BRAKE: Biometric Resilient Authenticated Key Exchange

Bauspiess, Pia; Silde, Tjerand; Poljuha, Matej; Tullot, Alexandre; Costache, Anamaria; Rathgeb, Christian; Kolberg, Jascha; Busch, Christoph

Published in:
IEEE Access

Link to article, DOI:
10.1109/ACCESS.2024.3380915

Publication date:
2024

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 26 January 2024, accepted 15 March 2024, date of publication 22 March 2024, date of current version 3 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3380915

RESEARCH ARTICLE

BRAKE: Biometric Resilient Authenticated Key Exchange

PIA BAUSPIEß[1,2], TJERAND SILDE[2], MATEJ POLJUHA[3], ALEXANDRE TULLOT[4], ANAMARIA COSTACHE[2], CHRISTIAN RATHGEB[1], JASCHA KOLBERG[1], AND CHRISTOPH BUSCH[1,2], (Senior Member, IEEE)

[1]Biometrics and Security Research Group (da/sec), Department of Computer Science, Hochschule Darmstadt, 64295 Darmstadt, Germany
[2]Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), 7034 Trondheim, Norway
[3]Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU Compute), 2800 Kongens Lyngby, Denmark
[4]National Higher French Institute of Aeronautics and Space (ISAE-SUPAERO), 31055 Toulouse, France

Corresponding author: Pia Bauspieß (pia.bauspiess@ntnu.no)

This work was supported by German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science, and the Arts within their joint support of the National Research Center for Applied Cybersecurity (ATHENE).

ABSTRACT Biometric data are uniquely suited for connecting individuals to their digital identities. Deriving cryptographic key exchange from successful biometric authentication therefore gives an additional layer of trust compared to password-authenticated key exchange. However, biometric data are sensitive personal data that need to be protected on a long-term basis. Furthermore, efficient feature extraction and comparison components resulting in high intra-subject tolerance and inter-subject distinguishability, documented with good biometric performance, need to be applied in order to prevent zero-effort impersonation attacks. In this work, we present a novel protocol for *Biometric Resilient Authenticated Key Exchange* that fulfils the above requirements of biometric information protection compliant with the international ISO/IEC 24745 standard. In our protocol, we present a novel modification of unlinkable fuzzy vault schemes that allows their connection with oblivious pseudo-random functions to achieve resilient protection against offline attacks crucial for the protection of biometric data. Our protocol is independent of the biometric modality and can be implemented based on the security of discrete logarithms as well as lattices. We provide an open-source implementation of both instantiations of our protocol which achieve real-time efficiency with transaction times of less than one second from the image capture to the completed key exchange.

INDEX TERMS Authenticated key exchange, biometric information protection, fuzzy vault, oblivious pseudo-random function.

I. INTRODUCTION

Biometric characteristics provide accurate and non-repudiable identification of individuals over several decades [1]. This makes them suited for bridging the gap between real and digital identities in a way passwords or other machine-generated identifiers cannot. At the same time however, these properties also make them uniquely vulnerable. In particular, biometric information cannot be revoked or replaced in the same way a password or cryptographic token can. Once a digital representation of a biometric characteristic, further referred to as a biometric template, has been leaked, the underlying source (e.g., a particular finger or eye), can no longer be used securely for authentication. In fact, biometric templates provide no protection of the underlying data, as they can be reversed to samples sufficient for attacks [2], [3], [4].

Due to this risk, biometric data have been recognised as sensitive personal data by the European Union's General Data Protection Regulation (GDPR) [5] and the ISO/IEC 24745 international standard on biometric information protection [6]. The latter defines three security requirements for secure biometric systems: *i) unlinkability and renewability*, meaning that an attacker cannot connect two protected biometric templates stored in different applications, and new templates from the same source look indistinguishable to a

The associate editor coordinating the review of this manuscript and approving it for publication was Vincenzo Conti.

previously stored reference, *ii) irreversibility*, it should be impossible for an attacker to retrieve original samples given only protected templates, and *iii) performance preservation*, the computational performance and the recognition accuracy of the system should not be impacted significantly by adding a layer of protection to the original data.

At first sight, the performance preservation requirement in ISO/IEC 24745 seems to be a question of convenience only. However, it details a second and crucial dimension that determines the security of biometric authentication: the accuracy of the underlying biometric comparison function. Contrary to passwords, which can be compared in an exact manner, captured samples of the same biometric characteristic are never exactly equal, but *fuzzy*. They are subject to noise such as ageing, environmental influence, or image quality. Comparison of two samples is therefore based on some measure of similarity. If this measure is too imprecise, or the feature representation is not discriminative enough, an authentication system is not capable of accurately distinguishing between mated comparisons, where the samples stem from the same subject, and non-mated authentication attempts, where the samples stem from different subjects. Trust in the derived authentication would consequently be low.

Recently, the idea of building authenticated key exchange on the basis of biometrics has gained interest with the proposal of Biometrics-Authenticated Key Exchange (BAKE) [7]. Analogously to Password-Authenticated Key Exchange (PAKE) [8], a client and server negotiate a shared cryptographic key that should be equal if and only if the biometric authentication was successful.

With their protocol, the authors of [7] achieve security in terms of the protection of the biometric data with classical security assumptions. However, their biometric comparator is vulnerable, as we show by reproducing their results experimentally. The reason for this imprecision is a fingerprint comparison algorithm that is specific to their protocol, but has not been evaluated in terms of biometric performance (i.e., accuracy). We provide this evaluation and show that the algorithm is not able to distinguish between mated comparison trials within the same identity and non-mated comparison trials between different identities in a sufficient manner (see Appendix A). More generic protocols both on symmetric fuzzy PAKE (fPAKE) [9] and asymmetric fuzzy PAKE (fuzzy aPAKE) [10] have been proposed. However, with regard to biometrics, they have the following shortcomings: fPAKE [9] does not achieve protection of the biometric data, which is shared with the server in plaintext. Fuzzy aPAKE [10] achieves security in both dimensions in theory, but is inefficient in practice as it is based on generic oblivious transfer which is performed once for each bit in the biometric template. In addition, [9] and [10] only enable comparison of fixed-length biometric representations. The most accurate comparison metric for fingerprints, one of the most popular biometric modalities, is however based on variable-length representations, the similarity of which cannot be expressed as a simple distance function.

A. CONTRIBUTION

In this work, we present a protocol for *Biometric Resilient Authenticated Key Exchange* (BRAKE) that addresses the deficiencies of previous works [7], [9], [10]. Our BRAKE protocol achieves effective protection of the biometric data against offline attacks through the application of an *Oblivious Pseudo-Random Function* (OPRF). Our protocol is efficient with execution times of under one second on commodity hardware from the biometric capture to the completed key exchange, including communication cost. To the best of our knowledge, our protocol is the first to achieve secure biometric authenticated key exchange with high biometric and computational performance, thus fulfilling ISO/IEC 24745. More precisely, we contribute:

- Biometric resilient authenticated key exchange secure against offline attacks: through a novel modification of unlinkable fuzzy vault schemes, we build a seamless integration of biometric authentication into oblivious pseudo-random functions to achieve resilient protection against offline attack, which is crucial for the long-term protection of biometric data according to the ISO/IEC 24745 [6] standard.
- Classical and post-quantum security: Our two-round protocol can be instantiated both with a discrete logarithm OPRF [8] and Diffie-Hellman key exchange [11] as well as a lattice-based OPRF [12] and the state-of-the art post-quantum key encapsulation mechanism CRYSTALS Kyber [13], which was recently standardized in NIST IR 8413 [14]. Through our protocol's compatibility with lattice-based primitives, which are assumed to be post-quantum secure, we further achieve long-term protection of the underlying biometric data.
- Interchangeability of biometric modalities: our protocol can be instantiated with different fuzzy vault schemes that have been designed for different biometric modalities and feature representations. In particular, it is compatible with both fixed-length and variable-length representations of biometric characteristics.
- Open-source implementation: an implementation of our protocol based on discrete logarithms as well as lattices is available at https://github.com/dasec/DL-BRAKE and https://github.com/dasec/PQ-BRAKE, respectively. We show that our protocol achieves real-time efficiency with transaction times of under one second from the fingerprint image capture at the sensor to the completed key exchange. To support the reproducibility of our results, we provide automated installation scripts with all dependencies alongside our implementation.

B. RELATED WORK

We briefly discuss the state-of-the-art to motivate two principles for secure biometrics-authenticated key exchange: recognition accuracy and reciprocal interaction.

TABLE 1. Comparison of our protocol to related work.

Scheme	Year	Feature representation	Cryptographic primitives	Asymmetric	Efficient	Accurate	Post-quantum security	Compliant with ISO/IEC 24745
fPAKE [9]	2018	binary, fixed-length	GC + ECC	✗	✓	✓	✗	✗
fuzzy aPAKE [10]	2020	binary, fixed-length	ECC + OT	✓	✗	✓	✗	✗
BAKE [7]	2021	integer, variable-length	ECC + LWE	✓	✓	✗	✓	✗
iPAKE [15]	2023	binary, fixed-length	ECC + PAKE	✗	✓	✓	✗	✗
ttPAKE [16]	2023	binary, fixed-length	Secret sharing + OT	✓	✓	✓	✗	✗
BAKA [17]	2023	binary, fixed-length	ECC + Blockchain	✓	✓	✓	✗	✗
BRAKE *(ours)*	2023	integer, variable-length	ECC + PAKE	✓	✓	✓	✓	✓

The main concern with the protocol proposed in [7] is the generation of the biometric secret key constructed from fingerprint representations. The authors use a simplified version of the well-studied nearest-neighbour approach first proposed by [18], which they chose due to its anticipated rotation invariance. However, this algorithm and its flaws have been studied for two decades, specifically, its inability to tolerate missing genuine minutiae [19]. It has therefore been found unusable in practice, and improved rotation-invariant fingerprint recognition algorithms have been proposed that mitigate the known shortcomings [19]. Such improved algorithms require a more complex comparison subsystem however, and are not compatible with the constructor offered in [7]. Notably, the authors of [7] fail to state the recognition accuracy of their iris and fingerprint based protocols, and do not give an experimental evaluation detailing the security with regard to the biometric performance.

Their construction for iris is based on the established fixed-length feature representation IrisCode [20] and can be assumed to achieve adequate accuracy as long as the sample quality is high. It is worth noting that the state-of-the-art in iris recognition is based on samples captured under near-infrared light, and therefore requires designated capture devices, i.e., near-infrared sensors. Such specific sensors are however not part of most personal communications devices such as smartphones. The use of classical iris recognition in the Signal [21] protocol as motivated by [7] is therefore not meaningful. In such a scenario, iris recognition in the visual spectrum would need to be considered, which is a more challenging task and provides, as of today, lower accuracy [22].

Secondly, the public keys derived from the biometric secret keys in [7] are vulnerable to offline attacks: in their construction, any adversary can guess a biometric template and check if it corresponds to the public key in hand, without interacting with another party. In such an attack, the adversary does not have to guess an exact biometric feature representation, but succeeds as soon as she finds an input that is close enough with regard to the distance metric used. This probability can be expressed as the false-match rate of the biometric system, i.e., the proportion of authentication attempts from non-mated samples falsely accepted as authentication attempts of an enrolled data subject. Again, low biometric accuracy leads to a low effort in an offline search attack.

Even with assumed high biometric accuracy, offline attacks expose biometric data to high risks. Therefore, we construct our protocol such that interaction is required for every adversarial guess, which allows for rate-limiting that can be enforced as long as at least one party remains honest. The concept of enforcing interaction through a third party OPRF service in itself is not new [23]. However, the construction previously presented by [23] is neither trivially compatible with fuzzy secrets such as biometric features, nor with lattice-based primitives as our proposed protocol. In particular, no lattice-based partially OPRF as required for the protocol given in [23] is known as of today, and its construction lies outside of the scope of this work.

An overview of how our proposed scheme compares to related works can be found in Table 1. An efficient solution to fuzzy PAKE was presented by [9]. However, the solution is constructed as a symmetric protocol, where the server learns the biometric reference template. The approach of [9] does therefore not fulfil the ISO/IEC 24745 [6] requirements. Building on this line of research, [15] recently proposed fuzzy PAKE based on Error-Correcting Codes (ECC). While their protocol is efficient with a small overhead compared to [9] and improves upon the security of [9], the symmetric construction remains an obstacle with regard to ISO/IEC 24745 [6].

A different line of research emerged with the fuzzy asymmetric PAKE construction of [10]. Here, the asymmetric protocol does not allow the server to learn the biometric reference template. However, the expensive computation of bit-wise Oblivious Transfer (OT) makes the solution impractical for real-world applications. More recently, [16] proposed their solution ttPAKE to typo-tolerance PAKE, which can be considered related to the challenges posed by biometric authentication with regard to the fuzziness of input data. Their solution builds on the idea of [10], but is based on double-layered secret sharing. While their protocol is asymmetric, the password is shared with the server in the setup phase for the purpose of constructing a secret-shared password table, and is deleted by the

semi-honest server afterwards. If this protocol were applied to biometric data, this plaintext disclosure of the authentication secret would violate the ISO/IEC 24745 [6] requirements. Another recent work presents BAKA [17], a protocol for biometric authentication and key agreements based on fuzzy extractors. However, this work applies blockchain to store biometric data, which is an inherent violation of the ISO/IEC 24745 [6] renewability requirement. Through the immutability of blockchain records, compromised reference templates cannot be renewed. Furthermore, none of the above works apart from [7] have been instantiated using post-quantum secure cryptographic primitives.

Further recent works are concerned with authentication based on fuzzy input data, however, with different aims to our work. Motivated by more private solutions for TLS authentication, [24] proposed single message Credential Hiding Login (CHL). Their one-round protocol allows for efficient user authentication both for static and fuzzy secrets, with biometric authentication as a possible application. Their scheme is based on the security of Learning with Errors (LWE) problems and can be instantiated with post-quantum secure parameters. In contrast to our work however, not session keys are exchanged as a result from the successful login. Another solution to biometric authentication based on functional encryption was recently presented by [25]. While their solution is computationally efficient, no key material is generated from the successful biometric two-factor authentication. Similarly, [26] presented post-quantum secure biometric authentication using searchable encryption, a cryptographic technique related to functional encryption as applied in [25].

Other related works have been directed on extracting uniformly distributed cryptographic keys directly from biometric templates without running an interactive protocol [27]. Similar to [9] and [10], only fixed-length representations are considered that can be compared with some distance metric. From fuzzy extractors, two-factor authentication protocols have been built [28]. More recently, [29] proposed a session key generation protocol specifically for fingerprint based on so-called cancellable biometrics, which are one-way transforms on the biometric data that are not based on well-studied cryptographic problems and can therefore not be assumed to underlie specific hardness assumptions.

C. STRUCTURE OF PAPER

The rest of this paper is structured as follows: In Section II, background information and definitions required for the construction of our protocol are presented. As our main contribution, Section III presents our BRAKE protocol with security definitions and proof sketches, before we give concrete instantiations based on discrete logarithms and lattices in Section IV. Section V presents the experimental evaluation of the protocol and practical comparison with related work, before we outline our conclusions in Section VI.

II. PRELIMINARIES

The framework for automated and interoperable biometric recognition has been standardised in ISO/IEC 19794-1 [30], and subsequent parts of the standard define biometric data interchange formats for the modalities fingerprint, face, iris, voice, handwritten signatures, and vascular biometrics. For the scope of our work, we look at the three most prevalent modalities fingerprint, face, and iris, for which well-tested fuzzy vault schemes exist.

A. BIOMETRIC PERFORMANCE METRICS

Biometric performance testing and reporting is standardised in ISO/IEC 19795-1 [31] and subsequent parts. The evaluation of biometric systems is based on two components: error rates and throughput rates. For a verification scenario, the most important error metrics are:

- *False Non-Match Rate (FNMR):* proportion of mated comparisons that resulted in a reject decision.
- *False Match Rate (FMR):* proportion of non-mated comparisons that resulted in an accept decision.

The FMR can be thought of as the security level of the biometric system, detailing how many zero-effort impostors were able to be verified. In most scenarios, systems with a FMR below 1% are considered secure, while high-security applications such as automated border control require a FMR lower than 0.1% [32]. The FNMR on the other hand can be considered as the convenience level of the system, detailing how many mated comparison trials were not able to be verified. A FNMR up to 5% is considered acceptable [32].

Factors impacting the recognition performance of a biometric system are first and foremost the sample quality both during enrolment and verification, and the robustness of the feature representation and comparison algorithm with regard to rotation, translation, and noise of the samples [33], [34]. Furthermore, any feature transformation such as binarisation may impact the accuracy of the system.

B. ENTROPY OF BIOMETRIC REPRESENTATIONS

The entropy of biometric data is a topic that is often referred to in works about fuzzy cryptographic primitives [9]. In the literature, the entropy of a face has been determined at 56 bits [35], a minutiae-based fingerprint representation at 82 bits [36], and an iris at 249 bits [37]. However, these numbers can only be considered as an upper bound of the entropy of a certain biometric instance, as the amount of information in a biometric sample heavily depends on the capture device used and its fidelity (e.g., its resolution) as well as the feature extraction algorithm used. Indeed, [38] argues that it is not in all scenarios appropriate to use the entropy of a single biometric template as a measure for security, which is an overestimate when it comes to comparisons between biometric features. Here, the false-accept security defined as $\log_2(FMR^{-1})$ gives a more accurate measure, as it is sufficient for an attacker to guess a template that is close enough to a reference template.

Enrolment

Setup party	Server
t reference template	
$(f, H(f), V) \leftarrow \texttt{lock}(t)$	
$\xrightarrow{H(f), V}$	
	store $(H(f), V)$

Verification

Client	Server
t' probe template	$(H(f), V)$
$\xrightarrow{\text{request } H(f), V}$	
$\xleftarrow{H(f), V}$	
$f' \leftarrow \texttt{unlock}(V, H(f), t')$	
return $H(f) = H(f')$	

FIGURE 1. Fuzzy vault authentication protocol based on [39].

C. FUZZY VAULT

The concept of fuzzy vaults was first introduced by [39], who propose a scheme that allows to *lock* a biometric feature secret set t with a secret polynomial f using a biometric feature secret set t using a probabilistic algorithm. The output of this algorithm is a locked fuzzy vault that can be *unlocked* using a second biometric feature set t', if there are enough points the intersection of t and t'. We give a short definition of their original scheme before we move on to the state-of-the-art for different biometric modalities.

Definition 1 (Fuzzy Vault Scheme [39]): Let $\mathcal{C}$ be an error-correcting code, $H : \mathcal{C} \to \{0,1\}^{2\lambda}$, for security parameter λ, be a cryptographic hash function H, and let τ a biometric comparison threshold. Then, a *fuzzy vault scheme* is a set of the following algorithms:

- $(f, H(f), V) \leftarrow \texttt{lock}(t)$: On input of a biometric feature set t, the algorithm samples a random secret $f \in \mathcal{C}$ and outputs a locked fuzzy vault V together with the hash digest $H(f)$.
- $f' \leftarrow \texttt{unlock}(V, H(f), t')$: On input of a locked fuzzy vault V and a biometric feature set t', the algorithm outputs an opening polynomial $f' \in \mathcal{C}$. The unlocking can be verified by comparing $H(f)$ to $H(f')$.

A basic authentication protocol based on the fuzzy vault scheme is given in Figure 1.

INSTANTIATION FOR FINGERPRINT

The original schemes by [39] and a similar scheme by [40] have been proven to be insecure due their construction based on large point clouds to hide the secret f, which are vulnerable to correlation attacks [41]. Therefore, [38] presented an improved scheme to mitigate correlation attacks (see [38], Section 1.2.3), building on the initial proposal by [27]. These improved fuzzy vault schemes fulfil the requirements of ISO/IEC 24745 [6].

The improved fuzzy vault scheme has first been constructed for minutiae-based fingerprint representations [38]. From the pattern of fingerprint ridge lines, significant points known as *minutiae* are extracted as compact and distinguishing features, specifically, ridge endings and bifurcations, namely the location and orientation where one ridge line splits into two. In the scheme by [38], minutiae are encoded into a finite field $\mathbb{F}_{p'}$ using absolute pre-alignment and quantisation to account for a certain degree of noise with regard to the position of the minutiae. The set of minutiae $t \subset \mathbb{F}_{p'}$ is then considered the biometric template. A polynomial $f \in \mathbb{F}_{p'}[x]$ of degree $\tau - 1$ is chosen uniformly at random and locked as

$$\texttt{lock}(t) = (f, f(x) + \prod_{a \in t}(x - a)) =: (f, V).$$

To unlock the vault, V is evaluated on the probe minutiae set t' and decoded using a Reed-Solomon decoder, yielding

$$\texttt{unlock}(V, t') = \text{decode}(\{(b, V(b)) \mid b \in t'\}) =: f'.$$

Lemma 1 (Theorem 1 in [38]): Let $(f, H(f), V) \leftarrow \texttt{lock}(t)$ be a commitment to a polynomial $f \in \mathbb{F}_{p'}[x]$ with minutiae set t, and $f' \leftarrow \texttt{unlock}(V, H(f), t')$ an unlocking of V using a minutiae set t'. Then, $f = f'$ if and only if $|t \cap t'| \geq \tau$.

Analogue constructions exist for iris [42] and face [43] recognition, which we refer the reader to for full details.

D. CRYPTOGRAPHIC PRIMITIVES

Definition 2 (Pseudo-Random Function, [44]): A family of functions $f_k : \{0,1\}^{\lambda} \times \{0,1\}^{n} \to \{0,1\}^{n'}$, with key $k \in \{0,1\}^{\lambda}$, are called Pseudo-Random Functions (PRFs) if the following holds:

- $f_k(x)$ is efficiently computable from k and x.
- It is not efficiently decidable whether one has access to a computation oracle for $f_k(\cdot)$ or to an oracle producing uniformly random bit-strings of length n.

Definition 3 (Oblivious Pseudo-Random Function, [45]): A two-party protocol π between a client and a server is an Oblivious Pseudo-Random Function (OPRF) if there exists some PRF family f_k, such that π privately realizes the following functionality:

- Client has input x; Server has input k.
- Client outputs $f_k(x)$; Server outputs nothing.

Definition 4 (Hashed Diffie-Hellman OPRF, [46]): Let $\mathbb{G}$ be a cyclic group of prime order p, $x \in \{0,1\}^*$ the client input, $k \in \mathbb{Z}_p$ the evaluator's secret key, $H_{\mathbb{G}} : \{0,1\}^* \to \mathbb{G}$ and $H_{\mathbb{Z}_p} : \{0,1\}^* \to \mathbb{Z}_p$ cryptographic hash functions that output values in $\mathbb{G}$ and $\mathbb{Z}_p$, respectively. The protocol HashDH consists of the following algorithms:

- $(B, r) \leftarrow \texttt{blind}(x)$: The client samples a random $r \leftarrow \mathbb{Z}_p$ and outputs r and $B \leftarrow [r]H_{\mathbb{G}}(x)$.
- $S \leftarrow \texttt{eval}(B, k)$: On input $B \in \mathbb{G}$, the evaluator outputs $S \leftarrow [k]B$.

- $U \leftarrow \texttt{unblind}(S, r)$: On input $S \in \mathbb{G}$ and $r \in \mathbb{Z}_p$, the client outputs $U \leftarrow H_{\mathbb{Z}_p}(x, [r^{-1}]S)$.

As a result of this protocol, the client privately obtains $H_{\mathbb{Z}_p}(x, [k]H_{\mathbb{G}}(x))$ without learning k and without the evaluator learning the input x nor the output U.

Definition 5 (Key Encapsulation Mechanism, [47]): A Key Encapsulation Mechanism (KEM) is a scheme with three algorithms KeyGen, encap and decap, where

- $(\texttt{pk}, \texttt{sk}) \leftarrow \texttt{KeyGen}(1^\lambda)$: takes as input the security parameter λ and outputs a public key pk and a secret key sk.
- $(\texttt{ctx}, \gamma) \leftarrow \texttt{encap}(\texttt{pk})$: takes as input a public key pk, samples a session pre-key γ, and outputs γ and an encapsulation ctx of γ under the public key pk.
- $\gamma' \leftarrow \texttt{decap}(\texttt{ctx}, \texttt{sk})$: takes as input an encapsulated session pre-key ctx and a secret key sk and outputs a decapsulated session pre-key γ'.

We require that for all (pk, sk) generated from KeyGen we have that $\gamma = \texttt{decap}(\texttt{encap}(\gamma, \texttt{pk}), \texttt{sk})$, except with negligible probability, and that the scheme is IND-CCA secure.

E. LATTICE-BASED CRYPTOGRAPHY

Lattice-based cryptography builds upon certain lattice problems which are considered hard to solve even for quantum computers, and these can be used as the basis for designing a variety of cryptographic systems [48]. The two most popular lattice problems are the *Learning With Errors* (LWE) decision-problem introduced in [49] and the *Short Integer Solution* (SIS) search-problem introduced in [50]. In this work, we use the module variants of these problems, where we are working over cyclotomic rings $R_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle$ where N is a power of two and q a prime. The norm of elements in R_q is computed on coefficient vectors of polynomials in $\mathbb{Z}$.

Definition 6: (Module-LWE). Let χ be a bounded distribution over R_q^d and let $s \leftarrow \chi$ be a secret vector. Then, sample $A_i \in R_q^{d\times d}$ uniformly at random and $e_i \leftarrow \chi$, and finally set $(A_i, b_i = A_i \cdot s + e_i)$ in $R_q^{d\times d} \times R_q^d$. The M-LWE$_{d,s,\chi}$ decision-problem is to decide with non-negligible advantage whether m independent samples $\{(A_i, b_i)\}_{i=1}^m$ are computed as above or sampled from the uniform distribution over $R_q^{d\times d} \times R_q^d$.

Definition 7: (Module-SIS). Given m uniform vectors $a_i \in R_q^d$, the M-SIS$_{d,m,\beta}$ problem is to find polynomials $s_i \in R_q$ such that all $||s_i|| \leq \beta$ and

$$\sum_{i=1}^{m} a_i \cdot s_i = 0 \in R_q.$$

III. BIOMETRIC RESILIENT AUTHENTICATED KEY EXCHANGE

In this Section, we introduce our protocol for Biometric Resilient Authenticated Key Exchange (BRAKE) built from a fuzzy vault scheme, an OPRF, and a KEM.

A. SETTING

For our proposed protocol, we assume that a biometric capture device is linked to a client which performs the preprocessing and feature extraction, and acts as a communicating party in the protocol. Its communication counterparts are a server which controls a database of locked fuzzy vaults and client reference public keys, and an evaluator which is in possession of a secret OPRF key. In practice, the evaluator can be instantiated by a trusted execution environment at the server. For this reason, we do not model direct communication between the client and the evaluator, but work under the weaker assumption that all communication between client and evaluator is seen by the server. This is a common practice in biometric information protection [51], as it allows for enhanced network security choices that protect the party handling secret key material. Furthermore, we assume that authenticated channels are established between all parties, e.g., through TLS. Thereby, mutual authentication can be established between a client and the server.

B. MODIFICATION OF FUZZY VAULT SCHEMES

In the original improved fuzzy vault schemes, the decoding algorithm with highest performance both in terms of execution times and accuracy is the Guruswami-Sudan decoder [52]. Thereby, unlocking a fuzzy vault with feature vector t' corresponds to a randomised brute-force decoding strategy, where subsets of t' are chosen uniformly at random and evaluated as unlocking sets for the reference fuzzy vault. During this randomised decoding, a candidate polynomial f' is generated for each subset and compared against the stored hash $H(f)$ corresponding to the biometric reference template t. When a candidate polynomial is found for which $H(f) = H(f')$, the decoding attempts are stopped. If no candidate polynomial is found within a certain number of decoding attempts, the underlying comparison of t and t' is classified as a non-mated comparison trial.

In our protocol however, we do not wish to store $H(f)$ at the server as it allows for offline brute-force attacks. Instead, we run the full decoding attempts until the threshold for non-mated comparison trials is reached, even when we expect a mated comparison trial. During decoding, we temporarily store all candidate polynomials and sort them with respect to their frequency. For a mated comparison, we expect the correct candidate polynomial f' for which $H(f') = H(f)$ to appear as the most frequently reconstructed polynomial due to the large overlap of the sets t and t'. A similar strategy is applied in [40] and is supported by our experimental evaluation, showing only a negligible deviation with regard to the biometric performance.

Notably, the FMR and thereby security of the system is not affected by the change to highest-frequency decoding. In both cases, no non-mated comparisons yield matching candidate polynomials within the list decoder threshold. Therefore, the polynomial that occurs with the highest frequency is also not a matching candidate polynomial. Consequently, the FMR is

not affected by the change from hash-verified decoding to highest-frequency decoding.

In addition, the frequency pattern found in a mated comparison does not give an attacker an advantage in terms of an offline-brute force attack. Through the additional roots of the randomly generated secret polynomial f, a number of seemingly correct polynomials of degree $\tau - 1$ could be interpolated by an attacker that is not in possession of a mated feature set. Therefore, a brute-force attack on a locked vault alone, without the confirmation of $H(f)$ or a successful key exchange, corresponds to a non-mated comparison attempt with no clear frequency pattern.

C. PROTOCOL

In this Section, we give the formal definition of our proposed protocol for biometric resilient authenticated key exchange.

Definition 8: (Biometric Resilient Authenticated Key Exchange) A three-party protocol BRAKE between a client, a server and an evaluator is a Biometric Resilient Authenticated Key Exchange, if it realizes the following functionalities:

- Enrolment: A trusted setup party inputs a biometric reference template t and corresponding identifier id. The setup party computes a locked vault (f, V) based on t. The evaluator inputs a key k. Then the parties jointly compute a client public key $\mathtt{cpk}_t$ derived from f. The server outputs $(V, \mathtt{cpk}_t = \mathtt{eval}(f, k), \mathtt{id})$ and the other parties outputs nothing. The enrolment protocol is detailed in Figure 2.
- Verification: The client inputs a biometric probe feature set t' and a biometric claim id, the server inputs $(V, \mathtt{cpk}_t, \mathtt{id})$ and the evaluator inputs k. The client requests the locked vault V for id and interpolates a polynomial f' from t'. The parties jointly compute a key exchange on input f'. The server outputs a session key ρ and the client outputs a session key ρ' and a bit indicating if $H(\rho) = H(\rho')$. The verification is detailed in Figure 3.

Here, the client will output the bit 1 if and only if $|t \cap t'| \geq \tau$ for τ the biometric verification threshold. For the algorithms defined in Definition 8, we require the following building blocks:

Definition 9 (Building blocks): We define the following building blocks for the BAKE protocol:

- $\mathtt{pp} \leftarrow \mathtt{setup}(1^\lambda)$: The setup algorithm defines a universe $\mathcal{P}$, randomness space $\mathcal{R}$, key space $\mathcal{K}$ and a cryptographic hash function $H : \{0,1\}^* \rightarrow \{0,1\}^{2\lambda}$. Further, the setup algorithm defines an error-correcting code $\mathcal{C}$ with correction capacity τ. These are incorporated in the public parameters pp and all following algorithms implicitly inherit pp.
- $(f, V) \leftarrow \mathtt{lock}(t)$: The algorithm takes as input a biometric template t, samples a random polynomial $f \in \mathcal{C}$, and outputs f and a locked fuzzy vault V. Note that the fuzzy vault scheme do not include the hash digest $H(f)$.
- $f' \leftarrow \mathtt{unlock}(V, t')$: The algorithm takes as input a biometric probe feature vector t' and locked fuzzy vault V, and outputs an opening polynomial f'.
- $(B, r) \leftarrow \mathtt{blind}(f)$: The algorithm samples a random element $r \in \mathcal{R}$ and outputs an element $B \in \mathcal{P}$.
- $S \leftarrow \mathtt{eval}(B, k)$: On input $B \in \mathcal{P}$ and key $k \in \mathcal{K}$, the server outputs an evaluation $S \in \mathcal{P}$.
- $\mathtt{sk} \leftarrow \mathtt{unblind}(S, r)$: On input $S \in \mathcal{P}$ and $r \in \mathcal{R}$, the algorithm outputs an evaluation t U that can further be used as (or to generate) a client secret key $\mathtt{csk} \in \mathcal{K}$.
- $(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KeyGen}(1^\lambda)$: The algorithm outputs a secret key $\mathtt{sk} \in \mathcal{K}$ and a public key $\mathtt{pk} \in \mathcal{P}$.
- $\mathtt{pk} \leftarrow \mathtt{pkGen}(\mathtt{sk})$: The algorithm takes as input a secret key $\mathtt{sk} \in \mathcal{K}$ and outputs a public key $\mathtt{pk} \in \mathcal{P}$.
- $(\mathtt{ctx}, \gamma) \leftarrow \mathtt{encap}(\mathtt{cpk})$: The algorithm takes as input a client public key cpk, samples a session pre-key γ and outputs γ and an encapsulation ctx of γ under cpk.
- $\gamma' \leftarrow \mathtt{decap}(\mathtt{ctx}, \mathtt{csk})$: The algorithm takes as input an encapsulated session pre-key ctx and a client secret key csk and outputs a decapsulated session pre-key γ'.
- $\rho \leftarrow \mathtt{KDF}(\mathtt{cpk}, \mathtt{spk}, \mathtt{cpk}_e, \mathtt{spk}_e, \gamma)$: The key derivation function KDF takes as input the client and server static and ephemeral public keys cpk, spk, $\mathtt{cpk}_e$, $\mathtt{spk}_e$ as well as a pre-key γ and outputs a session key $\rho \in \{0,1\}^{2\lambda}$.

The detailed functioning of the BRAKE protocol can be seen in Figures 2 and 3. We also give a short semantic description in the following. During enrolment (Figure 2), a client public key $\mathtt{cpk}_t$ is derived from a biometric reference template t and the OPRF key k, and is stored at the server together with a locked fuzzy vault V of t using a secret random polynomial f. First, the client generates f and locks the vault with template t. Note that now, the fuzzy vault scheme no longer includes the hash digest $H(f)$ of the secret polynomial sampled during locking. Then, the client initiates the OPRF evaluation on input f. The evaluator evaluates the blinded input B using the OPRF key k, and the client is able to unblind and obtain its secret key $\mathtt{csk}_t$, from which it computes the corresponding public key $\mathtt{cpk}_t$. To conclude the enrolment step, the client sends the tuple $(V, \mathtt{cpk}_t, \mathtt{id})$ to the server to be stored for future reference.

For verification and key exchange (Figure 3), the client requests the fuzzy vault V stored at the server for identity id, and, using a biometric probe t', unlocks the vault to a polynomial f'. Then, the OPRF evaluation on f is computed analogously to the enrolment step. At the same time, the client and server generate ephemeral key pairs to prepare the key exchange. Additionally, the server has a static key pair (ssk, spk) generated during setup that is not derived from any biometric information. For the key exchange, we assume that the client has access to the static server public key spk as discussed above. Once all keys have been generated, the server encapsulates a session pre-key γ using the client's public key $\mathtt{cpk}_t$. The client can decapsulate γ if and only if the secret reconstructed from the fuzzy vault was correct, i.e.,

Enrolment

Setup party	Server	Evaluator
t reference template	$\mathtt{ssk} \in \mathcal{K}$	$k \in \mathcal{K}$
$\mathtt{id}$ verified identity	$\mathtt{spk} \in \mathcal{P}$	

$(f, V) \leftarrow \mathtt{lock}(t)$
$(B, r) \leftarrow \mathtt{blind}(f)$

B → (Server) → B → (Evaluator)

$S \leftarrow \mathtt{eval}(B, k)$

(Evaluator) S → (Server) S →

$\mathtt{csk}_t \leftarrow \mathtt{unblind}(S, r)$
$\mathtt{cpk}_t \leftarrow \mathtt{pkGen}(\mathtt{csk}_t)$

$V, \mathtt{cpk}_t, \mathtt{id}$ →

store
$(V, \mathtt{cpk}_t, \mathtt{id})$

FIGURE 2. BRAKE enrolment protocol.

Verification

Client	Server	Evaluator
t' probe feature vector	$\mathtt{ssk} \in \mathcal{K}$	$k \in \mathcal{K}$
server public key $\mathtt{spk} \in \mathcal{P}$	$\mathtt{spk} \in \mathcal{P}$	
biometric claim $\mathtt{id}$	$(V, \mathtt{cpk}_t, \mathtt{id})$	

$\mathtt{id}$ →
← V

$f' \leftarrow \mathtt{unlock}(V, t')$
$(B', r') \leftarrow \mathtt{blind}(f')$
$(\mathtt{csk}_e, \mathtt{cpk}_e) \leftarrow \mathtt{KeyGen}(1^\lambda)$

$(\mathtt{ssk}_e, \mathtt{spk}_e) \leftarrow \mathtt{KeyGen}(1^\lambda)$

$B', \mathtt{cpk}_e$ → (Server) B' → (Evaluator)

$(\mathtt{ctx}, \gamma) \leftarrow \mathtt{encap}(\mathtt{cpk}_t)$
$\rho \leftarrow \mathtt{KDF}(\mathtt{cpk}_t, \mathtt{spk}, \mathtt{cpk}_e, \mathtt{spk}_e, \gamma)$

$S' \leftarrow \mathtt{eval}(B', k)$

(Evaluator) S' → (Server) $S', \mathtt{spk}_e, \mathtt{ctx}, H(\rho)$ →

$\mathtt{csk}_{t'} \leftarrow \mathtt{unblind}(S', r')$
$\mathtt{cpk}_{t'} \leftarrow \mathtt{pkGen}(\mathtt{csk}_{t'})$
$\gamma' \leftarrow \mathtt{decap}(\mathtt{ctx}, \mathtt{csk}_{t'})$
$\rho' \leftarrow \mathtt{KDF}(\mathtt{cpk}_{t'}, \mathtt{spk}, \mathtt{cpk}_e, \mathtt{spk}_e, \gamma')$
return $H(\rho') = H(\rho)$

FIGURE 3. BRAKE verification protocol.

in the case where t and t' are closer than threshold τ. Finally, the session key ρ is derived from γ using the client and server static and ephemeral public keys $\mathtt{cpk}$, $\mathtt{spk}$, $\mathtt{cpk}_e$, $\mathtt{spk}_e$ in the key derivation function $\mathtt{KDF}$. We note that the hashed session key ρ allows for the authentication to be explicit.

D. SECURITY DEFINITIONS

Following the definition of the BRAKE protocol in Figures 2 and 3, we give formal definitions of the security of the protocol. For simplicity, we implicitly model the use of identifiers within the enrolment database. In theory,

an adversary wants to learn a biometric feature vector that is close to any enrolled template. In practice however, it always needs to choose a specific identity to attack or run attacks on multiple specific identities in parallel. The following definitions and proof sketches model security in the case where a template t is enrolled in the database held by the server, and an honest client would use a feature vector t' to authenticate.

Notation. Denote by $f^{-1} = \log_2(FMR^{-1})$ the false-accept security of a biometric feature extractor and comparator, let ℓ be the rate limit enforced by the server and the evaluator, and let $\ell_{\mathcal{A}}$ be the brute-force capacity of the attacker $\mathcal{A}$.

Definition 10: **(Correctness)** We say that a BRAKE protocol is correct if a capture subject presenting a biometric probe feature vector t' and identifier id can successfully authenticate to an honest server if and only if $|t \cap t'| \geq \tau$ for a fixed biometric verification threshold τ, except with negligible probability.

Definition 11: **(Client Privacy)** We say that a BRAKE protocol has client privacy if an adversary $\mathcal{A}$ controlling the client has the following advantage in obtaining a biometric feature vector t' that is close to an enrolled biometric template t:

$$\Pr\left[\begin{array}{c}\texttt{dist}(t,t') < \tau \\ \forall i \in [\ell]: \end{array}\begin{array}{c}\texttt{pp} \leftarrow \texttt{setup}(1^\lambda) \\ \{V, \texttt{cpk}_t\} \leftarrow \texttt{enroll}(\texttt{pp}, t) \\ \begin{cases}(B', \texttt{cpk}_e) \leftarrow \mathcal{A}(\texttt{pp}, V) \\ (\texttt{ssk}_e, \texttt{spk}_e) \leftarrow \texttt{KeyGen}(1^\lambda) \\ S' \leftarrow \texttt{eval}(B', k)\end{cases} \\ t' \leftarrow \mathcal{A}(S', \texttt{spk}, \texttt{spk}_e, \texttt{ctx})\end{array}\right] \leq \ell f^{-1} + \mathsf{negl}(\lambda).$$

Definition 12: **(Server Privacy)** We say that a BRAKE protocol has server privacy if an adversary $\mathcal{A}$ controlling the computation server has the following advantage in obtaining a biometric feature vector t' that is close to an enrolled biometric template t:

$$\Pr\left[\begin{array}{c}\texttt{dist}(t,t') < \tau : \\ \end{array}\begin{array}{c}\texttt{pp} \leftarrow \texttt{setup}(1^\lambda) \\ \{V, \texttt{cpk}_t\} \leftarrow \texttt{enroll}(\texttt{pp}, t) \\ \forall i \in [\ell]: \begin{cases}B' \leftarrow \mathcal{A}(\texttt{pp}, \{V, \texttt{cpk}_t\}) \\ S' \leftarrow \texttt{eval}(B', k)\end{cases} \\ t' \leftarrow \mathcal{A}(S')\end{array}\right] \leq \ell f^{-1} + \mathsf{negl}(\lambda).$$

If client and server run the protocol BRAKE honestly, the evaluator only sees the blinded element, which is information-theoretically secure, and hence, independent of the biometric template. We therefore do not model evaluator privacy.

The advantage of an adversary controlling both the client and the server effectively reduces to server privacy. In this scenario, the information the adversary needs to guess is the evaluated element S'. However, as discussed above, the evaluator cannot distinguish between evaluation requests for different biometric feature vectors corresponding to mated authentication attempts, or repeated evaluation requests for a single identity aimed at running a brute-force search. Therefore, rate-limiting at the evaluator can be enforced by user-specific OPRF keys. This way, the evaluator will learn the identifier of the user attempting to authenticate, but is not able to gain any more knowledge about her biometric data, while effectively preventing the server from learning it.

The advantage of an adversary controlling both the client and the evaluator initially reduces to the definition of client privacy, as the adversary seeks to learn the reference public key stored during enrolment. However, after running one (unsuccessful) authentication attempt for a specific identity, the adversary will receive the encapsulated key derived from the biometric reference data of the data subject in question. From that point on, it can guess a biometric feature vector, issue an evaluation by use of the evaluation key, and compare the resulting key against the obtained one. Therefore, we realistically model an adversary controlling both the client and the evaluator as being able to run an offline search on the biometric enrolment database. Due to the architecture considerations, this scenario is somewhat unlikely in practice, and a more realistic threat is the server and evaluator colluding.

Definition 13: **(Client-Evaluator Privacy)** We say that a BRAKE protocol has client-evaluator privacy if an adversary $\mathcal{A}$ controlling both the client and the authentication server does not have an advantage in obtaining a biometric feature vector t' that is close to any enrolled biometric template t above running a brute-force search on V:

$$\Pr\left[\begin{array}{c}\texttt{dist}(t,t') < \tau : \\ \end{array}\begin{array}{c}\texttt{pp} \leftarrow \texttt{setup}(1^\lambda) \\ \{V, \texttt{cpk}_t\} \leftarrow \texttt{enroll}(\texttt{pp}, t) \\ \forall i \in [\ell]: \begin{cases}(B', \texttt{cpk}_e) \leftarrow \mathcal{A}(\texttt{pp}, \texttt{id}, V) \\ (\texttt{ssk}_e, \texttt{spk}_e) \leftarrow \texttt{KeyGen}(1^\lambda) \\ S' \leftarrow \mathcal{A}(B', k) \\ \texttt{ctx} \leftarrow \texttt{encap}(\rho, \texttt{cpk}_t)\end{cases} \\ t' \leftarrow \mathcal{A}(S', \texttt{spk}, \texttt{spk}_e, \texttt{ctx})\end{array}\right] \leq \ell_{\mathcal{A}} f^{-1} + \mathsf{negl}(\lambda).$$

Definition 14: **(Server-Evaluator Privacy)** We say that a BRAKE protocol has server-evaluator privacy if an adversary $\mathcal{A}$ controlling both the server and the evaluator does not have an advantage in obtaining a biometric feature vector t' that is close to any enrolled biometric template t above running a brute-force search on V:

$$\Pr\left[\begin{array}{c}\texttt{dist}(t,t') < \tau : \\ \end{array}\begin{array}{c}\texttt{pp} \leftarrow \texttt{setup}(1^\lambda) \\ \{V, \texttt{cpk}_t\} \leftarrow \texttt{enroll}(\texttt{pp}, t) \\ f' \leftarrow \texttt{unlock}(V, t') \\ B' \leftarrow \texttt{blind}(f') \\ (\texttt{csk}_e, \texttt{cpk}_e) \leftarrow \texttt{KeyGen}(1^\lambda) \\ t' \leftarrow \mathcal{A}(\texttt{pp}, \texttt{id}, V, B', k, \texttt{cpk}_t, \texttt{cpk}_e)\end{array}\right] \leq \ell_{\mathcal{A}} f^{-1} + \mathsf{negl}(\lambda).$$

IV. CONCRETE INSTANTIATIONS

We now give two concrete instantiations of BRAKE, where the first is based on the hardness of discrete logarithms, while the second utilises lattice-based cryptography. Thereby, we show that both classical security and post-quantum security can be achieved using BRAKE. For both instantiations, the modified improved fuzzy vault scheme described in Section III-B is used. The detailed description of the instantiations includes their cryptographic building blocks, complete instantiated protocols, and security proofs.

A. INSTANTIATION BASED ON DISCRETE LOGARITHMS

In this Section, we give an instantiation of the protocol defined in Figures 2 and 3 using cryptographic primitives that build on the security of discrete logarithms (DL). Concretely, we instantiate the universe $\mathcal{P}$ with a cyclic group $\mathbb{G}$, which can be the group of points on an elliptic curve, and the key

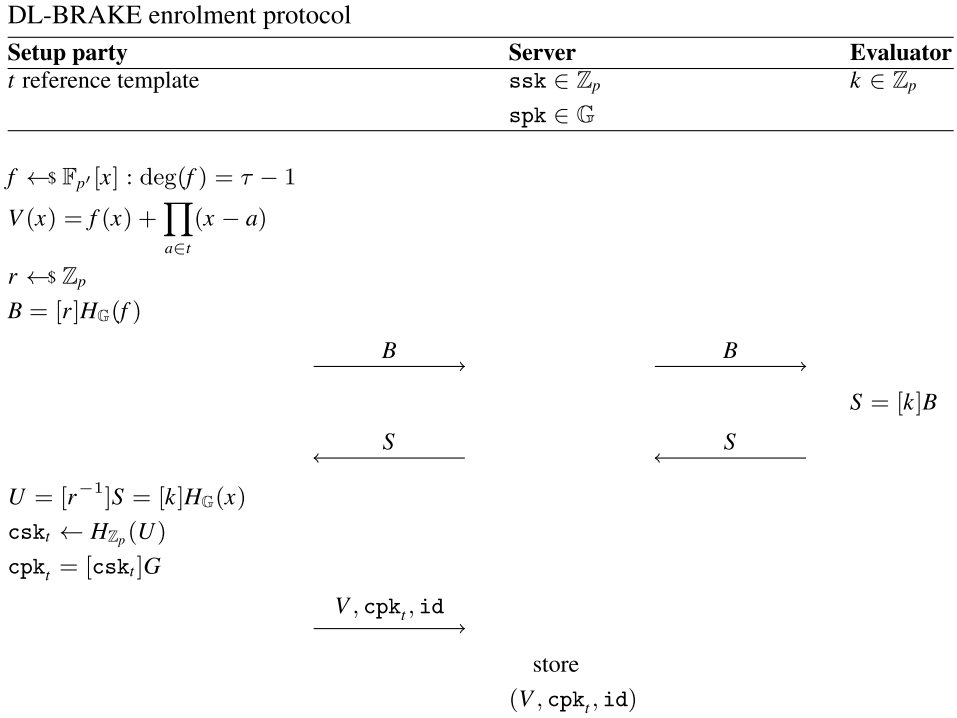


FIGURE 4. DL-BRAKE enrolment protocol instantiated with discrete-logarithm OPRF and Diffie-Hellman key exchange.

space $\mathcal{K}$ and randomness space $\mathcal{R}$ with a scalar field $\mathbb{Z}_p$, where p is the prime order of $\mathbb{G}$. Further, we also define two hash functions $H_{\mathbb{G}} : \{0,1\}^* \to \mathbb{G}$ and $H_{\mathbb{Z}_p} : \{0,1\}^* \to \mathbb{Z}_p$.

Building on these foundations, the respective algorithms of Definition 9 are instantiated with the Hash-DH OPRF defined in Definition 4 and ephemeral Diffie-Hellman key exchange with a key-derivation function KDF. The detailed protocols for enrolment and verification are defined in Figures 4 and 5, respectively. In the following, we refer to the verification protocol in Figure 5 as DL-BRAKE. We note that in the setting where the evaluator rate-limits the number of evaluations per user, the protocol can trivially be updated to send the identity of the user (or a fixed pseudonym) together with the blinded value, and the evaluator evaluates a partially oblivious PRF where the identity is a public input to the function together with the secret evaluation key. Implementing the techniques from [53] and [54] allows us to perform this slightly different evaluation without (noticeable) increased computation nor communication compared to the protocol we have described.

B. DL-BRAKE SECURITY PROOFS

In this Section, we provide theorems stating the security of the DL-BRAKE based on the hardness of discrete logarithms, and we sketch the security proofs.

Theorem 1 (Correctness): Assume that a probe sample t' is within the verification threshold τ compared to a biometric template $t_{\mathtt{id}}$ for some registered identity id. Then the DL-BRAKE protocol in Figure 5 is correct.

Proof sketch: This follows directly from the construction. If the comparison result of the probe feature set t' to a biometric template $t_{\mathtt{id}}$ is within the verification threshold τ for some registered identity id, then the client will successfully reconstruct the correct polynomial f' using interpolation. From the correctness of the OPRF, the KEM, and the KDF, we then conclude that the client and the server compute the same values, and the data subject is correctly authorised. If the distance between probe and reference feature set is more than τ points, by correctness of Lagrange interpolation, two different polynomials will be reconstructed, and, but for a collision in the hash function, the key exchange will fail. □

Theorem 2 (Client Privacy): Let $\mathcal{A}_0$ be an adversary against *client privacy* in the DL-BRAKE protocol in Figure 5 with advantage ϵ_0. Then there exists an adversary $\mathcal{A}_1$ against the fuzzy vault V with advantage ϵ_1 and an adversary $\mathcal{A}_2$ against the OPRF with advantage ϵ_2, such that $\epsilon_0 \leq \epsilon_1 + f^{-1}(1+\epsilon_2)$. The runtime of $\mathcal{A}_0$ is essentially the same as of $\mathcal{A}_1$ and $\mathcal{A}_2$.

Proof sketch: We consider a single log-in attempt by an adversary $\mathcal{A}_0$ controlling the client. If $\mathcal{A}_0$ guesses a biometric probe, the probability that this probe is close to the reference sample is approximately f^{-1}. Furthermore, if $\mathcal{A}_0$ with probability ϵ_0 can output a valid probe sample t' given access to the fuzzy vault V, we can trivially turn $\mathcal{A}_0$ into an adversary $\mathcal{A}_1$ against V with the same advantage. Moreover, if $\mathcal{A}_0$ with advantage f^{-1} can output a valid probe sample t' when having access to values evaluated with

DL-BRAKE verification protocol

Client	Server	Evaluator
t' probe feature vector	$\mathtt{ssk} \in \mathbb{Z}_p$	$k \in \mathbb{Z}_p$
$\mathtt{spk} \in \mathbb{G}$	$\mathtt{spk} \in \mathbb{G}$	
	$(V, \mathtt{cpk}_t, \mathtt{id})$	

$\xrightarrow{\mathtt{id}}$

$\xleftarrow{V}$

find $\{(b, V(b)) : b \in t'\}$
and decode to $f' \in \mathbb{F}_{p'}[x]$
$r' \leftarrow\!\!\$\ \mathbb{Z}_p$
$B' = [r']H_{\mathbb{G}}(f')$
$\mathtt{csk}_e \leftarrow\!\!\$\ \mathbb{Z}_p$
$\mathtt{cpk}_e = [\mathtt{csk}_e]G$

$\mathtt{ssk}_e \leftarrow\!\!\$\ \mathbb{Z}_p$
$\mathtt{spk}_e = [\mathtt{ssk}_e]G$

$\xrightarrow{B', \mathtt{cpk}_e}$ $\xrightarrow{B'}$

$\rho \leftarrow \mathtt{KDF}([\mathtt{ssk}_e]\mathtt{cpk}_e,$ $S' = [k]B'$
$[\mathtt{ssk}]\mathtt{cpk}_e, [\mathtt{ssk}_e]\mathtt{cpk}_t,$
$\mathtt{cpk}_e, \mathtt{spk}_e, \mathtt{cpk}_t, \mathtt{spk})$

$\xleftarrow{S', \mathtt{spk}_e, H(\rho)}$ $\xleftarrow{S'}$

$U' = [r'^{-1}]S' = [k]H_{\mathbb{G}}(x')$
$\mathtt{csk}_{t'} \leftarrow H_{\mathbb{Z}_p}(U')$
$\mathtt{cpk}_{t'} = [\mathtt{csk}_{t'}]G$
$\rho' \leftarrow \mathtt{KDF}([\mathtt{csk}_e]\mathtt{spk}_e,$
$[\mathtt{csk}_e]\mathtt{spk}, [\mathtt{csk}_{t'}]\mathtt{spk}_e,$
$\mathtt{cpk}_e, \mathtt{spk}_e, \mathtt{cpk}_{t'}, \mathtt{spk})$
return $H(\rho') = H(\rho)$

FIGURE 5. DL-BRAKE verification protocol instantiated with discrete-logarithm OPRF and Diffie-Hellman key exchange.

key k, then we can turn $\mathcal{A}_0$ into an adversary $\mathcal{A}_2$ against the OPRF. Finally, we observe that the KEM are independent of $t_{\mathtt{id}}$, and hence, an adversary $\mathcal{A}_0$ cannot learn anything from interacting with this protocol. We conclude that the protocol achieves client privacy. □

Theorem 3 (Server privacy): Let $\mathcal{A}_0$ be an adversary against server privacy in the DL-BRAKE protocol in Figure 5 with advantage ϵ_0. Then there exists an adversary $\mathcal{A}_1$ against the fuzzy vault V with advantage ϵ_1 and an adversary $\mathcal{A}_2$ against the OPRF with advantage ϵ_2, such that $\epsilon_0 \leq \epsilon_1 + f^{-1}(1+\epsilon_2)$. The runtime of $\mathcal{A}_0$ is essentially the same as of $\mathcal{A}_1$ and $\mathcal{A}_2$.

We omit the proof of Theorem 3 since it is similar to Theorem 2.

Theorem 4 (Client-Evaluator Privacy): Let $\mathcal{A}_0$ be an adversary against client-evaluator privacy in the DL-BRAKE protocol in Figure 5 with advantage ϵ_0 controlling both the client and the evaluator. Then $\epsilon_0 \leq f^{-1}$ and $\mathcal{A}_0$ has no advantage in guessing a biometric probe within the threshold of an enrolled template above a brute-force search.

Proof sketch: We consider a colluding malicious client and malicious evaluator. Assume that $\mathcal{A}_0$ runs the verification protocol once on any input probe t' and receives $(S', \mathtt{spk}_e, H(\rho))$ from the server. Then $\mathcal{A}_0$ can guess a biometric probe, interpolate to get a polynomial f' and execute the OPRF on input f' using the evaluator's key k. For each guess, $\mathcal{A}_0$ can check if the KDF output corresponds to $H(\rho)$. No information about any enrolled template $t_{\mathtt{id}}$ is encoded in the messages from the server. □

Theorem 5 (Server-Evaluator Privacy): Let $\mathcal{A}_0$ be an adversary against server-evaluator privacy in the DL-BRAKE protocol in Figure 5 with advantage ϵ_0 controlling both the server and the evaluator. Then $\epsilon_0 \leq f^{-1}$ and $\mathcal{A}_0$ has no advantage in guessing a biometric template within the threshold of an enrolled template above a brute-force search.

Proof sketch: We consider a colluding malicious server and malicious evaluator. Then $\mathcal{A}_0$ can guess a biometric probe, interpolate to get a polynomial f' and execute the OPRF on input f' using the evaluator's key k. For each guess, $\mathcal{A}_0$ can check if $[H_{\mathbb{Z}_p}(B')]G = \mathtt{cpk}_r$. No information about

any enrolled template $t_{\mathtt{id}}$ is encoded in the messages from the client. □

C. INSTANTIATION BASED ON LATTICES

Our BRAKE protocol can also be instantiated with lattice-based cryptographic primitives, which are assumed to yield post-quantum security for certain parameter choices [55]. Two components in the protocol need to be instantiated: the OPRF and the KEM.

A construction of a lattice-based OPRF has recently been proposed by [12], which builds on the security of the M-LWE problem defined in Section II-E for $d = 1$ (often referred to as the Ring-Learning With Errors (R-LWE) problem [56]). Additionally, this specific construction has the additional property of being *verifiable* (making it a VOPRF), i.e., the client has a guarantee that the output received from the OPRF evaluation is truly correct and calculated with the server's publicly committed key k [12], [44].

However, the zero-knowledge proof appended to the lattice-based PRF for verifiability are not practical for real-world application due to proof sizes of several gigabytes [12]. The authors of [12] give a rough indication of the amounts in question at approximately 2^{40} bits or around 128 GB of communication data for realistic parameter choices of $\log_2(q) \approx 256$ and ring dimension 16384. Therefore, we only look at the case of passive security against dishonest clients for the lattice instantiation, which can be significantly simplified by replacing the PRF with a hash function. We will give a detailed description of the modifications applied to the lattice-based VOPRF by [12] in the following.

1) LATTICE OPRF

An option that is made possible by removing the zero-knowledge proofs is the ability to heavily reduce the computation time and communication cost generated by the PRF. Originally, the PRF is evaluated as

$$F_k(x) := \lfloor a_x \cdot k \rceil_{q'} \in R_{q'}^{d'},$$

where a_x is a lattice PRF [57]. This evaluation can be replaced with the PRF $F'_k(x) := \lfloor a_x \cdot k \rceil_{q'}$ where a_x a pseudorandom ring element output by a hash function evaluated on some secret input x. This truncation shrinks the calculations from a vector of polynomials to just single polynomials in $R_{q'}$.

In practical terms, the input a_x we wish to evaluate the OPRF on, is the random polynomial f generated by the fuzzy vault scheme. Therefore, the element f needs to be mapped to a ring element in a deterministic fashion. The procedure is described in the following steps:

1) Concatenate every coefficient of f into a string cf.
2) Create $h := H(cf)$ using a cryptographic hash function.
3) Produce N coefficients of the polynomial a_x by creating a hash of the form $h_i := H(i\|h)$ for $i = 0, \ldots, N-1$ using the same hash function as before and converting hashes into integers. Here, $\|$ denotes concatenation.

Modified lattice OPRF protocol

Client		Evaluator
$a \leftarrow\$ R_q$		
		$k \leftarrow D_\sigma(R_q)$
		$e \leftarrow D_\sigma(R_q)$
		$c := a \cdot k + e$
	$\xleftarrow{c}$	
store(c)		
$s \leftarrow D_\sigma(R_q)$		
$e' \leftarrow D_\sigma(R_q)$		
$a_x := H(x)$		
$c_x := a \cdot s + e' + a_x$		
	$\xrightarrow{c_x}$	
		$E \leftarrow D_{\sigma'}(R_q)$
		$d_x := c_x \cdot k + E$
	$\xleftarrow{d_x}$	
$y_x := \lfloor d_x - c \cdot s \rceil_{q'}$		
output(y_x)		

FIGURE 6. Modified OPRF protocol based on [12] using the truncated PRF.

4) Reduce the coefficients of a_x mod q (if needed).

This procedure results in a polynomial a_x which is an element of the ring $R_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle$ and can subsequently be used to compute an M-LWE sample. Using the truncated PRF described above, the lattice-based OPRF construction by Albrecht et al. [12] can be modified as will be described in the following Section. Figure 6 shows the functioning of the modified OPRF, using the truncated PRF, in more detail. Here, D_σ is a uniform distribution over R_q which produces ternary values, and $D_{\sigma'}$ is a uniform distribution over R_q which produces values in a range $[-B, B]$, where B is a large power of two smaller than q.

The final step, *rounding*, produces the Client's output, which is the polynomial y_x. If the rounding is implemented correctly and the protocol has been successfully executed, this rounded value will be equal to the rounded value $\lfloor a_x \cdot k \rceil_{q'}$. This is known as the unblinding operation, which allows the Client to receive the computation of $a_x \cdot k$ without learning the Evaluator's key k, while the Evaluator does not learn the value of a_x. Additionally, before rounding, it is necessary to represent the values that are to be rounded in $(-\frac{q-1}{2}, \ldots, \frac{q-1}{2})$.

The principle behind the validity of the rounding mechanism is shown in the following equations based on [12], which depict the total amount of noise that is accrued through the protocol. Firstly, we introduce the M-LWE samples c, d_x and c_x, which form the total noise value. These are elements of R_q and are transmitted between the Client and Evaluator during the protocol. We recall their definitions as given in Figure 6:

$$\begin{aligned} c &= a \cdot k + e \\ d_x &= c_x \cdot k + E \\ c_x &= a \cdot s + e' + a_x. \end{aligned}$$

PQ-BRAKE enrolment protocol

Client	Server	Evaluator
t reference template	$\mathtt{ssk} \in \mathcal{K}$	$c \in R_q$
$\mathtt{id}$ verified identity	$\mathtt{spk} \in \mathcal{P}$	$k \in R_q$
$c \in R_q$		
$(f, V) \leftarrow \mathtt{lock}(t)$		
$s \leftarrow D_\sigma(R_q)$		
$e' \leftarrow D_\sigma(R_q)$		
$a_x := H(f)$		
$c_x := a \cdot s + e' + a_x$		
$\xrightarrow{c_x}$	$\xrightarrow{c_x}$	
		$E \leftarrow D_{\sigma'}(R_q)$
		$d_x := c_x \cdot k + E$
$\xleftarrow{d_x}$	$\xleftarrow{d_x}$	
$y_x := \lfloor d_x - c \cdot s \rceil_{q'}$		
$\mathtt{csk}_t \leftarrow \mathtt{ExpKDF}(y_x)$		
$\mathtt{cpk}_t \leftarrow \mathtt{pkGen}(\mathtt{csk}_t)$		
$\xrightarrow{V, \mathtt{cpk}_t, \mathtt{id}}$		
	store $(V, \mathtt{cpk}_t, \mathtt{id})$	

FIGURE 7. PQ-BRAKE enrolment protocol instantiated with modified lattice OPRF and Kyber KEM.

Next, we recall the computation of the polynomial y on the Client's side, which includes the values d_x, c and s before they are summed and rounded in y_x:

$$\begin{aligned} y &= d_x - c \cdot s \\ &= c_x \cdot k + E - (a \cdot k + e) \cdot s \\ &= (a \cdot s + e' + a_x) \cdot k + E - a \cdot k \cdot s + e \cdot s \\ &= e' \cdot k + a_x \cdot k + E - e \cdot s. \end{aligned}$$

Then, as the polynomial y_x can be obtained from y as:

$$y_x = \left\lfloor \frac{q'}{q} \cdot (d_x - c \cdot s) \right\rceil = \left\lfloor \frac{q'}{q} \cdot a_x \cdot k \right\rceil.$$

In the expanded equation for y, we notice that it contains the polynomial $a_x \cdot k$ and a noise polynomial $e' \cdot k - e \cdot s + E$. Therefore, the last equation, showing the value of y_x, is correct with all but a negligible probability if the noise polynomial $\left| \frac{q'}{q} \cdot (e' \cdot k - e \cdot s + E) \right|$ is small enough for each coefficient to achieve acceptable correctness after rounding. In other words:

$$\left| \frac{q'}{q} \cdot (e' \cdot k - e \cdot s + E) \right|_\infty < \frac{1}{2}.$$

2) CRYSTALS KYBER KEY ENCAPSULATION MECHANISM

We exchange the Diffie-Hellman key exchange with a lattice-based KEM: the recently standardised CRYSTALS-Kyber [13]. Kyber is based on the M-LWE problem described in Section II-E and provides IND-CCA2 security [58]. The main parameters of Kyber, $N = 256$ and $q = 3329$, were specifically chosen for the ability to use the Number Theoretic Transform (NTT) providing an efficient way to perform multiplications in R_q [58]. In our work, the parameter set of Kyber768 was chosen due to its optimal performance while providing more than 128 bits of security [58]. While no significant changes were applied to Kyber on a theoretical basis, we give further details on the integration of Kyber into the implementation of the BRAKE protocol in Section V. In particular, we note that the security of the session key established through BRAKE is given through the security guarantees of Kyber.

3) PQ-BRAKE

Combining the introduced modified lattice OPRF and the Kyber KEM, we can define the PQ-BRAKE protocol as described in Figures 7 and 8.

D. PQ-BRAKE SECURITY PROOFS

The security proofs for PQ-BRAKE follow directly from the proofs given for the DL-BRAKE instantiation given in Section IV-B through the hardness of M-LWE and M-SIS.

E. IMPROVED SECURITY USING NIZK

The protocol can be further secured by the addition of non-interactive zero-knowledge proofs (NIZKs) using the established construction by Chaum and Pedersen [59] together with a Fiat-Shamir transform [60]. The NIZK is added to prove the honest evaluation of the OPRF. Thereby, a client can verify that the evaluator computed the evaluation

PQ-BRAKE verification protocol

Client		Server		Evaluator
t' probe feature vector		$\mathtt{ssk} \in \mathcal{K}$		$c \in R_q$
$\mathtt{spk} \in \mathcal{P}$		$\mathtt{spk} \in \mathcal{P}$		$k \in R_q$
biometric claim $\mathtt{id}$		$(V, \mathtt{cpk}_t, \mathtt{id})$		
$c \in R_q$				
	$\xrightarrow{\mathtt{id}}$			
	$\xleftarrow{V}$			
$f' \leftarrow \mathtt{unlock}(V, t')$				
$(\mathtt{csk}_e, \mathtt{cpk}_e) \leftarrow \mathtt{KeyGen}()$		$(\mathtt{ssk}_e, \mathtt{spk}_e) \leftarrow \mathtt{KeyGen}()$		
$s \leftarrow D_\sigma(R_q)$				
$e' \leftarrow D_\sigma(R_q)$				
$a_x := H(f')$				
$c_x := a \cdot s + e' + a_x$				
	$\xrightarrow{c_x, \mathtt{cpk}_e}$		$\xrightarrow{c_x}$	
		$(\mathtt{ctx}, \gamma) \leftarrow \mathtt{encap}(\mathtt{cpk}_t)$		$E \leftarrow D_{\sigma'}(R_q)$
		$\rho \leftarrow \mathtt{KDF}(\mathtt{cpk}_t, \mathtt{cpk}_e,$		$d_x := c_x \cdot k + E$
		$\mathtt{spk}, \mathtt{spk}_e, \gamma)$		
	$\xleftarrow[\mathtt{spk}_e, ctx]{d_x, H(\rho)}$		$\xleftarrow{d_x}$	
$y_x := \lfloor d_x - c \cdot s \rceil_{q'}$				
$\mathtt{csk}_{t'} \leftarrow \mathtt{ExpKDF}(y_x)$				
$\mathtt{cpk}_{t'} \leftarrow \mathtt{pkGen}(\mathtt{csk}_{t'})$				
$\gamma' \leftarrow \mathtt{decap}(\mathtt{ctx}, \mathtt{csk}_{t'})$				
$\rho' \leftarrow \mathtt{KDF}(\mathtt{cpk}_{t'}, \mathtt{cpk}_e,$				
$\mathtt{spk}, \mathtt{spk}_e, \gamma')$				
return $H(\rho') = H(\rho)$				

FIGURE 8. PQ-BRAKE verification protocol instantiated with modified lattice OPRF and Kyber KEM.

honestly. In the case of an unsuccessful authentication attempt, the client therefore gains more knowledge about the reason of failure, and can potentially reveal a corrupted evaluator. We note that above this additional information, the passively secure protocol already allows for the protection of the biometric data even in the presence of malicious adversaries, as long as at least one of the parties remains honest as given by the security definitions above. However, in the lattice-based instantiation, a malicious client may be able to learn the OPRF key, facilitating a similar attack as in the case of a colluding client and signer. Therefore, the lattice-based instantiation can only be considered in the semi-honest adversary model.

V. EXPERIMENTAL EVALUATION

We evaluated our protocol instantiated with elliptic curves presented in Figure 5 and lattices presented in Figure 8 experimentally and show the results in this Section. Our experiments were run on a commodity notebook with Intel Core i7-8565U CPU@1.80GHz and 8GB RAM. Our code is available at https://github.com/dasec/DL-BRAKE and https://github.com/dasec/PQ-BRAKE and includes automated installation scripts with all dependencies in order to support the reproducibility of our work.

To begin, we give a more detailed comparison of our work with closely related work in Table 2 by extending Table 1 in [7] with our protocol. In terms of round efficiency, our protocol compares well to [9] and [10] with two rounds of communication. In order to prevent offline attacks, a minimum number of two rounds of communication is necessary. Therefore, [9] and [10], and our protocol can be considered optimal in terms of number of rounds. As [7] constructed a one-round protocol, this leaves them open to offline attacks. In terms of the protection of the biometric data compliant with ISO/IEC 24745 [6], our protocol is the only compliant one: we inherit unlinkability, renewability, and irreversibility from the fuzzy vault schemes. Moreover, we show that our protocol is efficient in terms of execution times given in Table 3 and as well as in terms of biometric performance shown in Figure 9. In comparison,

TABLE 2. Summary of our protocol compared to previous published protocols as described in Table 1 of [7].

Scheme	Technique	Rounds	Communication Cost	Compatibility	ISO/IEC 24745 [6]
fPAKE-1 [9]	Garbled Circuits	5	N/A	iris, fixed-length fingerprint	✗
fPAKE-2 [9]	PAKE + Secret Sharing	2	N/A		✗
fuzzy aPAKE-1 [10]	ECC + OT	2	∼ 700 KB		✗
fuzzy aPAKE-2 [10]	Generic k-parallel aPAKE	2	∼ 1 MB		✗
BAKE-1 [7]	Random Linear Codes	1	5-8.4 KB	minutiae-based fingerprint	✗
BAKE-2 [7]	Secret Sharing + Polynomial Interpolation	1	1.7-96.6 KB	iris	✗
iPAKE [15]	ECC + PAKE	1	N/A	iris, fixed-length fingerprint	✗
DL-BRAKE (ours)	Fuzzy Vault + DL-OPRF + DL-KEM	2	0.3 KB	minutiae-based fingerprint, iris, face	✓
PQ-BRAKE (ours)	Fuzzy Vault + lattice OPRF + lattice KEM	2	60.2 KB	minutiae-based fingerprint, iris, face	✓

fPAKE [9] does not achieve irreversibility as templates are disclosed to the server in plaintext, fuzzy aPAKE [10] does not achieve computational efficiency, and [7] does not achieve an acceptable biometric performance, as we show in Appendix A.

A. FUZZY VAULT IMPLEMENTATION

For the fingerprint fuzzy vault instantiation, we used the open-source implementation provided by [38] with all original parameter settings, in particular, the minutiae quantisation and encoding into a product of finite field $\mathbb{F}_{2^{18}} \times \mathbb{F}_{2^{18}}$ which accommodates a unique encoding of at most $t_{max} = 44$ genuine minutiae as described in [38]. Keeping the parameter choices evaluated in the work of [38] ensures perfect replaceability with other state-of-the-art fuzzy vault instantiations, such as [42] for iris and [43] for face. In particular, we run our implementation on the same fingerprint database MCYT-330 [61] and same feature extractor, Digital Persona's FingerJetFX open source edition minutiae extractor.[1] This means that all evaluations of biometric performance can be compared directly to the original paper of [38] and papers that compare their work with the latter [42], [43].

The only modification applied to the implementation of [38] is in the unlocking function. Here, [38] use the stored hash $H(f)$ of the secret polynomial f corresponding to a reference template t, which allows for offline brute force attacks. Our protocol prevents offline attacks by removing the hash and using highest-frequency decoding in its place (see Section III-B). As discussed above, this does not impact the security in terms of the false-match rate of our protocol.

B. DL-BRAKE IMPLEMENTATION

Our implementation of the OPRF and Diffie-Hellman key exchange is based on OpenSSL. For all cryptographic operations, we used P-256 [62] as the elliptic curve and SHA-256 as the hash function.

[1] http://www.digitalpersona.com/fingerjetfx

TABLE 3. Execution times in milliseconds for the DL-BRAKE and PQ-BRAKE protocols using the fingerprint fuzzy vault by [38].

	Polynomial degree $\tau - 1$					
	6	8	10	12	14	16
Feature extraction and preprocessing	200.59					
`lock`	2.38					
`unlock`	112.24	185.99	276.37	385.26	511.91	694.87
`DL-OPRF`	0.21					
`PQ-OPRF`	31.81					
`DL-KeyGen`	0.05					
`PQ-KeyGen`	0.21					
`DL-encap`	0.16					
`PQ-encap`	0.08					
`DL-decap`	0.15					
`PQ-decap`	0.03					
DL-Verification (Figure 5)	313.4	387.15	477.53	586.42	713.07	896.03
PQ-Verification (Figure 8)	347.34	421.09	511.91	620.36	747.01	929.97
FMR (%)	1.04%	0.04%	0.00%	0.00%	0.04%	0.09%
1− FNMR (%)	92.88%	88.79%	81.97%	73.18%	60.45%	44.09%
Estimated security in bits based on [38]	17	23	29	36	44	—

TABLE 4. Communication cost for DL-BRAKE and PQ-BRAKE.

	DL-BRAKE	PQ-BRAKE
Locked fuzzy vault	99 B	
OPRF	128 B	114 KB
KEM	64 B	4672 B
Hash digest	32 B	
Total	0.3 KB	60.2 KB

Regarding the computational performance and recognition accuracy of our protocol, we give timings for increasing polynomial degrees $\tau - 1$ in Table 3, where τ is the biometric

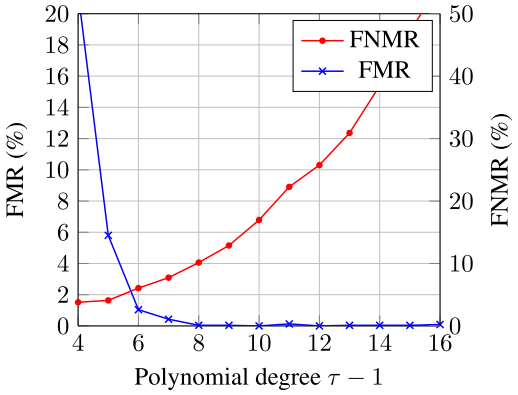


FIGURE 9. Biometric performance for the DL-BRAKE protocol instantiated with fingerprint fuzzy vault [38].

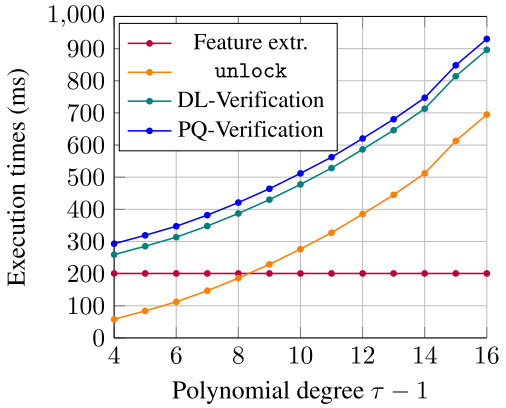


FIGURE 10. Execution times in milliseconds for the DL-BRAKE and PQ-BRAKE protocols instantiated with fingerprint fuzzy vault [38].

decision threshold. At the same time, we give the biometric performance in FMR and FNMR along with the estimated false-accept security in bits as evaluated in [38]. As these security levels are derived from the FMR and our modified unlocking function does not impact the FMR, we are able to refer to the evaluation performed in [38] directly. For an acceptable recognition accuracy at $\tau - 1 = 8$, the execution of the protocol DL-BRAKE given in Figure 5 takes 387.15 milliseconds. To compare, the fastest setting reported in Table 2 in [7] also achieves 387 milliseconds, but at significantly lower accuracy (see Appendix A).

The execution times are dominated by the constant cost of feature extraction (200.59 milliseconds) and the cost for unlocking, which is dependent on the polynomial degree. We note that timing for the enrolment part of the protocol given in Figure 4 is 203.23 milliseconds, where feature extraction dominates compared to the locking at 2.38 milliseconds. However, the enrolment step is a one-time effort when setting up the system, and does not affect verification performance.

Accordingly, Figure 9 shows the trade-off between FMR and FNMR for our protocol. To conclude the efficiency evaluation of our protocol, we report that the communication cost of objects transferred between the parties during the verification step of the protocol is 32 bytes for any point on the elliptic curve P-256 [62] (i.e., $\texttt{cpk}_e$, $\texttt{spk}_e$, B' and S'), 99 bytes for a locked fuzzy vault of degree at most 43 and coefficients in $\mathbb{F}_{2^{18}}$, and 32 bytes for the hash digest.

C. PQ-BRAKE IMPLEMENTATION

For the lattice-based instantiation of our protocol, we utilised the OpenSSL implementation of the SHA-256 hash function, Open Quantum Safe's `liboqs` C library [63] through its C++ wrapper, `liboqscpp`, for the CRYSTALS Kyber [13] implementation. To support key generation from a designated input (i.e., the fuzzy vault secret polynomial f), we extended the C++ wrapper to include the functionalities required for BRAKE. The documentation can be found in our repository at https://github.com/dasec/PQ-BRAKE.

For the OPRF part of the protocol, parameter choice is crucial for both communication and computation complexity along with security, and needs to be carefully evaluated. We therefore tested our parameter validity using the established `lwe-estimator` [64]. As a result, we chose the parameters $N = 4096$, $q \approx 2^{75}$, and $B = 2^{53}$ with security of 188 bits. In comparison, the Kyber KEM is instantiated with $N = 256$ and $q = 3329$.

Using these parameters, it is also possible to calculate a probability of the rounding step failing, which would result in a decryption failure in practice, due to noise wrapping the value around $\mathbb{Z} + 1/2$ and causing a rounding to the wrong value. As demonstrated in Section IV-C1, the upper bound on the noise is given as: $2N + B \leq \frac{q}{4}$. We consider the probability of one coefficient of the output polynomial y_x being wrongly decrypted to be: $\frac{2N+B}{q}$, and its complement situation, the probability of no error occurring as $1 - \frac{2N+B}{q}$. With this in mind, we claim that the probability of at least one decryption error occurring during the rounding of N polynomial coefficients and thus the protocol failing in the OPRF step, to be

$$1 - \left(1 - \frac{2N + B}{q}\right)^N. \tag{1}$$

Applying this formula, we set the parameters so that the failure rate is significantly smaller than the false-accept security of the biometric component, i.e., the improved fuzzy vault scheme. A success rate of 99.9% was chosen for this benchmark.

The computational performance of the PQ-BRAKE protocol can be seen in Table 3. Compared to DL-BRAKE, the most significant change is the lattice-based OPRF, which has a significantly higher computational workload of 31.81 milliseconds compared to the classically secure OPRF at only 0.21 milliseconds. However, compared to the overwhelming cost of feature extraction, preprocessing, and the unlocking step of the fuzzy vault, the lattice OPRF cost can still be considered feasible. A visual comparison of the execution times for both the Dl-BRAKE and PQ-BRAKE

protocols as well as the fixed costs of feature extraction and the individual effort of the fuzzy vault unlocking step is given in Figure 10.

The communication cost for PQ-BRAKE can be determined as 99 bytes for a locked fuzzy vault as before, 114KB for the OPRF, covering a total of three R-LWE samples, a total of 4672 bytes for the Kyber key exchange, and 32 bytes for the has digest. A comparison of the communication cost for DL-BRAKE, PQ-BRAKE, and the original lattice VOPRF by Albrecht et al. [12] can be seen in Table 4.

VI. CONCLUSION

In this work, we constructed biometric resilient authenticated key exchange from fuzzy vaults and proved its security in compliance with ISO/IEC 24745. Our protocol is efficient both in terms of execution times and biometric performance.

The combination of asymmetric, secure, and efficient biometric authenticated key exchange has not been achieved in prior works. Related protocols are either symmetric, and thus does not provide protection of the biometric data on the server side, or inefficient in terms of computational speed due to their generality, or else insufficient in terms of recognition accuracy, allowing for zero-effort imposter and low-effort brute-force attacks. The accuracy deficiencies of the latter cannot be addressed by exchanging the biometric comparison subsystem, as the construction is specific to the imprecise comparator used.

In our protocol, we enforce communication for every adversarial guess through OPRFs. Using established and interchangeable improved fuzzy vault schemes for different biometric modalities, the key exchange is only successful if the two biometric samples were close. Furthermore, we show that our protocol can be instantiated both with classical primitives, namely discrete logarithm based OPRFs and Diffie-Hellman key exchange, as well as with lattice-based OPRFs and KEMs.

Future works may focus on addressing the necessary pre-alignment processes of minutiae-based fingerprint representations. A promising approach both with regard to rotation and entropy is the use of four-finger captures, where four fingerprints are captured within one image. Through the relative position of the fingers, pre-alignment can be realised more efficiently than based on minutiae, and the intra-identity independence of fingerprint patterns yield the fourfold entropy of the biometric data. Notably, the implementation of the minutiae fuzzy vault evaluated in our work includes the option of combining four fingerprints into one fuzzy vault. However, auxiliary alignment data required for pre-alignment are not yet discussed in this context.

APPENDIX A BIOMETRIC PERFORMANCE ANALYSIS

In this Appendix, we give the experimental evaluation of the recent work on biometrics-authenticated key exchange proposed by [7]. Specifically, we show the biometric performance of their construction for fingerprint and discuss its shortcomings.

TABLE 5. Biometric performance of BAKE [7] compared to state-of-the-art (SOTA) performance.

	FVC2004 DB-1 [65]		CASIA-FPV5[3]	
	FMR	FNMR	FMR	FNMR
BAKE [7]	27.8%	25.4%	27.6%	30.90%
SOTA[2]	1.01%	17.29%	1.13%	9.85%

For this evaluation, we implemented Algorithm 2 in [7] according to the description available in the paper. According to the description, we set the number of neighbours for each minutia at $\mu = 4$ and, iterating through the minutiae in the template, construct the vectors $v_{j,\rho}$ from the minutia's x- and y-coordinates which are given in pixels (i.e., integers) from the upper left corner. The calculation of the Euclidean distances $d_{j,1}, \ldots, d_{j,4}$ therefore result in floating point numbers, whereas the angles $\phi_{j,\rho,1}, \ldots, d_{j,\rho,6}$ remain as integer values. In Section 6.2.2 in [7], the authors state that the number of neighbours $\mu = 4$ originates an encoding of the values $d_{j,\rho}$ and $\phi_{j,\rho,\omega}$ into $\mu = 4$ bits each. This relation is not clear to us and we were not able to satisfactorily follow the reasoning given by the authors of [7] during an email exchange. Therefore, we give the evaluation of the biometric performance for the original float and integer values, which can be considered an upper bound for the performance of a binary encoding. As comparison function, we determined the set difference by mapping minutiae based on their minimal Hamming distance.

We evaluated our implementation of Algorithm 2 in [7] on the FVC2004 DB-1 [65], which is the least challenging out of the four databases used in [7] in terms of image quality and rotation of the fingerprint images. We compare the performance against a state-of-the art rotation invariant minutiae comparator, SourceAFIS [66]. From the evaluation, it becomes evident that the fingerprint comparison algorithm proposed by [7] does not have an acceptable performance (see Table 5). For the optimal threshold, the FMR is measured at 27.8% with a FNMR of 25.4%. Both of these values are not close to the required FMR of 0.1% [32] and FNMR below 5%. Compared to the state-of-the-art, the performance that can be achieved in this dataset lies at a FMR of 1.01% at FNMR of 17.29% using the SourceAFIS comparison algorithm.[2] This shows the challenging nature of the dataset, which was collected as a fingerprint verification challenge with the goal of providing challenging fingerprint samples. Therefore, we also evaluated both algorithms on the less challenging CASIA-FPV5[3] database. However, the result are similar with a FMR of 27.6% and FNMR of 30.90% for BAKE-1 compared to a FMR of 1.13% and FNMR of 9.85% for SourceAFIS.

To conclude, the fingerprint comparison algorithm proposed for the construction in [7] is not able to distinguish

[2]https://sourceafis.machinezoo.com/
[3]http://biometrics.idealtest.org

between mated and non-mated comparison trials to a satisfactory degree.

APPENDIX B NOTATION

TABLE 6. Overview of parameters.

	Parameter	Explanation
Generic	t	Biometric lock feature set.
	t'	Biometric unlocking feature set.
	f	Secret random polynomial.
	τ	Correction capacity of $\mathcal{C}$.
	$\mathbb{F}_{p'}$	Finite field for minutiae encoding.
	$\mathcal{C}$	Error-correcting code.
	H	Cryptographic hash function.
	λ	Security level.
	V	Locked fuzzy vault.
	f_k	Pseudorandom function with key k.
	x	Secret client input for OPRF.
	r	Randomness sampled by client.
	B, B'	Blinded OPRF input.
	S, S'	OPRF evaluation.
	U, U'	Unblinded OPRF evaluation.
	k	Secret OPRF evaluation key.
	pp	Public parameters.
	id	Biometric claim.
	csk	Client secret key.
	cpk	Client public key.
	ssk	Static server secret key.
	spk	Static server public key.
	(sk, pk)	Ephemeral asymmetric keys.
	γ	Session pre-key.
	ctx	Encapsulation of session pre-key γ.
	γ'	Decapsulation of session pre-key γ.
	KDF	Key derivation function.
	ρ	Session key.
	f^{-1}	False-accept security.
	l	Rate limit enforced by the server.
	$\mathcal{A}$	Adversary.
	$l_{\mathcal{A}}$	Brute-force capacity of adversary.
	ϵ	Adversary advantage.
Group setting	p	Prime group order.
	$\mathbb{G}$	Cyclic group.
	$\mathbb{Z}_p$	Scalar field of order p.
	$H_{\mathbb{G}}$	Cryptographic hash function $H_{\mathbb{G}} : \{0,1\}^* \to \mathbb{G}$.
	$H_{\mathbb{Z}_p}$	Cryptographic hash function $H_{\mathbb{Z}_p} : \{0,1\}^* \to \mathbb{Z}_p$.
Lattice setting	q	Ciphertext modulus.
	$\mathcal{R}_q$	Cyclotomic ring $R_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle$.
	N	Ring dimension of cyclotomic ring.
	χ	Bounded distribution over R_q.
	d	Module dimension for M-LWE.
	s	M-LWE secret sampled from χ.
	e	M-LWE error sampled from χ.
	m	Number of M-SIS vectors.
	β	Bound for M-SIS solutions.
	$\mathcal{D}_\sigma$	Ternary distribution over $\mathcal{R}_q$.
	$\mathcal{D}_{\sigma'}$	Uniform distribution over $\mathcal{R}_q$ bounded by $[-B, B]$.
	B	Bound for $\mathcal{D}_{\sigma'}$.

REFERENCES

[1] R. Kessler, O. Henniger, and C. Busch, "Fingerprints, forever young?" in *Proc. 25th Int. Conf. Pattern Recognit. (ICPR)*, Jan. 2021, pp. 8647–8654.

[2] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[3] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Comput. Vis. Image Understand.*, vol. 117, no. 10, pp. 1512–1525, Oct. 2013.

[4] G. Mai, K. Cao, P. C. Yuen, and A. K. Jain, "On the reconstruction of face images from deep face templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 5, pp. 1188–1202, May 2019.

[5] *EU Regulation 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*, European Parliament, Strasbourg, France, 2016.

[6] *Information Technology—Security Techniques—Biometric Information Protection*, Standard ISO/IEC 24745:2022, ISO/IEC JTC1 SC27 Security Techniques, International Organization for Standardization, 2022.

[7] M. Wang, K. He, J. Chen, Z. Li, W. Zhao, and R. Du, "Biometrics-authenticated key exchange for secure messaging," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2021, pp. 2618–2631.

[8] S. Jarecki, H. Krawczyk, and J. Xu, "OPAQUE: An asymmetric PAKE protocol secure against pre-computation attacks," in *Proc. EUROCRYPT*, vol. 10822, J. B. Nielsen and V. Rijmen, Eds. Heidelberg, Germany: Springer, May 2018, pp. 456–486.

[9] P.-A. Dupont, J. Hesse, D. Pointcheval, L. Reyzin, and S. Yakoubov, "Fuzzy password-authenticated key exchange," in *Proc. EUROCRYPT*, vol. 10822, J. B. Nielsen and V. Rijmen, Eds. Heidelberg, Germany: Springer, May 2018, pp. 393–424.

[10] A. Erwig, J. Hesse, M. Orlt, and S. Riahi, "Fuzzy asymmetric password-authenticated key exchange," in *Proc. ASIACRYPT*, vol. 12492, S. Moriai and H. Wang, Eds. Heidelberg, Germany: Springer, Dec. 2020, pp. 761–784.

[11] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[12] M. R. Albrecht, A. Davidson, A. Deo, and N. P. Smart, "Round-optimal verifiable oblivious pseudorandom functions from ideal lattices," in *Proc. PKC*, vol. 12711, J. Garay, Ed. Heidelberg, Germany: Springer, May 2021, pp. 261–289.

[13] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, "CRYSTALS–kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroSP)*, Apr. 2018, pp. 353–367.

[14] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, and R. Peralta, "Status report on the third round of the NIST post-quantum cryptography standardization process," U.S. Dept. Commerce, NISTs, Gaithersburg, MD, USA, Tech. Rep. NIST IR 8413, 2022.

[15] J. Bootle, S. Faller, J. Hesse, K. Hostáková, and J. Ottenhues, "Generalized fuzzy password-authenticated key exchange from error correcting codes," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Singapore: Springer, 2023, pp. 110–142.

[16] Y. Han, C. Xu, S. Li, C. Jiang, and K. Chen, "TtPAKE: Typo tolerance password-authenticated key exchange," *J. Inf. Secur. Appl.*, vol. 79, Dec. 2023, Art. no. 103658.

[17] S. Zhang, Z. Yan, W. Liang, K.-C. Li, and C. Dobre, "BAKA: Biometric authentication and key agreement scheme based on fuzzy extractor for wireless body area networks," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 5118–5128, 2023.

[18] X. Jiang and W.-Y. Yau, "Fingerprint minutiae matching based on the local and global structures," in *Proc. Int. Conf. Pattern Recognit. (ICPR)*, vol. 2, 2000, pp. 1038–1041.

[19] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.

[20] J. Daugman, "How iris recognition works," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[21] S Foundation. (2022). *Technical Information—Specifications and Software Libraries for Developers*. [Online]. Available: https://signal.org/docs/

[22] H. Proença, "Unconstrained iris recognition in visible wavelengths," in *Handbook of Iris Recognition*. London, U.K.: Springer, 2016, pp. 321–358.

[23] A. Everspaugh, R. Chaterjee, S. Scott, A. Juels, and T. Ristenpart, "The Pythia PRF service," in *Proc. USENIX Secur. Symp.*, 2015, pp. 547–562.

[24] K. Lewi, P. Mohassel, and A. Roy, "Single-message credential-hiding login," *Cryptol. ePrint Arch.*, pp. 1–42, Dec. 2020.

[25] J. Ernst and A. Mitrokotsa, "A framework for UC secure privacy preserving biometric authentication using efficient functional encryption," in *Proc. Int. Conf. Appl. Cryptography Netw. Secur.* Cham, Switzerland: Springer, 2023, pp. 167–196.

[26] S. Xu, Y. Cao, X. Chen, S.-M. Yiu, and Y. Zhao, "Post-quantum public-key authenticated searchable encryption with forward security: General construction, implementation, and applications," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, vol. 1. Singapore: Springer, Dec. 2023, pp. 274–298.

[27] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 2004, pp. 523–540.

[28] M. Qi, J. Chen, and Y. Chen, "A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC," *Comput. Methods Programs Biomed.*, vol. 164, pp. 101–109, Oct. 2018.

[29] A. Sarkar and B. K. Singh, "A novel session key generation and secure communication establishment protocol using fingerprint biometrics," in *Handbook of Computer Networks and Cyber Security*. Cham, Switzerland: Springer, 2020, pp. 777–805.

[30] *Information Technology—Biometric Data Interchange Formats—Part 1: Framework*, Standard ISO/IEC 19794-1:2011, ISO/IEC JTC1 SC37 Biometrics, International Organization for Standardization, Jun. 2011.

[31] *Information Technology—Biometric Performance Testing and Reporting—Part 1: Principles and Framework*, Standard ISO/IEC 19795-1:2021, International Organization for Standardization, 2021.

[32] *Best Practice Technical Guidelines for Automated Border Control ABC Systems*, FRONTEX, Warsaw, Poland, 2015.

[33] M. A. Olsen, V. Šmida, and C. Busch, "Finger image quality assessment features–definitions and evaluation," *IET Biometrics*, vol. 5, no. 2, pp. 47–64, Jun. 2016.

[34] E. Tabassi, M. Olsen, O. Bausinger, C. Busch, A. Figlarz, G. Fiumara, O. Henniger, J. Merkle, T. Ruhland, C. Schiel, and M. Schwaiger, "NIST interagency report 8382," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Interagency Rep. 8382, Jul. 2021.

[35] A. Adler, R. Youmaran, and S. Loyka, "Towards a measure of biometric information," in *Proc. Can. Conf. Elect. Comput. Eng.*, Feb. 2006, pp. 210–213.

[36] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Int. Conf. Audio Video-Based Biometric Person Authentication*. Berlin, Germany: Springer, 2001, pp. 223–228.

[37] J. Daugman, "Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons," *Proc. IEEE*, vol. 94, no. 11, pp. 1927–1935, Nov. 2006.

[38] B. Tams, "Unlinkable minutiae-based fuzzy vault for multiple fingerprints," *IET Biometrics*, vol. 5, no. 3, pp. 170–180, Sep. 2016.

[39] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes Cryptography*, vol. 38, no. 2, pp. 237–257, Feb. 2006.

[40] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcard-based fingerprint authentication," in *Proc. ACM SIGMM Workshop Biometrics Methods Appl.*, 2003, pp. 45–52.

[41] B. Tams, "Decodability attack against the fuzzy commitment scheme with public feature transforms," 2014, *arXiv:1406.1154*.

[42] C. Rathgeb, B. Tams, J. Wagner, and C. Busch, "Unlinkable improved multi-biometric iris fuzzy vault," *EURASIP J. Inf. Secur.*, vol. 2016, no. 1, pp. 1–16, Dec. 2016.

[43] C. Rathgeb, J. Merkle, J. Scholz, B. Tams, and V. Nesterowicz, "Deep face fuzzy vault: Implementation and performance," *Comput. Secur.*, vol. 113, Feb. 2022, Art. no. 102539.

[44] S. Casacuberta, J. Hesse, and A. Lehmann, "SoK: Oblivious pseudorandom functions," in *Proc. IEEE 7th Eur. Symp. Secur. Privacy (EuroS&P)*, 2022, pp. 625–646.

[45] M. J. Freedman, Y. Ishai, B. Pinkas, and O. Reingold, "Keyword search and oblivious pseudorandom functions," in *Proc. Theory Cryptography Conf.* Oxford, U.K.: Springer, 2005, pp. 303–324.

[46] W. Ford and B. S. Kaliski, "Server-assisted generation of a strong secret from a password," in *Proc. IEEE 9th Int. Workshops Enabling Technol., Infrastructure Collaborative Enterprises (WET ICE)*, Jun. 2000, pp. 176–180.

[47] T. Okamoto, "Authenticated key exchange and key encapsulation in the standard model," in *Proc. ASIACRYPT*, vol. 4833, K. Kurosawa, Ed. Heidelberg, Germany: Springer, Dec. 2007, pp. 474–484.

[48] C. Peikert, "A decade of lattice cryptography," *Found. Trends® Theor. Comput. Sci.*, vol. 10, no. 4, pp. 283–424, 2016.

[49] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, Sep. 2009.

[50] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proc. 28th ACM STOC*. New York, NY, USA: ACM Press, May 1996, pp. 99–108.

[51] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, and T. Koshiba, "Packed homomorphic encryption based on ideal lattices and its application to biometrics," in *Proc. Int. Conf. Availability, Rel., Secur.* New York, NY, USA: Springer, 2013, pp. 55–74.

[52] V. Guruswami and M. Sudan, "Improved decoding of Reed–Solomon and algebraic-geometric codes," in *Proc. Annu. Symp. Found. Comput. Sci.*, 1998, pp. 28–37.

[53] T. Silde and M. Strand, "Anonymous tokens with public metadata and applications to private contact tracing," in *Financial Cryptography and Data*. Cham, Switzerland: Springer, 1007, pp. 179–199.

[54] N. Tyagi, S. Celi, T. Ristenpart, N. Sullivan, S. Tessaro, and C. A. Wood, "A fast and simple partially oblivious PRF, with applications," in *Proc. EUROCRYPT*, vol. 13276, O. Dunkelman and S. Dziembowski, Eds. Heidelberg, Germany: Springer, Jun. 2022, pp. 674–705.

[55] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, and K. Lauter, "Homomorphic encryption standard," in *Protecting Privacy Through Homomorphic Encryption*. Cham, Switzerland: Springer, 2021, pp. 31–62.

[56] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. EUROCRYPT*, vol. 6110, H. Gilbert, Ed. Heidelberg, Germany: Springer, Jun. 2010, pp. 1–23.

[57] A. Banerjee, C. Peikert, and A. Rosen, "Pseudorandom functions and lattices," in *Proc. EUROCRYPT*, vol. 7237, D. Pointcheval and T. Johansson, Eds. Heidelberg, Germany: Springer, Apr. 2012, pp. 719–737.

[58] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-kyber algorithm specifications and supporting documentation," *NIST PQC Round*, vol. 3, pp. 1–43, Nov. 2021.

[59] D. Chaum and T. P. Pedersen, "Wallet databases with observers," in *Proc. Annu. Int. Cryptol. Conf.* Santa Babara, CA, USA: Springer, Aug. 1992, pp. 89–105.

[60] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*. Berlin, Germany: Springer, 1986, pp. 186–194.

[61] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro, "MCYT baseline corpus: A bimodal biometric database," *IEE Proc. Vis., Image, Signal Process.*, vol. 150, no. 6, p. 395, 2003.

[62] E. Barker, "Digital signature standard (DSS)," Nat. Inst. Standards Technol. (NIST), Gaithersburg, MD, USA, Tech. Rep. FIPS 186-5, 2013.

[63] D. Stebila and M. Mosca, "Post-quantum key exchange for the internet and the open quantum safe project," in *Proc. Int. Conf. Sel. Areas Cryptogr.* Cham, Switzerland: Springer, 2016, pp. 14–37. [Online]. Available: https://eprint.iacr.org/2016/1017

[64] M. R. Albrecht, R. Player, and S. Scott, "On the concrete hardness of learning with errors," Cryptol. ePrint Arch., Tech. Tech. Rep. Paper 2015/046, 2015. [Online]. Available: https://eprint.iacr.org/2015/046

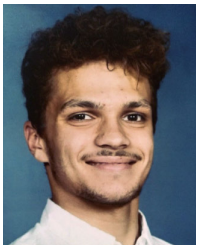
[65] *Fingerprint Verification Competition 2004*, The Biometric Systems Lab., The Biometric Test Center, San Jose State University, San Jose, CA, USA, Mar. 2004.

[66] R. Važan. (2018). *SourceAFIS Fingerprint Recognition Toolkit*. [Online]. Available: https://sourceafis.machinezoo.com

PIA BAUSPIEß received the B.Sc. degree in mathematics from the University of Freiburg, Breisgau, Germany, in 2018, and the M.Sc. degree in computer science from the University of Applied Sciences, Darmstadt, Germany, in 2021, with a focus on IT security. She is currently pursuing the Ph.D. degree with German National Research Center for Applied Cybersecurity, Darmstadt, Germany, and Norwegian University of Science and Technology, Trondheim, Norway. Her research interests include privacy-preserving biometrics with a particular interest in homomorphic encryption and post-quantum cryptography. She was a recipient of the CAST e.V. Award for the Best Master Thesis in the field of IT security in Germany, in 2021.

TJERAND SILDE received the Ph.D. degree in privacy-preserving cryptography from zero-knowledge proofs, in 2022. He is currently an Associate Professor in cryptology with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), where he is the Research Group Leader of the Applied Cryptology Laboratory. His research interests include lattice-based cryptography and zero-knowledge protocols, with further interests in the areas of post-quantum cryptography, anonymous communication, multiparty computation, homomorphic encryption, electronic voting, and secure implementation. He was a recipient of the 2020 Built-In Privacy Award awarded by the Norwegian Data Protection Authority and a member of the Program Committee for PETS 2024 and ACM CCS 2024.

MATEJ POLJUHA received the B.Sc. degree in informatics from the University of Rijeka. He is currently pursuing the M.Sc. degree in computer science and engineering with the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU). His research interests include post-quantum cryptography, privacy of biometric data, and data security.



ALEXANDRE TULLOT is currently pursuing the M.Sc. degree in aerospace and computer science with the National Higher French Institute of Aeronautics and Space (ISAE-SUPAERO). He is the President of the Supaero Computer Science Club with the purpose of promoting support and sharing of knowledge in cybersecurity and other fields of informatics. His research interests include cryptography, cybersecurity, and data privacy.

ANAMARIA COSTACHE received the Ph.D. degree from the University of Bristol, in 2018, with a focus on the practicality of ring-based fully homomorphic encryption schemes. From 2020 to 2021, she was a Postdoctoral Researcher with the Royal Holloway, University of London. She is currently an Associate Professor in cryptology with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology. Her research interests include privacy-preserving machine learning, fully homomorphic encryption and more broadly, computing on encrypted data, lattice-based, and post-quantum cryptography. She has served as the Program Chair and a Program Committee Member for several high-level cryptographic conferences, including MathCrypt 2019 and 2021, WAHC 2020 and 2021 (program chair) as well as 2022 and 2023 (co-organizer), ANTS 2022, ACM CCS 2022 and 2023, and FHE.org 2023. She is a member on the editorial board of the *IACR Communications in Cryptology* journal.

CHRISTIAN RATHGEB is currently a Professor with the Faculty of Computer Science, Hochschule Darmstadt, Germany. He is also a Principal Investigator with the National Research Center for Applied Cybersecurity (ATHENE). He has coauthored over 100 technical papers in the field of biometrics. His research interests include pattern recognition, iris and face recognition, the security aspects of biometric systems, secure process design, and privacy-enhancing technologies for biometric systems. He is a Winner of the EAB—European Biometrics Research Award in 2012, the Austrian Award of Excellence in 2012, the Best Poster Paper Awards (IJCB'11, IJCB'14, and ICB'15), the Best Paper Award Bronze (ICB'18), and the Best Paper Award (WIFS'21). He is a member of European Association for Biometrics (EAB) and the Program Chair of the International Conference of the Biometrics Special Interest Group (BIOSIG).

JASCHA KOLBERG received the B.Sc. and M.Sc. degrees in IT security/information technology from Ruhr-University Bochum, Bochum, Germany, in 2014 and 2017, respectively, and the Ph.D. degree in biometric information protection and presentation attack detection for fingerprint recognition, in 2021. He is currently a Senior Researcher with the National Research Center for Applied Cybersecurity (ATHENE), Darmstadt, Germany, and working with the da/sec Group, Faculty of Computer Science, Hochschule Darmstadt, Darmstadt. His current research interest includes fairness for biometric systems.

CHRISTOPH BUSCH (Senior Member, IEEE) is currently a member of the Norwegian University of Science and Technology (NTNU), Norway. He holds a joint appointment with Hochschule Darmstadt (HDA), Germany. He has been lecturing on biometric systems with DTU, Denmark, since 2007. On behalf of the German BSI, he has been the Coordinator for the project series BioIS, BioFace, BioFinger, BioKeyS Pilot-DB, KBEinweg, and NFIQ2.0. He was/is a Partner of the EU projects 3D-Face, FIDELITY, TURBINE, SOTAMD, RESPECT, TReSPsS, and iMARS. He is also a Principal Investigator with the German National Research Center for Applied Cybersecurity (ATHENE) and the Co-Founder of the European Association for Biometrics (EAB). He has coauthored more than 500 technical papers and has been a speaker at international conferences. He is a member of the editorial board of the *IET Journal on Biometrics* and formerly of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. Furthermore, he chairs the TeleTrusT biometrics working group and German standardization body on biometrics and the Convenor of WG3 in ISO/IEC JTC1 SC37.