs or even other IoT platforms (e.g. Raspberry Pi).

5.1 Barreto-Naehrig curves and the `rabe-bn` library

Barreto and Naehrig [37] proposed a family of pairing-friendly elliptic curves (usually called *BN curves*). A Rust-only implementation of concrete BN curves and a pairing is provided in the library `rabe-bn`[1], a derivative of the `bn` library by Zcash [38].

This implementation unfortunately relies on the standard library (mostly through the use of dynamically sized vectors, i.e. `std::vec::Vec`) and is thus not suited for bare-metal applications.

Therefore, it was rewritten to introduce a feature `std` which controls the inclusion of the standard library and is enabled by default. If this feature is disabled, stack-allocated collections of fixed size from the `heapless`[2] crate are used instead. This modification was fairly straight-forward, as in most occurrences of `std::vec::Vec` the exact maximum size was fairly obvious.

Some further modifications were necessary to implement the `core::fmt::Display` trait for the `Gt` struct in a bare-metal compatible manner. The implementation of this trait was used in conjunction with SHA-3 as a key derivation function to create an AES key from curve points.

With these relatively minor modifications, the `rabe-bn` library runs on the SoC.

[1] `https://github.com/georgbramm/rabe-bn`
[2] `https://crates.io/crates/heapless`

```
#[derive(Debug)]
pub struct GpswAbePublic<'attr, 'own> {
    g1: G1,
    g2: G2,
    atts: &'own FnvIndexMap<&'attr str, G2, S>,
    pk: Gt,
}
```

6 Challenges encountered during the implementation

6.1 Rust specialties

The borrow checkaaa...

- Nightly Rust
  - Features and dev-dependencies: enabling the stdlib in the tests, but **not** in the final binary is non-trivial

6.2 Lack of Operating System

This means lack of

- allocator and standard library (replaced by `core`, but much less powerful)
  - any dynamically allocated data structures
  - No Vectors and HashMaps Vectors and HashMaps
  - no easy implementation of (access-) trees using recursive enums (as these would become infinitely large when not using indirections)
  - most dependencies depend on `std` in some way, so a lot more work to make all those independent
  - Solution: `heapless` crate and linear representation of access trees (TODO make bounds on size of data types configurable)
- Random Number Generation
  - Problem: need cryptographically secure randomness, but have no OS randomness pool
  - can't just use `/dev/urandom` to get randomness (there is no such thing as a file anyway)

  - standard implementations of `random` resp. `getrandom` crates don't work (rely on stdlib)
  - need own randomness source
  - nrf50 series provides hardware RNG, but we need Rust to be able to interface with this
  - probably need own implementation of `getrandom` crate for Zephyr OS or bare-metal nrf50

- Unit testing abilities

6.3 Performance Limitations

That is, CPU speed (64MHz) and RAM size (..KiB?).

- probably too slow for computing actual pairings
- Solution 1: Scheme without pairings (Yao et al 2015)
- Solution 2: Still do pairings, but hyper-optimize (see TinyPBC on AVR)

List of Figures

List of Tables

Glossary

access policy A policy that defines what combination of attributes shall be required to access data. Formalized by an access structure and usually realized by an access tree, see Section 2.2.4 plural. 3, 5–7, 23, 34, 35

access structure defines the attribute combinations that are required and sufficient to decrypt a ciphertext. See Section 2.2.4 and Section 2.2.5. 6–9, 19, 20, 25

access tree construction to realize (monotone) access structures. See Section 2.2.5. 9, 19, 20, 23–26

asymmetric encryption scheme type of encryption scheme where different keys are used for encryption and decryption. The encryption key may be made public, while the decryption key is kept private.. 2, 4

attribute Property of an actor or object, e.g. „is student" or "has blonde hair". 24, 34, 35

attribute universe set of possible attributes. 4

ciphertext-policy ABE Variant of ABE where the key is associated with an access policy and the ciphertext is associated with a set of attributes. 3, 6, 21, 36

diffie-hellman key exchange key agreement protocol that allows two parties A and B to agree on a shared secret value over an insecure channel. A and B can derive the same secret value, while any adversaries cannot (as long as they only passively eavesdrop, but not modify, the information exchanged between A and B). 20

digital signature scheme asymmetric cryptographic scheme/protocol for ensuring message authenticity and integrity. 20

elliptic curve Algebraic structure that forms a group, see Section 2.4. 14, 16

generic group model formal security model assuming that the attacker only has oracle access to the group operation (provides less formal security than the standard model). 19

group A set together with a binary operation that satisfies the group axioms, see Section 2.4.1. 34

identity-based encryption type of encryption where data is encrypted using a unique identity (e.g. an email address or phone number), and only the participant holding the secret key corresponding to that identity is able to decrypt the ciphertext.. 19

key derivation function function that derives a suitable cryptographic key from some other data, that may be too long or not in the right format to serve as a key. Usually, hash functions are used as KDF. 25, 28

key generation center Trusted central authority that sets up an ABE scheme and generates keys for users of an ABE scheme . 4, 6, 7, 36

key-policy ABE Variant of Attribute-Based Encryption (ABE) where the ciphertext is associated with an access policy and the key is associated with a set of attributes. 3

large universe type of ABE construction where any string can be used as an attribute. 4

linear secret sharing scheme secret sharing scheme in which the share generation can be described by a matrix. See [3]. 9, 19, 36

monotone span program linear algebraic computation model that is equivalent to LSSS. See Section 2.2.6. 9, 36

security level measure of the strength of a cryptographic scheme, usually given in bits. A security level of n bits means that the most efficient attack needs to perform at least around 2^n operations to break the scheme. Note that this does not directly translate to the size of the used parameters: to guarantee a security level of n bits, usually the the size of the field underlying our elliptic curve (i.e. the number of bits of its modulus) needs to be *at least* $2n$, sometimes much larger. 20

small universe type of ABE construction where the possible attributes have to be fixed when the system is instantiated. 4, 23

standard model formal security model that imposes no restrictions on the attacker, except for the limit on the complexity of their computations. 19, 34

symmetric encryption scheme type of encryption scheme where the same key is used for encryption and decryption. This means that the key has to be shared among all parties via some secure channel (e.g. a personal meeting).. 2

Acronyms

ABE Attribute-Based Encryption. 2–4, 6, 7, 19–22, 28, 34–36

ABE scheme Attribute-Based Encryption scheme. 4, 9, 19–21, 23, 32, 35

CP-ABE Ciphertext-Policy ABE. 4, 6, 7, 12, 19, 22, 32, *Glossary:* ciphertext-policy ABE

CSPRNG cryptographically secure pseudorandom number generator. 28

IoT Internet of Things. 21, 28

KGC Key Generation Center. 4–7, 13, *Glossary:* Key Generation Center

KP-ABE Key-Policy ABE. 4–7, 12, 19–21, 23, 32, *Glossary:* key-policy ABE

LSSS linear secret sharing scheme. 9, 19, 35, *Glossary:* linear secret sharing scheme

MSP monotone span program. 9, 10, *Glossary:* monotone span program

SHA-3 Secure Hash Algorithm 3. 28

SIMD single instruction, multiple data. Vectorized CPU instruction that processes several pieces of data at once. 21

Bibliography

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," en, in *Proceedings of the 13th ACM conference on Computer and communications security - CCS '06*, Alexandria, Virginia, USA: ACM Press, 2006, pp. 89–98, ISBN: 978-1-59593-518-2. DOI: 10.1145/1180405.1180418. [Online]. Available: http://dl.acm.org/citation.cfm?doid=1180405.1180418 (visited on Nov. 28, 2020).

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," en, in *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA: IEEE, May 2007, pp. 321–334, ISBN: 978-0-7695-2848-9. DOI: 10.1109/SP.2007.11. [Online]. Available: http://ieeexplore.ieee.org/document/4223236/ (visited on Dec. 2, 2020).

[3] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," en, Ph.D. thesis, Technion - Israel Institute of Technology, Haifa, 1996. [Online]. Available: https://www.iacr.org/phds/index.php?p=detail&entry=548 (visited on Feb. 8, 2021).

[4] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," en, *Future Generation Computer Systems*, vol. 49, pp. 104–112, Aug. 2015, ISSN: 0167-739X. DOI: 10.1016/j.future.2014.10.010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X14002039 (visited on Dec. 3, 2020).

[5] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," en, in *Advances in Cryptology – EUROCRYPT 2011*, vol. 6632, Series Title: Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 568–588, ISBN: 978-3-642-20464-7 978-3-642-20465-4. DOI: 10.1007/978-3-642-20465-4_31. [Online]. Available: http://link.springer.com/10.1007/978-3-642-20465-4_31 (visited on Jan. 25, 2021).

[6] Z. Liu, Z. Cao, and D. S. Wong, "Efficient Generation of Linear Secret Sharing Scheme Matrices from Threshold Access Trees," en, p. 28, 2010.

[7] S. Agrawal and M. Chase, *FAME: Fast Attribute-based Message Encryption*. 2017, Published: Cryptology ePrint Archive, Report 2017/807.

[8] A. Shamir, "How to share a secret," en, *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, ISSN: 0001-0782, 1557-7317. DOI: 10.1145/359168.359176. [Online]. Available: https://dl.acm.org/doi/10.1145/359168.359176 (visited on Jan. 7, 2021).

[9] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," in *Proceedings of the 15th ACM Conference on Computer and Communications Security*, ser. CCS '08, event-place: Alexandria, Virginia, USA, New York, NY, USA: Association for Computing Machinery, 2008, pp. 417–426, ISBN: 978-1-59593-810-7. DOI: 10.1145/1455770.1455823. [Online]. Available: https://doi.org/10.1145/1455770.1455823.

[10] N. Attrapadung and H. Imai, "Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes," in *Cryptography and Coding*, M. G. Parker, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 278–300, ISBN: 978-3-642-10868-6.

[11] J. Katz and Y. Lindell, *Introduction to modern cryptography*, second edition, ser. Chapman Hall, CRC cryptography and network security. Boca Raton ; London ; New York: CRC Press, 2015, ISBN: 978-1-4665-7026-9 1-4665-7026-1.

[12] L. C. Washington, *Elliptic curves: number theory and cryptography*, en, 2nd ed, ser. Discrete mathematics and its applications. Boca Raton, FL: Chapman & Hall/CRC, 2008, OCLC: ocn192045762, ISBN: 978-1-4200-7146-7.

[13] M. S. Kiraz and O. Uzunkol, "Still Wrong Use of Pairings in Cryptography," en, *arXiv:1603.02826 [cs]*, Nov. 2016, arXiv: 1603.02826. [Online]. Available: http://arxiv.org/abs/1603.02826 (visited on Dec. 2, 2020).

[14] I. Blake, G. Seroussi, and N. Smart, Eds., *Advances in elliptic curve cryptography*, ser. Lecture note series. Cambridge [u.a.]: Cambridge University Press, 2005, ISBN: 0-521-60415-X.

[15] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in *Advances in Cryptology – EUROCRYPT 2005*, R. Cramer, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 457–473, ISBN: 978-3-540-32055-5.

[16] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," in *Public Key Cryptography – PKC 2011*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 53–70, ISBN: 978-3-642-19379-8.

[17] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," en, in *Proceedings of the 14th ACM conference on Computer and communications security - CCS '07*, Alexandria, Virginia, USA: ACM Press, 2007, p. 195, ISBN: 978-1-59593-703-2. DOI: 10.1145/1315245.1315270. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1315245.1315270 (visited on Feb. 8, 2021).

[18] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with Very Small Private Keys," Tech. Rep. 2008/309, 2008, Published: Cryptology ePrint Archive, Report 2008/309. [Online]. Available: https://eprint.iacr.org/2008/309.

[19] S.-Y. Tan, K.-W. Yeow, and S. O. Hwang, "Enhancement of a Lightweight Attribute-Based Encryption Scheme for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6384–6395, Aug. 2019, ISSN: 2327-4662, 2372-2541. DOI: 10.1109/JIOT.2019.2900631. [Online]. Available: https://ieeexplore.ieee.org/document/8651482/ (visited on Dec. 3, 2020).

[20] K. Sowjanya, M. Dasgupta, S. Ray, and M. S. Obaidat, "An Efficient Elliptic Curve Cryptography-Based Without Pairing KPABE for Internet of Things," en, *IEEE Systems Journal*, vol. 14, no. 2, pp. 2154–2163, Jun. 2020, ISSN: 1932-8184, 1937-9234, 2373-7816. DOI: 10.1109/JSYST.2019.2944240. [Online]. Available: https://ieeexplore.ieee.org/document/8869901/ (visited on Jan. 12, 2021).

[21] J. Herranz, "Attacking Pairing-Free Attribute-Based Encryption Schemes," *IEEE Access*, vol. 8, pp. 222 226–222 232, 2020. DOI: 10.1109/ACCESS.2020.3044143.

[22] A. Joux, "A One Round Protocol for Tripartite Diffie–Hellman," in *Algorithmic Number Theory*, W. Bosma, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 385–393, ISBN: 978-3-540-44994-2.

[23] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," in *Advances in Cryptology — ASIACRYPT 2001*, C. Boyd, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 514–532, ISBN: 978-3-540-45682-7.

[24] B. Lynn, "ON THE IMPLEMENTATION OF PAIRING-BASED CRYPTOSYSTEMS," en, Dissertation, Stanford University, Stanford, California, 2007. [Online]. Available: https://crypto.stanford.edu/pbc/thesis.pdf.

[25] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, and A. D. Rubin, "Self-Protecting Electronic Medical Records Using Attribute-Based Encryption," 2010, Published: Cryptology ePrint Archive, Report 2010/565. [Online]. Available: https://eprint.iacr.org/2010/565.

[26] L. B. Oliveira, D. F. Aranha, C. P. Gouvêa, M. Scott, D. F. Câmara, J. López, and R. Dahab, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Special Issue of Computer Communications on Information and Future Communication Security*, vol. 34, no. 3, pp. 485–493, Mar. 2011, ISSN: 0140-3664. DOI: 10.1016/j.comcom.2010.05.013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366410002483.

[27] M. Scott, "On the Deployment of curve based cryptography for the Internet of Things," 2020, Published: Cryptology ePrint Archive, Report 2020/514.

[28] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: A framework for rapidly prototyping cryptosystems," *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 111–128, 2013, Publisher: Springer-Verlag, ISSN: 2190-8508. DOI: 10.1007/s13389-013-0057-3. [Online]. Available: http://dx.doi.org/10.1007/s13389-013-0057-3.

[29] M. Green and J. A. Akinyele, *The Functional Encryption Library (libfenc)*. [Online]. Available: https://code.google.com/archive/p/libfenc/.

[30] S. Zickau, D. Thatmann, A. Butyrtschik, I. Denisow, and A. Küpper, "Applied Attribute-based Encryption Schemes," en, Paris, 2016, p. 8.

[31] A. H. Sánchez and F. Rodríguez-Henríquez, "NEON Implementation of an Attribute-Based Encryption Scheme," in *ACNS*, 2013.

[32] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 725–730. DOI: 10.1109/ICC.2014.6883405.

[33] M. Ambrosin, M. Conti, and T. Dargahi, "On the Feasibility of Attribute-Based Encryption on Smartphone Devices," in *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*, ser. IoT-Sys '15, event-place: Florence, Italy, New York, NY, USA: Association for Computing Machinery, 2015, pp. 49–54, ISBN: 978-1-4503-3502-7. DOI: 10.1145/2753476.2753482. [Online]. Available: https://doi.org/10.1145/2753476.2753482.

[34] M. Ambrosin, A. Anzanpour, M. Conti, T. Dargahi, S. R. Moosavi, A. M. Rahmani, and P. Liljeberg, "On the Feasibility of Attribute-Based Encryption on Internet of Things Devices," en, p. 13, 2016.

[35] J. Borgh, *Attribute-Based Encryption in Systems with Resource Constrained Devices in an Information Centric Networking Context*, 2016.

[36] B. Girgenti, P. Perazzo, C. Vallati, F. Righetti, G. Dini, and G. Anastasi, "On the Feasibility of Attribute-Based Encryption on Constrained IoT Devices for Smart Systems," *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*, pp. 225–232, 2019.

[37] P. S. L. M. Barreto and M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order," in *Selected Areas in Cryptography*, B. Preneel and S. Tavares, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 319–331, ISBN: 978-3-540-33109-4.

[38] S. Bowe, *Bn - Pairing cryptography in Rust*, 2016. [Online]. Available: `https://electriccoin.co/blog/pairing-cryptography-in-rust/` (visited on Mar. 11, 2021).