A New Biometric Identity Based Encryption Scheme

Neyire Deniz Sarier

Bonn-Aachen International Center for Information Technology
Computer Security Group
Dahlmannstr. 2, D-53113 Bonn Germany
denizsarier@yahoo.com

Abstract

In this paper, we present a new and efficient biometric identity based encryption scheme (BIO-IBE) using the Sakai-Kasahara Key Construction and prove its security in the random oracle model based on the well-exploited k-DBDH computational problem. Our new scheme achieves better efficiency in terms of the key generation and decryption algorithms compared to the existing fuzzy IBE schemes. The main difference of the new BIO-IBE scheme is the structure of the key generation algorithm, where a unique biometric identity string ID obtained from the biometric attributes is used instead of picking a different polynomial for each user as in other fuzzy IBE schemes.

Keywords: Biometrics, fuzzy IBE, fuzzy extraction.

1. Introduction

Recently, Sahai and Waters proposed a new Identity Based Encryption (IBE) system called fuzzy IBE that uses biometric attributes as the identity instead of an arbitrary string like an email address. In fuzzy IBE, the private key components are generated by combining the values of a unique polynomial on each attribute with the master secret key. However, due to the noisy nature of biometrics, fuzzy IBE allows for error tolerance in the decryption stage, where a ciphertext encrypted with the biometrics would be decrypted by the receiver using the private key corresponding to the identity w', provided that w and w' are within a certain distance of each other. Besides, the biometric attributes are used as public information, hence the compromise of the biometrics does not affect the security of the system.

1.1. Related Work

The first fuzzy IBE scheme is described by Sahai and Waters in [11] and the security is reduced to the MBDH problem in the standard model, where the size of the public parameters is linear in the number of attributes of the system or the number of attributes of a user. Piretti et al [10] achieved a more efficient fuzzy IBE scheme with short public parameter size by using the random oracle model (ROM). Baek et al [1] described two new fuzzy IBE schemes with an efficient key generation algorithm and proved the security in the random oracle model based on the DBDH assumption. Besides, Burnett et al [4] described a biometric identity based signature scheme, where they used the biometric information as the identity and construct the public key of the user using a fuzzy extractor [8], which is then used in the modified SOK-IBS scheme [2].

1.2. Our Contribution

In this paper, we present a new biometric identity based encryption scheme using the Sakai Kasahara Key Construction [6] and achieve better efficiency compared to the existing fuzzy IBE schemes in terms of the key generation and decryption algorithms. First, we have a structurally simpler key generation algorithm compared to [10, 1] since we use an ordinary one-way hash function instead of a MapToPoint hash function and we reduce the number of exponentiations in the group G from 3n as in [10] (and from 2n as in [11]) to n. Also, the decryption algorithm requires d bilinear pairing computations and d exponentiations, whereas the existing schemes require d + 1 bilinear pairing computations and 2d exponentiations. The security of our new scheme reduces to the well exploited k-DBDH computational problem in the random oracle model. The main difference of our biometric IBE scheme is the structure of the key generation algorithm, where a unique biometric identity string ID obtained from the biometric attributes is used instead of picking a different polynomial for each user and computing the private key components for each attribute using this polynomial, the master key and the attributes. Thus, our scheme is constructed using a different approach compared to the existing fuzzy IBE schemes.
2. Definitions and Building Blocks

In order to introduce the new biometric IBE scheme, at first, we review the definitions and required computational primitives. Given a set $S$, $x \sim S$ defines the assignment of a uniformly distributed random element from the set $S$ to the variable $x$. A function $\epsilon(k)$ is defined as negligible if for any constant $c$, there exists $k_0 \in N$ with $k > k_0$ such that $\epsilon < (1/k)^c$. Finally, we define the Lagrange coefficient $\Delta_{\mu_i,S}$ for $\mu_i \in \mathbb{Z}_p$ and a set $S$ of elements in $\mathbb{Z}_p$ as

$$\Delta_{\mu_i,S}(x) = \prod_{\mu_j \in S, \mu_j \neq \mu_i} \frac{x - \mu_j}{\mu_j - \mu_i}$$

Definition 2.1. Bilinear Pairing

Let $\mathbb{G}$ and $\mathbb{F}$ be multiplicative groups of prime order $p$ and let $g$ be a generator of $\mathbb{G}$. $\mathbb{Z}_p$ denotes $\mathbb{Z}_p \setminus \{0\}$ and $\mathbb{G}^*$ denotes $\mathbb{G} \setminus \{1\}$, where $\{0\}$ and $\{1\}$ are the identity elements of $\mathbb{Z}_p$ and $\mathbb{G}$, respectively. A bilinear pairing is denoted by $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{F}$ if the following two conditions hold.

1. $\forall a, b \in \mathbb{Z}_p$, we have $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$
2. $\hat{e}(g, g) \neq 1$, namely the pairing is non-degenerate.

The security of our scheme is reduced to the well-exploited complexity assumption ($k$-BDHI) [6], which is stated as follows.

Definition 2.2. k-Bilinear Diffie-Hellman Inverse ($k$-BDHI)

For an integer $k$, and $x \in \mathbb{Z}_p^*$, $g \in \mathbb{G}^*$, $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{F}$, given $(g, g^x, g^{x^2}, ..., g^{x^k})$, computing $\hat{e}(g, g)^{1/x}$ is hard.

2.1. Fuzzy Identity Based Encryption

In [1], the generic fuzzy IBE scheme is defined as follows.

- **Setup()**: Given a security parameter $k_0$, the Private Key Generator (PKG) generates the master secret key $ms$ and the public parameters of the system.

- **Key Generation**: Given a user’s identity and $ms$, the PKG returns the corresponding private key $D_{1D}$.

- **Encrypt**: A probabilistic algorithm that takes as input an identity $w \in U$, public parameters and a message $m \in M$ and outputs the ciphertext $c \in C$. Here, $M$, $C$ and $U$ denote the message space, the ciphertext space and the universe of attributes.

- **Decrypt**: A deterministic algorithm that given the private key $D_{1D}$ and a ciphertext encrypted with $w'$ such that $|w \cap w'| \geq d$, returns either the underlying message $m$ or a reject message. Here $d$ is the error tolerance parameter of the scheme.

In our new biometric IBE scheme, the identity is equal to the biometric information of the user, from which the key generation algorithm obtains the biometric features (or attributes) $w$ and a unique biometric identity string $ID$. The details of this extraction process is presented in section 2.3.

2.2. Security Model

In [11], the Selective-ID model of security for fuzzy IBE (IND-FSID-CPA) is defined using a game between a challenger and an adversary as follows.

- **Phase 1**: The adversary declares the challenge identity $w^* = (\mu_1^*, ..., \mu_n^*)$.

- **Phase 2**: The challenger runs the Setup algorithm and returns to the adversary the system parameters.

- **Phase 3**: The adversary issues private key queries for any identity $w'$ such that $|w' \cap w^*| < d$.

- **Phase 4**: The adversary sends two equal length messages $m_0$ and $m_1$. The challenger returns the ciphertext that is encrypted using the identity $w^*$ and the message $m_\beta$, where $\beta \in \{0, 1\}$.

- **Phase 5**: Phase 3 is repeated.

- **Phase 6**: The adversary outputs a guess $\beta'$ for $\beta$.

The advantage of the adversary $A$ is defined as

$$Adv_A^{IND-FSID-CPA} = |Pr[\beta' = \beta] - \frac{1}{2}|$$

For our biometric IBE scheme we give the security proof based on the notion of IND-FSID-CPA (Indistinguishability against Fuzzy Selective Identity, Chosen Plaintext Attack), but our scheme can easily be modified using the generic construction REACT [9] to be secure against CCA (Chosen Ciphertext Attack).

2.3. Biometric Fuzzy Extraction

Any biometric based encryption or signature scheme requires the biometric measurement of the receiver or the signer, respectively. Basically, the framework for biometric encryption is (1) extracting features; (2) quantization and coding per feature and concatenating the output codes; (3) applying error correction coding (ECC) and hashing [5]. After capturing the biometric information of the user through a reading device, feature extraction is applied to obtain the feature vector (or the attributes) of the biometrics. In [11, 1], each attribute is associated with a unique integer $\mu_i \in \mathbb{Z}_p$, using a hash function and used as the identity $w = (\mu_1, ..., \mu_n)$ in the fuzzy IBE scheme. Here, $n$ denotes the size of the attributes of each user. Since some of the
attributes could be common in some users, a unique polynomial is selected for each user and included in the key generation algorithm to bind the private key to the user. This way, different users cannot collude in order to decrypt a ciphertext that should be only decrypted by the real receiver.

In our biometric IBE scheme, we use the biometric template \( b \) of the user, which is obtained by concatenating the extracted features, in order to bind the private key to the user’s identity and thus avoid collusion attacks. Instead of choosing a unique polynomial for each user, we use a fuzzy extractor to obtain a unique string \( ID \) via error correction codes from the biometric template \( b \) of the user in such a way that an error tolerance \( t \) is allowed. In other words, we will obtain the same string \( ID \) even if the fuzzy extractor is applied on a different \( b' \) such that \( \text{dis}(b, b') < t \). Here, \( \text{dis}(\cdot) \) is the distance metric used to measure the variation in the biometric reading and \( t \) is the error tolerance parameter.

Formally, an \((\mathcal{M}, l, t)\) fuzzy extractor is defined as follows.

**Definition 2.3.** Let \( \mathcal{M} = \{0, 1\}^v \) be a finite dimensional metric space with a distance function \( \text{dis} : \mathcal{M} \times \mathcal{M} \rightarrow \mathbb{Z}^+ \). Here, \( b \in \mathcal{M} \) and \( \text{dis} \) measures the distance between \( b \) and \( b' \), where \( b, b' \in \mathcal{M} \). An \((\mathcal{M}, l, t)\) fuzzy extractor consists of two functions \text{Gen} and \text{Rep}.

- **Gen:** A probabilistic generation procedure that takes as input \( b \in \mathcal{M} \) and outputs an identity string \( ID \in \{0, 1\}^l \) and a public parameter \( \text{PAR} \), that is used by the \text{Rep} function to regenerate the same string \( ID \) from \( b' \) such that \( \text{dis}(b, b') \leq t \).

- **Rep:** A deterministic reproduction procedure that takes as input \( b' \) and the publicly available parameter \( \text{PAR} \), and outputs \( ID \) if \( \text{dis}(b, b') \leq t \).

In [4], the authors describe a concrete fuzzy extractor using a \([n, k, 2t+1]\) BCH error correction code, Hamming Distance metric and a one-way hash function \( H : \{0, 1\}^n \rightarrow \{0, 1\}^t \). Specifically,

- The Gen function takes the biometrics \( b \) as input and returns \( ID = H(b) \) and public parameter \( \text{PAR} = b \oplus C_e(ID) \), where \( C_e \) is a one-to-one encoding function.

- The Rep function takes a biometric \( b' \) and \( \text{PAR} \) as input and computes \( ID' = C_d(b' \oplus \text{PAR}) = C_d(b \oplus b' \oplus C_e(ID)) \). \( ID = ID' \) if and only if \( \text{dis}(b, b') \leq t \). Here \( C_d \) is the decoding function that corrects the errors up to the threshold \( t \).

**3. A New Efficient Biometric IBE Scheme**

Our new biometric IBE scheme BIO-IBE uses Sakai-Kasahara’s Key Construction [6, 12] for the generation of the private keys. This way, BIO-IBE achieves better performance over existing fuzzy IBE schemes due to the use of an ordinary hash function and due to the total number of exponentiations and bilinear pairings required. Besides, the fuzzy extraction process is only performed by the sender to form the ciphertext and can be efficiently implemented on the finite field \( \mathbb{F}_{2^m} \), where \( m \approx 10 \) as described in [4, 8]. In order to encrypt a message, the sender obtains the biometric information and the corresponding public parameter \( \text{PAR} \) of the receiver, extracts the features (attributes) and computes the biometric string \( ID \) using the fuzzy extractor. We assume that if \(|w \cap w'| \geq d \), then we have \( \text{dis}(b, b') \leq t \) and thus \( ID = ID' \). The details of BIO-IBE is presented as follows.

- **Setup:** Given a security parameter \( k_0 \), the parameters of the scheme are generated as follows.
  1. Generate two cyclic groups \( G \) and \( \mathbb{F} \) of prime order \( p > 2^{k_0} \) and a bilinear pairing \( e : G \times G \rightarrow \mathbb{F} \). Pick a random generator \( g \in G \).
  2. Pick a random \( x \in \mathbb{Z}_p^* \) and compute \( P_{pub} = g^x \).
  3. Pick two cryptographic hash functions \( H_1 : \mathbb{Z}_p^* \times \{0, 1\}^k \rightarrow \mathbb{Z}_p^* \) and \( H_2 : \mathbb{F} \rightarrow \{0, 1\}^{k_1} \). In addition, the PKG picks \( H : b \rightarrow \{0, 1\}^*, \) an encoding function \( C_e \) and a decoding function \( C_d \) together with a specific feature extraction method \( F_c \) applied on the biometric \( b \).

The message space is \( M = \{0, 1\}^{k_1} \). The ciphertext space is \( C = U \times \mathbb{G}^n \times \{0, 1\}^{k_1} \). The master public key is \((p, G, \mathbb{F}, e, k_1, g, P_{pub}, H_1, H_2, H, C_e, C_d, F_c)\) and the master secret key is \( ms = x \).

- **Key Generation:** First, a user’s biometric attributes \( w \in U \) are obtained from the raw biometric information using a reader and the feature extractor \( F_c \) and each attribute \( \mu_i \in w \) is associated to a unique integer in \( \mathbb{Z}_p^* \) as in [11]. Besides, the identity string \( ID = H(b) \) is calculated from the biometric template \( b \) (which is composed of the \( \mu_i \)'s) using a fuzzy extractor as in [4]. Given a user’s biometric attributes \( w \) and \( ID \), the PKG returns \( \tilde{D}_{\mu_i, ID} = g^{1/(x + H_1(\mu_i, ID))} \) for each \( \mu_i \in w \).

- **Encrypt:** The sender obtains a biometric reading of the receiver together with the associated public parameter \( \text{PAR} \), extracts the feature vector \( w' \) and computes \( ID' = \text{Rep}(b', \text{PAR}) \). Here, if \( \text{dis}((b, b') < t \), then \( ID = ID' \). Given a plaintext \( m \in \mathcal{M} \), \( ID' \) and \( w' \), the following steps are performed.
  1. Pick a random polynomial \( r(\cdot) \) of degree \( d - 1 \) over \( \mathbb{Z}_p \) such that \( r(0) = r \) and compute the shares \( r(\mu_i) = r_i \in \mathbb{Z}_p \) for \( \mu_i \in w' \).
Here, the polynomial \( r(\cdot) \) of degree \( d - 1 \) is interpolated using \( d \) points by polynomial interpolation in the exponents using Shamir’s secret sharing method [13]. Also, \( h_i^{LD} = h_i^{ID} \) for each \( \mu_i \in S \) and \( ID = ID' \).

**Theorem 3.1.** Suppose the hash functions \( H_1, H_2 \) are random oracles and there exists a polynomial time adversary \( A \) with advantage \( e \) that can break the scheme BIO-IBE in the Fuzzy Selective ID model by making \( q_1, q_2 \) random oracle queries, and \( q_{ex} \) private key extraction queries. Then there exists a polynomial time algorithm \( B \) that solves the \( k \)-BDHI problem with \( k = q_1 + q_{ex} + 1 \).

**Proof.** Assume that a polynomial time attacker \( A \) breaks BIO-IBE, then using \( A \), we show that one can construct an attacker \( B \) solving the \( k \)-BDHI problem.

Suppose that \( B \) is given the \( k \)-BDHI problem \((g, \hat{g}, \hat{e}, G, F, P_{pub}, H_1, H_2, d, D_E)\), for every \( \mu_i \in w \), run the \( H_1 \)-oracle simulator and obtain \((j, l, \mu_i, ID^w, h_j + h_0, Q_1^{(x+h_j)})\) from \( H_1 \)-List. If \( ID^w \neq ID^* \), return \( D_i^{LD} = Q_1^{(x+h_j)} \) for each \( \mu_i \in w \).

**Remark 3.1.** To improve the reduction cost, we can add the following condition to the extraction queries: If the extraction query is on the challenge identity \( ID^w = ID^* \) (namely \(|w \cap w^*| \geq d \)), \( A \) is given the first \( d - 1 \) private key components \( D_i^{LD} = Q_1^{(x+h_j)} \) up to the case when \( \mu_i = \mu^* \), which is the \( d^{th} \) entry in the \( H_1 \)-List with respect to the second counter. Then, we slightly change the security model of our scheme by requiring the adversary \( A \) to select the arbitrary subset \( S \) of \( w^* \) for the computation of the session key such that \( \mu^* \in S \) with \(|S| = d \).

**Phase 3:** \( B \) simulates the private key extraction queries of \( A \) as follows.

**Extraction queries:** Upon receiving a query \((w, ID^w)\) with \(|w \cap w^*| < d \), for each \( \mu_i \in w \), run the \( H_1 \)-oracle simulator and obtain \((j, l, \mu_i, ID^w, h_j + h_0, Q_1^{(x+h_j)})\) from \( H_1 \)-List. If \( ID^w \neq ID^* \), return \( D_i^{LD} = Q_1^{(x+h_j)} \) for each \( \mu_i \in w \).

**Phase 4:** Upon receiving the messages \((m_0, m_1)\) with \(|m_0| = |m_1| \), \( B \) generates the challenge \( C^* \).

1. Pick \( r_t \leftarrow \mathbb{Z}_p \) for each \( \mu_t \in w \) unless \( \mu_t = \mu^* \).
2. Compute $U_{\mu_i} = Q^{r_i(x+H_1(\mu_i, ID^*))}$ for each $\mu_i \in w^*$ except for $\mu_i = \mu^*$. 
3. Pick $r^* \sim \mathbb{Z}_p$ and compute $U_{\mu^*} = Q^{r^*}$. 
4. $B$ chooses $\beta \in \{0, 1\}$ and $W^* \sim \mathbb{Z}_p \times \{0, 1\}^k$. 
5. Set the ciphertext to $C^* = (w^*, U_{\mu^*}, m_{\beta} \oplus W^*)$ where $\mu_i \in w^*$.

**Remark 3.2.** If the condition in Remark 3.1 is applied, then the only way for the adversary $A$ to have any advantage is to query the $H_2$ oracle with the correct session key constructed using the $d$ private key components, where $A$ already knows $d - 1$ of them except for $\mu^*$. And $A$ has to compute the private key share of $\mu^*$ due to the Remark 3.1.

- **Phase 5:** $B$ answers $A$’s random oracle and private key extraction queries as before. The only condition on the private key extraction queries is that the attacker $A$ cannot query the private key $D_{\mu^*}^{ID^*}$. 
- **Phase 6:** At some point, $A$ responds with its guess $\beta^*$ for the underlying plaintext $m_{\beta}$, which could only be computed from

$$m_{\beta} = W^* \oplus H_2(\Pi_{\mu_i \in S}(\hat{e}(U_{\mu_i}, D_{\mu_i}^{ID^*}))).$$

The only way for $A$ to have any advantage in this game is when $H_2$ contains the value 

$$R^* = \Pi_{\mu_i \in S}(\hat{e}(U_{\mu_i}, D_{\mu_i}^{ID^*})) = \hat{e}(Q, Q^{1/x})^{r^*} \Delta_{\mu^*, z(0)} \Lambda$$

where $\Lambda = \Pi_{\mu_i \in S, \mu_i \neq \mu^*}(\hat{e}(Q, Q)^{r_i} \Delta_{\mu_i, z(0)})$

**Remark 3.3.** Obviously, the value $\Lambda$ can be computed by $B$ (also computable by $A$ if the conditions of Remark 3.1 is applied), since $B$ knows the private key components $D_{\mu_i}^{ID^*}$ for each $\mu_i \in S, \mu_i \neq \mu^*$, and $B$ also knows the corresponding $r_i$’s.

We set $T = (R^*/\Lambda)^{1/(r^* \Delta_{\mu^*, z(0)})} = \hat{e}(Q, Q^{1/x})$. The solution to the $k$-BDHI problem, $\hat{e}(g, g^{1/x})$, is obtained by outputting $(T/T_0)^{1/\phi_0} = \hat{e}(g, g^{1/x})$ as in [7].

$$T/T_0 = \hat{e}(g, g)^{f(x)/x} = \hat{e}(g^{f(x)-c_0})^{f(x)/x + c_0} = \hat{e}(g, g)^{c_0} / x$$

Let $\mathbb{H}$ be the event that algorithm $A$ issues a query for $H_2(R^*)$ at some point during the simulation. $\Pr[\mathbb{H}]$ in the simulation above is equal to $\Pr[\mathbb{H}]$ in the real attack [3]. Also, in the real attack we have $\Pr[\mathbb{H}] \geq \epsilon$ due to the following facts.

If the $H_2$ does not contain the value $R^*$, then we have $\Pr[\beta = \beta' | \mathbb{H}] = \frac{1}{2}$.

By the definition of $A$, we have $|Pr[\beta = \beta'] - \frac{1}{2}| > \epsilon$.

Combining all the results and defining the event $E$ as $E = Pr[\beta = \beta']$, we obtain the following as in [3]

$$E = \Pr[\beta = \beta'] \mathbb{H} + \Pr[\beta = \beta' | \mathbb{H}] \Pr[\mathbb{H}] + \Pr[\beta = \beta' | \mathbb{H}] \Pr[\mathbb{H}]$$

$$\iff \Pr[\beta = \beta'] \geq \frac{1}{2}(1 - \Pr[\mathbb{H}])$$

$$\iff \Pr[\beta = \beta'] \leq \frac{1}{2}(1 + \Pr[\mathbb{H}]).$$

Therefore,

$$\epsilon \leq |Pr[\beta = \beta'] - \frac{1}{2}| \leq \frac{1}{2} \Pr[\mathbb{H}] \iff \Pr[\mathbb{H}] \geq 2\epsilon.$$ 

It follows that $B$ produces the correct answer by picking a random entry from the $H_2$ list with probability at least $\frac{2\epsilon}{\Pr[\mathbb{H}] + \epsilon}$ due to the $q_2$ entries in the $H_2$ list and \(\binom{n}{d}\) different choices for $A$ to compute the session key. Hence,

$$\Pr[\beta = \beta'] \leq q_2 \cdot \text{Adv}^{\text{key-recovery}}(B)$$

When we apply the condition on Remark 3.1, the adversary $A$ will have only one choice for the set $S$, thus the factor \(\binom{n}{d}\) is eliminated from the reduction cost resulting in

$$\Pr[\beta = \beta'] \leq q_2 \cdot \text{Adv}^{\text{key-recovery}}(B)$$

The modified security model gives the adversary as much power as possible by providing the adversary with $d - 1$ private key components, and the restriction for the set $S$ is necessary for $B$ to have any advantage in this game. Thus, the improved reduction cost is obtained by requiring a stronger security model than the Fuzzy Selective-ID model of [11, 11].

\[\Box\]

### 4. Conclusion

In this paper, we propose a new biometric identity based encryption scheme BIO-IBE. Due to the employment of the Sakai Kasahara Key Construction, we obtain a more efficient scheme compared to the schemes in [10, 1]. We summarize in the following tables the properties of BIO-IBE and compare the computational costs of each algorithm used in the schemes. Obviously, BIO-IBE is more efficient in terms of the sub-algorithms of the schemes. Besides, the computational cost of the fuzzy extraction $FE$ is small, since the operations in $FE$ algorithm are performed on the finite field of $\mathbb{F}_{2^m}$, where $m \approx 10$ according to [4]. The only disadvantage is that the reduction is not tight, however, the BIO-IBE is reduced to a well-exploited computational
problem. Finally, an open problem is to prove the security of BIO-IBE in the standard model.

Table 1. Properties of Various Fuzzy IBE Schemes

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Assumption</th>
<th>Hash Function</th>
<th>Security Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW-RO</td>
<td>Decisional BDH</td>
<td>MaptoPoint</td>
<td>ROM</td>
</tr>
<tr>
<td>EFIBE-I</td>
<td>Decisional BDH</td>
<td>MaptoPoint</td>
<td>ROM</td>
</tr>
<tr>
<td>EFIBE-II</td>
<td>Decisional BDH</td>
<td>MaptoPoint</td>
<td>ROM</td>
</tr>
<tr>
<td>BIO-IBE</td>
<td>Computational k-BDHI</td>
<td>One-way</td>
<td>ROM</td>
</tr>
</tbody>
</table>

Acknowledgement

The author is grateful to her supervisor Prof. Dr. Joachim von zur Gathen for his valuable support.

References