

Adaptive Multiplicity Codes based PIR Protocol for Multi-Cloud Plateform Services

Lou Salaun, Amira Alloum, Philippe Jacquet

▶ **To cite this version:**

Lou Salaun, Amira Alloum, Philippe Jacquet. Adaptive Multiplicity Codes based PIR Protocol for Multi-Cloud Plateform Services. IEEE 5G 2018 - World Forum : Workshop on 5G Cloud Native Design, Jul 2018, Santa Clara, California, United States. pp.1-8, 10.1109/5GWF.2018.8517057 . hal-01831322

HAL Id: hal-01831322
https://hal.science/hal-01831322

Submitted on 5 Jul 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Adaptive Multiplicity Codes based PIR Protocol for Multi-Cloud Plateform Services

Lou Salaun*, Amira Alloum*, Philippe Jacquet*
*Mathematics of Complex and Dynamic Networks, Maths and Algo Group, Nokia Bell-labs, France

***Abstract*—Our contribution consists in deriving an adaptive multiplicity code based PIR protocol based on a code selection algorithm which guarantees minimal communication overhead for a given system architecture. We formulate the related constrained optimization problem, analyze it and introduce an algorithm for enabling the adaptive Information Theoretical secure PIR protocol to operate in highly dynamic multi cloud platform services. In addition, we prove that this algorithm also solves the feasibility problem and achieves optimal solution.**

I. Introduction : Industrial Challenge and Related Work

With the promise of offering ultra-reliable, low-latency and high data rates, the fifth generation of wireless mobile networks 5G [1], [2], is expected to introduce a golden digital age of remote healthcare, autonomous cars and advanced robotics use-cases. It heralds an explosion of augmented and virtual reality applications and accelerates the already rapid growth of the Internet of Things (IoT). However, today's mobile networks are not set up in a way that can handle 5G requirements without an extensive over-engineering. They will need to borrow principles of more scalable and flexible networks that deliver cloud-based services from the web scale players. This transformation is called cloud native 5G.

For realizing this vision, the IT and Telecommunication industries innovate on developing novel cloud solutions to face the increasing demand for computational resources with storage capacity, as well as on bringing new guarantees for data security and privacy. That is because a significant amount of sensitive data generated through mobile sensing, together with control signalling are to be stored and processed as a service by the telecom operator together or independantly to the cloud service provider, and should be protected from curious cloud providers, misbehaving insiders and malicious tenants. Accordingly, data privacy and security is being a growing concern for all parties (service providers, corporate clients and private users), and the need for novel solutions inherent to cloud based services is increasing [3], [4].

In this context, the focus of our paper is related to securing the access to large scale outsourced cloud storage, in the context of multi-cloud service providers. More specifically, revealing the queries executed by a client can leak sensitive data on the ongoing operations to the service provider. Private Information Retrieval (PIR) protocols originally introduced in [5] can be used to hide the access action by concealing the query, in order to prevent any information from being intercepted by the cloud service provider. A naive solution to this problem would be to download the entire database which is inefficient. Most PIR algorithms are categorized based on their design assumptions, such as the computational capability of the servers, the number of servers or the type of hard problem at the foundation of the algorithm as most of practical existing solutions are computationally secure.

Information theoretical secure PIR algorithms [6], [7] assume that the adversary may have unbounded computational capacity, as they target to decrease the communication overhead for retrieving the information compared to the trivial solution. This line of work follows numerous theoretical insights back to C. E. Shannon [8], [9], and considers the use of coding constructions which achieve unconditional security [10] and bring a major alternative for facing the security challenges of post quantum era after the collapse of the contemporary protocols and cryptography algorithms based mainly on factorization and discrete logarithm problems.

Initially, information theoretical secure PIR protcols have been approached theoretically and asymptotically. In particular, the locally decodable codes (LDC) based PIR protocols where most of the early constructions were only theoretical [6], [7], [11]–[13]. As a consequence, building practical efficient LDC based PIR protocols is a novel challenge recently tackled by academicians and industrials involved in coding and information theory research communities [14]–[19].

Locally decodable codes (LDC) appeared formally in the literature in [6]. These coding schemes enable the retrieval of a particular symbol from a codeword by using only few positions of its encoding symbols. The number of needed positions is proportional to a sub-linear space of the code length and is qualified as *locality* [20]. When a local decoding algorithm retrieves a symbol of the codeword instead of an information symbol, one speaks of locally correctable codes (LCC). The locality concept brings natural applications to PIR schemes as well as multi-party computation and average case complexity [7], [11].

Reed Muller codes belong to the LDC family, as does their generalized construction using derivative, known as Multiplicity codes [12]. Multiplicity codes were known to satisfy LCC properties at good coding rate compared to Reed Muller codes. However making them locally decodable in the strictest sense remained an open issue until came the ideas of Kopparty in [13] and the practical construction in [21] and [22] to build fast systematic Multiplicity encoding algorithm at quasi linear time. Those recent advances in complexity enable the feasibility of Multiplicity codes based PIR protocol originally

introduced in [14], where the storage overhead is optimal and equals the error correcting code overhead. However, the latter protocol is challenged by an increasing communication overhead that can even be reaching to the database size. This drawback finds a natural interpretation in the augmenting of the Reed Muller construction to an additional degree of freedom, by the evaluation of the derivatives of the corresponding multivariate polynomial up to a given order.

Our contribution in the present paper consists in deriving an adaptive PIR protocol extending the original one in [14] by the use of an optimization algorithm selecting the optimal Multiplicity code satisfying the lowest communication overhead for some given system parameters. Accordingly, we model the related optimization problem, analyze it and introduce an algorithm for enabling the adaptive PIR protocol to operate in highly dynamic multi-cloud platform services.

Our paper is organized as follows: in section II we introduce the system model, the security scenario and the corresponding assumptions. The proposed adaptive protocol is described in section III. We formulate the communication overhead minimization problem and analyze its feasible region in Section IV. In Section V, we develop an algorithm based on root-finding methods and a simple local search to solve the proposed optimization problem. In addition, we prove its termination and optimality. Finally, we conclude in Section VI.

II. System Model, Notations and Problem Statement

A. System Model, Assumptions and Motivations

Our scheme considers a given database composed of K entries and modeled as a K-tuple $(S_1, ..., S_K)$. The database belongs to a client, that outsources their data storage to multiple platform service providers that might be classical storage providers. Let us accordingly denote the set of servers used by ℓ considered storage providers as an ℓ-tuple $(SP_1, ..., SP_\ell)$. In all the following, we consider the strict assumption that the service providers do not collude. The current scheme can be extended to a multi-client case.

Let us precise that the database is not secret, it is not encrypted when stored at the cloud service providers' servers, where each one can contain the whole database, a subset of it or redundant versions of one of them.

Besides, our security scenario considers the service providers to be honest but curious. Accordingly, we consider the use of a PIR Protocol as an encryption-free cryptographic solution preventing the service providers from inferring any information about the client queries. For instance repeated queries of a banker about a company stock exchange quotation,if leaked may reveal indications about the market trend and impact reciprocally the stock exchange quotation of that company . We also precise our approach is targeted toward infrequently-updated data, and can be adapted for datasets updated in a sequential manner and not randomly.

In the specific case of information theoretically secure PIR protocols, the use of locally decodable codes is particularly convenient as they allow a symbol of the information message to be probabilistically recovered after querying a sub-linear number of coded symbols. This quantity is the locality denoted as ℓ. Consequently, during the initialization step it is required to systematically encode the original database into a redundant database with N entries denoted $(E_1, ..., E_N)$ where $N > K$. In order to retrieve an original entry S_i without revealing it to the servers, the client has to ask for one entry from each server where all of them are different from the sought entry S_i: the client thus gets ℓ symbols and by local decoding can compute S_i. The symbols queried are not random, they are chosen according to the decoding algorithm. However the queries are perceived by each server as following a random distribution.

B. From Generalized Reed Muller codes to Multiplicity Codes

1) Generalized Reed Muller Codes: Generalized Reed Muller codes are constructed by complete evaluation of low degree multivariate polynomial over a finite field. The code is specified by parameters (r, m, q) where:

- q is the alphabet size and is a prime power.
- m denotes the number of variables, as the dimension of the considered affine space over $\mathbf{F}_q$ in the following.
- $r \leq q - 2$ is the degree of the polynomial.

Let $\mathbf{F}_q = \{\gamma_i\}_{i=0}^{q-1}$ denotes a finite field with q elements. Let us consider the variable vector $\mathbf{X} = (X_1, \ldots, X_m)$ where $F(\mathbf{X}) \in \mathbf{F}_q[\mathbf{X}]$ denotes an m-variable polynomial of degree at most $r \leq q - 2$. The number of coefficients of $F(\mathbf{X})$ is the code dimension $K = \binom{m+r}{r}$, the minimum distance is $d = (q - r)q^{m-1}$ and $N = q^m$ is the code length [23].

The (r, m) Reed-Muller code over $\mathbf{F}_q$ is defined as: $(F(\mathbf{P}_1), F(\mathbf{P}_2), \ldots, F(\mathbf{P}_n))$ where each point $\mathbf{P}_i \in \mathbf{F}_q^m$ belongs to the m-dimensional affine space over $\mathbf{F}_q$.

Let us consider the vector: $V = [v_0 \ldots v_{m-1}]^T \in \mathbf{F}_q^m \setminus \{0\}$, and the point: $P = [p_0 \ldots p_{m-1}]^T \in \mathbf{F}_q^m$. The q elements:

$$y_i = F(P + \gamma_i \cdot V) = F_{P,V}(\gamma_i), \qquad \gamma_i \in \mathbf{F}_q, \tag{1}$$

build a $(q, r + 1)$ Reed-Solomon RS codeword, of dimension $r + 1$, and length q. $F_{P,V}$ is a polynomial of degree at most r. Local decoding is possible when at least $r + 1$ received symbols are evaluating the points aligned on such a line, then the RS decoding algorithm can occur on the received symbols and perfectly reconstruct at most the erased $q-(r+1)$ symbols using classical polynomial interpolation algorithms.

2) Multiplicity Codes: The multiplicity code is a vector space construction augmenting the RM codeword to an additional degree of freedom σ, referring to the vector size. For thus, the evaluation of the derivatives of the original RM multivariate polynomials is performed up to a given order s, named the multiplicity, and thus at all points of the affine space $\mathbf{F}_q^m$ [22]. The derivatives considered in this context are the Hasse derivatives defined as follows:

Definition 1. *The Hasse derivatives of an m-variable polynomial of degree at most $r \leq q - 2$, $F(\mathbf{X}) \in \mathbf{F}_q[\mathbf{X}]$ are given by the coefficients of the shifted polynomial $F(\mathbf{X} + \mathbf{Z}) \in \mathbf{F}_q[\mathbf{X}][\mathbf{Z}]$. Hence, the coefficient of $\mathbf{Z}^{\mathbf{i}} = Z_1^{i_1} ... Z_m^{i_m}$ with the multi index $\mathbf{i} = (i_1, ..., i_m) \in \mathcal{N}^m$ in the shifted polynomial*

is called the $\mathbf{i}$ *th Hasse derivative of* $F(\mathbf{X})$ *and denoted by* $H(F, \mathbf{i})$ *. The order of the derivative is evaluated as the weight of the multi index* $\mathbf{i}$ *denoted* $|\mathbf{i}|$.

In Multiplicity construction, the derivatives order is restricted to be lower than the called multiplicity s including the set of derivative degrees $\mathcal{S}_{s,m} = \{\mathbf{i} \in \mathcal{N}^m || \mathbf{i}| < s\}$ where the cardinality of $\mathcal{S}_{s,m}$ is $\sigma = \binom{m+s-1}{m}$ and denotes the extension order of the RM. When $s = 1$ the Multiplicity is reduced to an RM. The coding rate of a Multiplicity code is $\frac{\binom{m+r}{m}}{\binom{m+s-1}{m} \times q^m}$.

C. Multiplicity Codes Based PIR Protocol

In the original work [14], multiplicity codes have been used to construct an information-theoretically secure PIR protocol. The latter outperforms the standard construction for LDC codes, as it exploits the geometric properties of the Multiplicity to reduce the number of servers to q which brings better security guarantees to the protocol. Besides the same properties are leveraged to distribute the storage of the encoded database across the servers according to an orthogonal partition, rather than replicating them on each server. Hence, the protocol benefits from an reduced storage overhead that equals the code redundancy overhead. With respect to the original protocol in [14], let us introduce the following parameters:

- q denotes the servers number meeting the dimension of the considered finite Galois Field $\mathbf{F}_q$ of reference.
- m is the dimension of the projective space $\mathbf{F}_q^m$ over $\mathbf{F}_q$.
- s is the multiplicity of a polynome $F(\mathbf{X}) \in \mathbf{F}_q[\mathbf{X}]$, and is defined as the largest integer such that for every multi-index $\mathbf{i} \in \mathcal{N}^m$ that satisfies $|\mathbf{i}| < s$ the Hasse derivatives $H(F, \mathbf{i})$ evaluates the projective space $\mathbf{F}_q^m$.
- $\sigma = \binom{m+s-1}{m}$ is the Hasse derivatives number to consider in the Multiplicity code construction.
- $K = \binom{m+r}{r}$ and $N = q^m$ are respectively the dimension and the codelength of the considered Multiplicity code.

We consider that the database size is $k = K \times E$ bits, where E is a database entry length in bits. In the classical case we can choose $E = \log_2(q')$ where q' could meet the value of q or not. For sake of simplicity, we consider that $q' = q$ in all the following. We also consider in the rest of the paper, only constructions where the maximum degree r of considered polynomials is $r = s(q-1) - 1$. Besides let us consider the following notations for the protocol performance indicators:

- The LDC Locality is the number of queries $\sigma(q-1)$. For recoverering a symbol from a codeword, it is required to use σ randomly chosen lines in $\mathbf{F}_q^m$ passing through the point, whose evaluation at a given derivative is to recover.
- The PIR Locality is the number of servers q. This is specific to the protocol designed in [14] and exploits the geometric properties of multiplicity codes guaranteeing an optimal storage overhead with the use of few servers.
- The coding rate is $R = \binom{m+r}{r}/(q^m\sigma)$ and $1/R$ denotes the storage overhead.
- The communication complexity χ is defined as the number of exchanged information required to retrieve one database entry, i.e. in our case a symbol of $\log_2(q)$ bits. For protocol [14], we have $\chi = (m-1+\sigma)q\sigma$ symbols or equivalently $(m-1+\sigma)q\sigma \log_2 q$ bits.
- The capacity $\mathcal{C} = 1/\left(q\sigma^2\right)$ as defined in [16] is the number of bits retrieved per bit of total download. It differs from communication complexity as it does not consider the queries sent from the client to servers.

For ease of reading, in the rest of the paper the aforementioned database size K and computational complexity χ will be expressed in terms of symbols. The conversion to bits is done by a $\log_2(q)$ multiplication under the assumptions taken above.

D. Problem Statement

The main limitation of the protocol is that it suffers from a communication complexity polynomial with the data base size K, while the trivial protocol communication overhead equals the database size. Though the protocol proposed in [14] is optimal in terms of storage overhead, nowadays the bandwidth on a network is more scarce and expensive than the storage capacity. Moreover, it is important to consider that most of the databases stored in the cloud are very large scale ones as for instance genomic data or medical records. This fact drastically impacts the efficiency of the transmission over the network during the execution of the PIR protocol. In the following we bring a solution to this problem by the proposal of an adaptive multiplicity code based PIR Protocol.

III. Adaptive Multiplicity Codes Based PIR Protocol

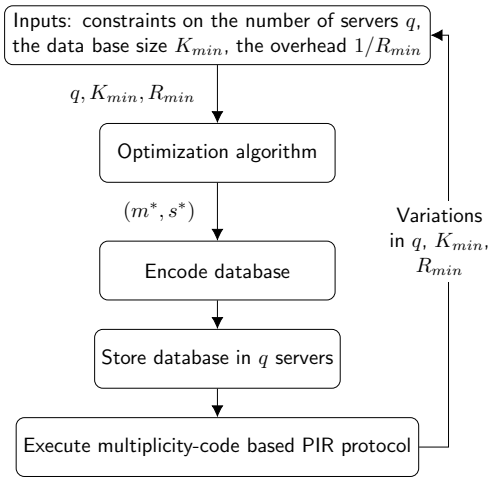


Fig. 1: Adaptive Multiplicity Codes Based PIR Protocol

With respect to the highly dynamic architecture of cloud platform services, our proposal consists in a novel protocol enabling the selection of the optimal multiplicity code construction, underlying a coded based PIR Protocol, in terms of minimal communication complexity (or maximal capacity) for a given database size K_{min}, and a given number of servers and locality q as for a constrained overhead level $1/R_{min}$ in the cloud storage system. For doing so, we model the selection mechanism as an optimization problem, and bring an algorithm as a solution underlying and enabling an

adaptive PIR protocol that provides the guarantee of minimal communication complexity (or maximal capacity) when:

- The size of the database varies, because of an update.
- The cloud service providers number, as the quantity of available storage experience a variation because of a cloud service provider architecture update, or backup maintemance operation in case one of the servers is down.

The proposed adaptive PIR protocol is described in the diagram of Fig. 1. Each time the number of servers, the storage capacity or the database size vary, another iteration of the algorithm is ran to select a new optimized parameters (m^*, s^*) such that the database is re-encoded and re-stored for a new instance of the multiplicity-codes based PIR protocol.

IV. Code Selection Optimization Problem Formulation and Analysis

A. Problem formulation

In this section, we consider the following constrained optimization problem:

$$\begin{aligned} \underset{(m,s)\in\mathbb{N}_+^2}{\text{minimize}} \quad & obj(m,s) \\ \text{subject to} \quad & C1:\ K(m,s) \geq K_{min}, \\ & C2:\ R(m,s) \geq R_{min}, \\ & C3:\ \sigma(m,s) \leq \frac{q^m-1}{q-1}. \end{aligned} \tag{$\mathcal{P}$}$$

The formulation of $\mathcal{P}$ expresses the problem of selecting the multiplicity code construction, specified by parameters (m, s), such that the communication complexity is minimized when one considers $obj = \chi$ or the capacity is maximized when one considers $obj = 1/\mathcal{C}$. These two objectives are in fact closely related as $\chi = (m - 1 + \sigma)q\sigma = O(q\sigma^2) = O(1/\mathcal{C})$ when $m \ll \sigma$ as soon as $s > 1$. They are also both strictly increasing in m and s. The proposed Algorithm 1 in Section V is able to solve both problems.

Constraint $C1$ guarantees to encode a database of K_{min} symbols. The storage overhead is limited to $1/R_{min}$ by constraint $C2$. We assume that the database consists of at least 1 symbol so that $K_{min} \geq 1$, the number of servers $q \geq 2$ is fixed and $R_{min} \in [0, 1]$. The constraint $C3$ is related to the local decoding algorithm described in [14] and the finite dimension of the considered affine space. The latter considers that the σ lines needed for local decoding should be lower to or equal the total number of lines crossing the point whose the evaluation at a given derivative is the entry to recover [24].

In this analysis, we relax $\mathcal{P}$'s search space to the real domain, i.e. $(m, s) \in \mathbb{R}_+^2$. To this end, the binomial coefficient is extended to the positive real domain by using the Γ function

$$\forall x, y \in \mathbb{R}_+,\ \binom{x}{y} \triangleq \frac{\Gamma(x+1)}{\Gamma(y+1)\Gamma(x-y+1)}. \tag{2}$$

For the sake of clarity, we use the following notations: $\mathbb{R}_+ = (0, +\infty)$ is the positive real domain, $\mathbb{R}_{\geq 1} = [1, +\infty)$ is the set of real numbers greater or equal to 1, and $\mathbb{N}_+$ is the set of positive integers. In addition, $\ln$, $\log_2$ and $\log_{10}$ represent respectively the natural, base-2 and base-10 logarithms. The floor and ceiling functions are denoted $\lfloor\cdot\rfloor$ and $\lceil\cdot\rceil$ resepctively.

B. Feasible region analysis

Let $\mathcal{F}_{\mathbb{R}}$ denotes the real domain feasible region on $\mathbb{R}_{\geq 1}^2$ satisfying constraints $C1$ to $C3$, and $\mathcal{F}_{\mathbb{N}} \triangleq \mathcal{F}_{\mathbb{R}} \cap \mathbb{N}_+^2$ the integer feasible set. In this section, we will prove that $\mathcal{F}_{\mathbb{R}}$ is delimited by three monotonous function $s = f_{C1}(m)$, $s = f_{C2}(m)$ and $s = f_{C3}(m)$ in the two dimensional plane, as shown in Figure 2. In order to demonstrate so, we transform the implicit constraints between m and s into computable functions of one variable m. Their existence and well-definedness are derived in Theorem 3 from the implicit function theorem [25]. Let F_{C1}, F_{C2} and F_{C3} be functions of class C^∞ from $\mathbb{R}_{\geq 1} \times \mathbb{R}_+$ to $\mathbb{R}$ defined as

$$\begin{aligned} F_{C1}(m,s) &= K(m,s) - K_{min}, \\ F_{C2}(m,s) &= R(m,s) - R_{min}, \\ F_{C3}(m,s) &= \sigma(m,s) - \frac{q^m-1}{q-1}. \end{aligned}$$

They characterize problem $\mathcal{P}$'s constraints, i.e. $(m, s) \in \mathbb{N}_+^2$ is a feasible point of $\mathcal{P}$ if and only if $F_{C1}(m, s) \geq 0$, $F_{C2}(m, s) \geq 0$ and $F_{C3}(m, s) \leq 0$. Let us introduce the 2-dimensional implicit function theorem [25] as follows.

Theorem 2 (2-dimensional implicit function theorem)**.** *Let $\mathcal{U}$ be an open set of $\mathbb{R}^2$ and $F\colon \mathcal{U} \to \mathbb{R}$ be a function of class C^k, $k \geq 1$. Let $(a, b) \in \mathcal{U}$ such that*

$$F(a,b) = 0 \quad \textit{and} \quad \frac{\partial F}{\partial y}(a,b) \neq 0, \tag{3}$$

where $\frac{\partial F}{\partial y}$ denotes the partial derivative of F with respect to its second variable. Then there exists neighborhoods $\mathcal{V}$ and $\mathcal{W}$ of a and b and a function $f\colon \mathcal{V} \to \mathcal{W}$ of class C^k such that $\mathcal{V} \times \mathcal{W} \subset \mathcal{U}$ and

$$\forall x \in \mathcal{V},\ y \in \mathcal{W}, F(x,y) = 0 \Leftrightarrow y = f(x).$$

Furthermore, $\mathcal{V}$ and $\mathcal{W}$ can be chosen such that $\frac{\partial F}{\partial y}(a, b) \neq 0$ for any $(a, b) \in \mathcal{V} \times \mathcal{W}$, then

$$\forall x \in \mathcal{V},\ f'(x) = -\frac{\frac{\partial F}{\partial x}(x, f(x))}{\frac{\partial F}{\partial y}(x, f(x))}. \tag{4}$$

Theorem 2 allows us to prove the following feasible region characterization. The proof can be found in the Appendix.

Theorem 3 (Feasible region characterization)**.** *The feasible regions $\mathcal{F}_{\mathbb{N}}$ and $\mathcal{F}_{\mathbb{R}}$ are delimited by the following three functions f_{C1}, f_{C2} and f_{C3}:*

1) *There exists a strictly decreasing function $f_{C1}\colon \mathbb{R}_{\geq 1} \to \mathbb{R}_+$ of class C^∞ and its inverse f_{C1}^{-1} such that for all $(m, s) \in \mathbb{R}_{\geq 1} \times \mathbb{R}_+$, $F_{C1}(m, s) \geq 0 \Leftrightarrow s \geq f_{C1}(m)$.*
2) *Constraint $C3$ can be characterized in different ways depending on the values of R_{min} and q:*
   a) *If $R_{min} > (q - 1)/q$, then $\mathcal{F}_{\mathbb{N}} = \emptyset$.*
   b) *If $R_{min} = (q - 1)/q$, then only codes with $m = 1$ satisfy constraint $C2$.*

c) If $R_{min} < (q-1)/q$ and $q \geq 3$, then let $a = \max\{1, -\ln(R_{min})/\ln(q)\}$ and $b = \ln(R_{min})/\ln((q-1)/q)$. There exists a strictly increasing function $f_{C3}\colon [a,b] \to \mathbb{R}_+$ of class C^∞ and its inverse f_{C2}^{-1} such that for all $(m,s) \in [a,b] \times \mathbb{R}_+$, $F_{C2}(m,s) \geq 0 \Leftrightarrow f_{C2}^{-1}(s) \geq m$.
In addition, constraint $C2$ is unfeasible for any $m > b$.

d) If $R_{min} < (q-1)/q$ and $q = 2$, then constraint $C2$ is satisfied if and only if $m \leq -\log_2(R_{min})$. For simplicity of notations in Algorithm 1, we define $f_{C2}^{-1}\colon s \mapsto -\log_2(R_{min})$, even if function f_{C2} does not exists in this case. This way, the equivalence $F_{C2}(m,s) \geq 0 \Leftrightarrow f_{C2}^{-1}(s) \geq m$ remains valid.

3) There exists a strictly increasing function $f_{C3}\colon \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 1}$ of class C^∞ and its inverse f_{C3}^{-1} such that for all $(m,s) \in \mathbb{R}^2_{\geq 1}$, $F_{C3}(m,s) \leq 0 \Leftrightarrow s \leq f_{C3}(m)$.

Apart from the trivial cases $R_{min} \geq (q-1)/q$ and $q = 2$ for constraint $C2$, Theorem 3 states that each constraint $C \in \{C1, C2, C3\}$ can be characterized by a curve $s = f_C(m)$ which separates feasible and unfeasible regions. It follows that the feasible set $\mathcal{F}_\mathbb{R}$ is the intersection of f_{C1}'s supergraph, f_{C2}^{-1}'s epigraph and f_{C3}'s epigraph, as shown in Figure 2, i.e.

$$\forall (m,s) \in \mathbb{R}^2_{\geq 1},\ s \geq f_{C1}(m) \text{ and } f_{C2}^{-1}(s) \geq m \text{ and } s \leq f_{C3}(m) \Leftrightarrow (m,s) \in \mathcal{F}_\mathbb{R}.$$

Let us notice that these functions f_C can be evaluated at any $m \in \mathrm{range}(f_C)$ in their domain of definition by solving $F_C(m,s) = 0$ for $s \in \mathrm{range}(f_C^{-1})$. We know from Theorem 3 that it admits a unique solution and F_C is strictly monotone in s, it can therefore be computed using classical root-finding algorithms such as Newton's method (which takes advantage of f_C's derivatives), the secant method and the dichotomy method (which does not require derivative information).

V. Optimal Code Selection Algorithm

Based on the previous feasible region analysis, we propose an algorithm which solves both the feasibility of $\mathcal{P}$ in the integer domain and computes its optimal solution if it exists: Algorithm 1 returns the optimal code (m^*, s^*) if $\mathcal{F}_\mathbb{N} \neq \emptyset$, and returns $\emptyset$ otherwise. The basic idea of this algorithm is, first, to check whether $\mathcal{F}_\mathbb{R}$ is empty or not. Indeed, if $\mathcal{F}_\mathbb{R} = \emptyset$ then $\mathcal{F}_\mathbb{N} = \emptyset$ and $\mathcal{P}$ has no solution. To this end, we distinguish between the three different cases of Theorem 3:

- If $R_{min} > (q-1)/q$, then there is no solution (lines 2-3).
- If $R_{min} = (q-1)/q$, then only codes with parameter $m = 1$ satisfy constraint $C2$ (lines 4-5).
- If $R_{min} < (q-1)/q$ and $q = 2$, then we know that constraint $C2$ is satisfied if and only if $m \leq -\log_2(R_{min})$. We choose to initialize $m \leftarrow -\log_2(R_{min})$ at line 7, which is greater than 1 since $R_{min} \leq 0.5$.
- If $R_{min} < (q-1)/q$ and $q \geq 3$, then $\mathcal{F}_\mathbb{R}$ is delimited by f_{C1}, f_{C2}, f_{C3}. Since f_{C1} is strictly decreasing and f_{C2} is strictly increasing, we compute at line 9 their intersection (m,s) using root-finding algorithm as mentioned in Section IV-B.

Algorithm 1 Optimal Code Selection Algorithm

Input: obj, q, k_{min}, R_{min}.

```
. . . . . Check if F_R = ∅ . . . . .
1: ▷ m and s are temporary real variables
2: if R_min < (q−1)/q then
3:     return ∅
4: else if R_min = (q−1)/q then
5:     m ← 1
6: else if q = 2 then
7:     m ← −log2(R_min)
8: else
9:     m ← solution of f_C1(m) − f_C2(m) = 0 for m ≥ 1
10: end if
11: s ← f_C1(m)
12: if s > f_C3(m) then
13:     return ∅
14: end if
. . . . . Local search on F_R . . . . .
15: (m*, s*) ← ∅                    ▷ current best integer solution
16: obj* ← +∞                       ▷ temporary value of obj(m*, s*)
17: s ← ⌈s⌉ − 1                     ▷ s now only takes integer values
18: while true do
19:     s ← s + 1                   ▷ increment s
20:     m ← max{f_C1^{-1}(s), f_C3^{-1}(s)}
21:     if m > ln(R_min)/ln((q−1)/q) ∨ obj(f_C3^{-1}(s), s) > obj* then
22:         return (m*, s*)
23:     else if f_C2^{-1}(s) ≥ ⌈m⌉ ∧ obj(⌈m⌉, s) < obj* then
24:         (m*, s*) ← (⌈m⌉, s)
25:         obj* ← obj(m*, s*)
26:     end if
27: end while
```

In the three latter cases, at line 11, (m,s) is the point satisfying both $C1$ and $C2$ with the lowest y-coordinate s. Hence, at line 12, if $s > f_{C3}(m)$ then no point can satisfy $C1$, $C2$ and $C3$. Otherwise,that reflects that $\mathcal{F}_\mathbb{R} \neq \emptyset$ as $(m,s) \in \mathcal{F}_\mathbb{R}$.
At line 15, since $\mathcal{F}_\mathbb{R} \neq \emptyset$, we use a local search method to find possible values of $\mathcal{F}_\mathbb{N}$. m and s are temporary variables, (m^*, s^*) stores the best integer solution found and $obj^* = obj(m^*, s^*)$. We iterate a while loop by incrementing s starting at the lowest integer value in $\mathcal{F}_\mathbb{R}$. At each iteration, we compute the $m \in \mathbb{R}_+$ which minimize obj and satisfies both $C1$ and $C3$ (line 20). By this construction, $(\lceil m \rceil, s)$ satisfies $C1$ and $C3$, but $C2$ may not be satisfied. Hence, on lines 23-25, we replace (m^*, s^*) with a better solution $(\lceil m \rceil, s)$ if in addition it is feasible with respect to $C2$, i.e. $f_{C2}^{-1}(s) \geq \lceil m \rceil$. The while loop terminates if one of the two conditions is true:

- if $m > \ln(R_{min})/\ln(\frac{q-1}{q})$, then (m,s) does not satisfy $C2$. Since f_{C1} is strictly decreasing it cannot intersect f_{C3} a second time, therefore $m = f_{C3}^{-1}(s)$. We know from the monotonicity of f_{C3} that by further incrementing $s' > s$, line 20 will necessarily assign $m' \leftarrow f_{C3}^{-1}(s') > f_{C3}^{-1}(s) = m > \ln(R_{min})/\ln(\frac{q-1}{q})$. Thus, Theorem 3's part 2) c) ensures that no more solution can be found

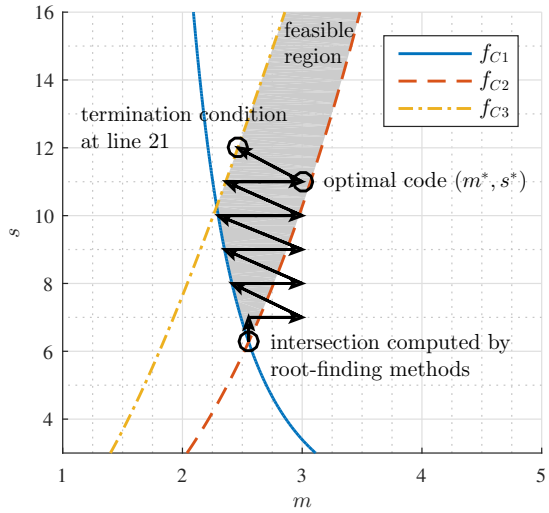


Fig. 2: Feasible region and our algorithm's iterations in the (m, s)-plane.

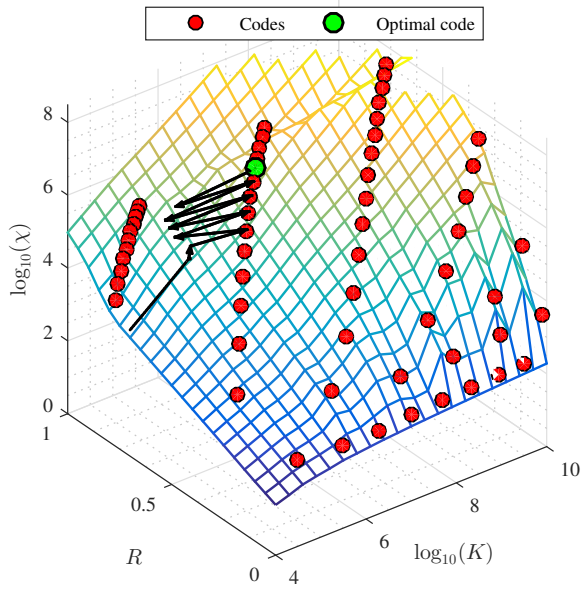


Fig. 3: Multiplicity codes versus R, $\log_{10}(K)$ and $\log_{10}(\chi)$.

by incrementing s. All possible codes in $\mathcal{F}_{\mathbb{N}}$ have been analyzed, the algorithm terminates and is optimal.

- if $obj(f_{C3}^{-1}(s), s) > obj^*$, then any remaining feasible points (m', s') with $s' > s$ achieve worse solution than (m^*, s^*). Indeed, by monotonicity of f_{C3}, any remaining feasible points $(m', s') \in \mathcal{F}_{\mathbb{R}}$ with $s' > s$ also has $m' > f_{C3}^{-1}(s)$. It follows, by monotonicity of obj, that $obj(m', s') > obj(f_{C3}^{-1}(s), s) > obj(m^*, s^*)$. Thus, the algorithm terminates and is optimal.

The analysis above proves that Algorithm 1 is optimal and terminates. Fig. 2 and Fig. 3 shows the behavior of Algorithm 1 with inputs $q = 32$, $K_{min} = 2 \times 10^5$ symbols and $R_{min} = 0.7$. In both figures, Algorithm 1's iterations are indicated by arrows. Fig. 2 shows the feasible set $\mathcal{F}_{\mathbb{R}}$ colored grey and delimited by f_{C1}, f_{C2} and f_{C3} in the (m, s)-plane. This is consistent with the theoretical analysis of Section IV. We present in Fig. 3 the communication complexity $\log_{10}(\chi)$ of various codes versus R and $\log_{10}(K)$. These codes are obtained through an exhaustive search. We see that Algorithm 1 converges to the optimal of $\mathcal{P}$.

VI. Conclusions

In the current paper we proposed a Multiplicity codes based adaptive PIR protocol that is beneficial for multi cloud platform services featured by a high variability in terms of resources, as servers availabilities and storage capacity. Besides the proposed protocol can handle occasional updates when database size varies, with guaranteed minimal communication overhead compared to the trivial case of PIR.

Acknowledgments

The authors are grateful to V.Kumar,D. Augot, F. Levy-Dit-Vehel, N. Coxon, B. Sayadi, S. Papillon, S. Dubus, H. El Abed and F. Mathieu for the helpful technical discussions. This work is in the framework of the H2020 5G-PPP phase 2 NGPaaS project (http://ngpaas.eu).

References

[1] R. Vannithamby and S. Talwar, *Towards 5G: Applications, Requirements and Candidate Technologies*. John Wiley & Sons, 2017.
[2] D. Soldani, "5G beyond radio access," *Mondo Digitale*, p. 2, 2018.
[3] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 32–39, 2016.
[4] V. Jeyakumar *et al.*, "EyeQ: Practical network performance isolation for the multi-tenant cloud." in *HotCloud*, 2012.
[5] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in *Proc. 36th Annual IEEE Symp. Foundations Comput. Sci.*, 1995, pp. 41–50.
[6] J. Katz and L. Trevisan, "On the efficiency of local decoding procedures for error-correcting codes," in *Proc. 32nd Annual ACM Symp. on Theory of comput.* ACM, 2000, pp. 80–86.
[7] S. Yekhanin, "Private information retrieval," *Commun. of the ACM*, vol. 53, no. 4, pp. 68–73, 2010.
[8] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.
[9] ——, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
[10] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, 2013.
[11] S. Yekhanin *et al.*, "Locally decodable codes," *Found. Trends Theor. Comput. Sci.*, vol. 6, no. 3, pp. 139–255, 2012.
[12] S. Kopparty, S. Saraf, and S. Yekhanin, "High-rate codes with sublinear-time decoding," *Journal of the ACM (JACM)*, vol. 61, no. 5, p. 28, 2014.
[13] S. Kopparty, "List-decoding multiplicity codes." *Theory of Computing*, vol. 11, no. 5, pp. 149–182, 2015.
[14] D. Augot, F. Levy-Dit-Vehel, and A. Shikfa, "A storage-efficient and robust private information retrieval scheme allowing few servers," in *Int. Conf. on Crypt. and Network Security*. Springer, 2014, pp. 222–239.
[15] R. Freij-Hollanti, O. W. Gnilke, C. Hollanti, and D. A. Karpuk, "Private information retrieval from coded databases with colluding servers," *SIAM J. Appl. Algebra Geom.*, vol. 1, no. 1, pp. 647–664, 2017.
[16] K. Banawan and S. Ulukus, "The capacity of private information retrieval from coded databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1945–1956, 2018.
[17] A. Fazeli, A. Vardy, and E. Yaakobi, "Codes for distributed PIR with low storage overhead," in *IEEE Int. Symp. on Inform. Theory (ISIT)*, 2015, pp. 2852–2856.
[18] S. Kumar, E. Rosnes, and A. G. i Amat, "Private information retrieval in distributed storage systems using an arbitrary linear code," in *IEEE Int. Symp. on Inform. Theory (ISIT)*, 2017, pp. 1421–1425.
[19] S. R. Blackburn and T. Etzion, "PIR array codes with optimal PIR rates," in *IEEE Int. Symp. on Inform. Theory (ISIT)*, 2017, pp. 2658–2662.
[20] S. Madhu. (2015) Locality in coding theory. IEEE Information Theory Society, Microsoft Research. [Online]. Available: https://www.youtube.com/watch?v=QCjTA8vB3MY
[21] D. Augot, F. L. dit Vehel, and C. M. Ngô, "Information sets of multiplicity codes," in *IEEE Int. Symp. on Inform. Theory (ISIT)*, 2015, pp. 2401–2405.

[22] N. Coxon, "Fast systematic encoding of multiplicity codes," *arXiv preprint arXiv:1704.07083*, 2017.
[23] G. Lachaud, "Projective reed-muller codes," in *International Colloquium on Coding Theory and Applications*. Springer, 1986, pp. 125–129.
[24] A. Alloum, S.-J. Lin, and T. Y. Al-Naffouri, "On locality of generalized reed-muller codes over the broadcast erasure channel," in *IEEE Int. Symp. on Broadband Multimedia Syst. and Broadcast.*, 2016, pp. 1–4.
[25] S. G. Krantz and H. R. Parks, *The implicit function theorem: history, theory, and applications*. Springer Science & Business Media, 2012.
[26] N. Batir, "Inequalities for the gamma function," *Archiv der Mathematik*, vol. 91, no. 6, pp. 554–563, 2008.
[27] F. Qi, "Bounds for the ratio of two gamma functions," *Journal of Inequalities and Applications*, vol. 6, 2010.

APPENDIX
PROOF OF THEOREM 3

Let us first define some useful properties and inequalities for the rest of the proof. Recall that we consider the extended binomial coefficient as in Eq. (2). $\binom{x}{y}$ is a strictly increasing function of x for $x \geq y > 0$, so that σ and K are strictly increasing in m and s. In addition, we have

$$\forall x, y \in \mathbb{R}_+,\ \frac{\partial \binom{x}{y}}{\partial x}(x,y) = \binom{x}{y}\left(\psi(x+1) - \psi(x-y+1)\right),$$

where ψ is the digamma function defined as $\psi = \Gamma'/\Gamma$. We will also use the following bounds on ψ [26], [27],

$$\forall x \geq 1,\ \ln(x-1/2) < \psi(x) < \ln(x) - \frac{1}{2x} < \ln(x). \quad (5)$$

The proof is organized in four subsections: we first tackle part 1) of Theorem 3 in Subsection A. Then, we show parts 2) a) and 2) b) in Subsection B, parts 2) c) and 2) d) in Subsection C, part 3) in Subsection D.

A. Proof of 1)

Let $m \in \mathbb{R}_{\geq 1}$, we have $\lim_{s\to+\infty} F_{C1}(m,s) = +\infty$ and $F_{C1}(m,0) = \binom{m-1}{m} - K_{min} \leq 0$. We also know that $K(m,\cdot)$ is a strictly increasing function of $s \in \mathbb{R}_+$. Thus, by continuity and monotonicity, there exists a unique $s \in \mathbb{R}_+$ such that $F_{C1}(m,s) = 0$. Conditions (3) of Theorem 2 are satisfied for all $m \in \mathbb{R}_{\geq 1}$, therefore the relation $F_{C1}(m,s) = 0$ induces a unique function $f_{C1}\colon \mathbb{R}_{\geq 1} \to \mathbb{R}_+$ of class C^∞.

$K(\cdot, s)$ is also a strictly increasing function of $m \in \mathbb{R}_{\geq 1}$, for any $s \in \mathbb{R}_+$. We derive from (4) that f_{C1} is strictly decreasing and has an inverse f_{C1}^{-1}. □

B. Proof of 2) a) and 2) b)

Let $m, s \in \mathbb{N}_+$, then

$$R(m,s) = \frac{(m+s(q-1)-1)!\,(s-1)!}{q^m\,(s(q-1)-1)!\,(m+s-1)!}, \quad (6)$$

$$= \frac{1}{q^m}\prod_{i=1}^{m}\left(1 + \frac{s(q-2)}{i+s-1}\right) \leq \frac{1}{q^m}\prod_{i=1}^{m}\left(1 + \frac{s(q-2)}{s}\right), \quad (7)$$

$$= \left(\frac{q-1}{q}\right)^m \leq \frac{q-1}{q}. \quad (8)$$

Eq. (6) comes from the definition of R. Inequality (7) holds since each term of the product satisfies $i-1 \geq 0$. Inequality (8) follows from $(q-1)/q < 1$. It is direct to see that constraint $C2$ has no solution in $\mathbb{N}_+$ if $(q-1)/q < R_{min}$. The equality in Eq. (8) only holds if $m = 1$, therefore only codes with $m = 1$ are possible solutions if $(q-1)/q = R_{min}$. □

C. Proof of 2) c) and 2) d)

Suppose that $(q-1)/q > R_{min}$ and $q = 2$, then $R(m,s) = 2^{-m}$, therefore constraint $C2$ is satisfied if and only if $m \leq -\log_2(R_{min})$.

Now, assume $(q-1)/q > R_{min}$ and $q \geq 3$, it is direct from inequality (8) that constraint $C2$ is only satisfied if $((q-1)/q)^m \geq R_{min}$. Let $a = \max\{1, -\ln(R_{min})/\ln(q)\}$, $b = \ln(R_{min})/\ln((q-1)/q)$, and $m \in [a,b]$. We have by construction $F_{C2}(m,0) = 1/q^m - R_{min} \leq 0$ and $\lim_{s\to+\infty} F_{C2}(m,s) = ((q-1)/q)^m - R_{min}$. Moreover, its partial derivative with respect to $s \in \mathbb{R}_+$ is strictly positive:

$$\frac{\partial F_{C2}}{\partial s}(m,s) = R(m,s)\big[(q-1)\left(\psi(m+s(q-1)) - \psi(s(q-1))\right) - \psi(m+s) + \psi(s)\big] > 0. \quad (9)$$

Hence, by continuity and monotonicity, there exists a unique $s \in \mathbb{R}_+$ such that $F_{C2}(m,s) = 0$. It follows from Theorem 2 and Eq. (9) that the relation $F_{C2}(m,s) = 0$ induces a unique function $f_{C2}\colon [a,b] \to \mathbb{R}_+$ of class C^∞.

For any $m \in [a,b]$, $s \in \mathbb{R}_+$, we show that F_{C2} is strictly decreasing with respect to m as follows

$$\left(\frac{1}{R}\frac{\partial F_{C2}}{\partial m}\right)(m,s) = \psi(m+s(q-1)) - \psi(m+s) - \ln(q),$$

$$< \ln(m+s(q-1)) - \ln(m+s-0.5) - \ln(q), \quad (10)$$

$$= \ln\left(\frac{(q-1)}{q} \times \frac{m/(q-1)+s}{m+s-0.5}\right) < 0. \quad (11)$$

Eq. (10) is obtained by applying inequality (5), and (11) comes from the fact that $(q-1)/q < 1$ and $m/(q-1) \leq m - 0.5$. It follows from (4) that f_{C2} is strictly increasing on $[a,b]$, and it has an inverse f_{C2}^{-1}. □

D. Proof of 3)

Let $m \in \mathbb{R}_{\geq 1}$, we have $\lim_{s\to+\infty} F_{C3}(m,s) = +\infty$ and $F_{C3}(m,1) = 1 - \frac{q^m-1}{q-1} \leq 0$. We know that $\sigma(m,\cdot)$ is strictly increasing on $s \in \mathbb{R}_{\geq 1}$, we derive from Theorem 2 that the relation $F_{C3}(m,s) = 0$ induces a unique function $f_{C3}\colon \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 1}$ of class C^∞.

In order to prove that f_{C3} is strictly increasing, we first show $\frac{\partial F_{C3}}{\partial m}(m, f_{C3}(m)) < 0$. Let $m \in \mathbb{R}_{\geq 1}$ and $s = f_{C3}(m)$,

$$\frac{\partial F_{C3}}{\partial m}(m,s) = \sigma(m,s)\left(\psi(m+s) - \psi(m+1)\right) - \frac{\ln(q)q^m}{q-1},$$

$$< \sigma(m,s)\left(\psi(m+s) - \psi(m+1) - \ln(q)\right), \quad (12)$$

$$< \sigma(m,s)\ln\left(\frac{m+s}{q(m+0.5)}\right). \quad (13)$$

Eq. (12) comes from the fact that $\sigma(m, f_{C3}(m)) = (q^m - 1)/(q-1)$. We obtain (13) by applying inequality (5). Suppose for the sake of contradiction that $m + s \geq q(m+0.5)$, then

$$\sigma(m,s) = \binom{m+s-1}{m} \geq \binom{q(m+0.5)-1}{m} \geq \binom{qm}{m}, \quad (14)$$

$$\geq q^m > \frac{q^m-1}{q-1}. \quad (15)$$

We used $q \geq 2$ in (14) and the well-known property $\frac{x^y}{y^y} \leq \binom{x}{y}$ in (15). This contradicts with $s = f_{C3}(m)$, hence $m + s < q(m + 0.5)$ and (13) is negative. It follows from (4) that f_{C3} is strictly increasing and has an inverse f_{C3}^{-1}. $\square$