Designs, Codes and Cryptography (2023) 91:3915–3932
https://doi.org/10.1007/s10623-023-01279-5

Private simultaneous messages based on quadratic residues

Kazumasa Shinagawa[1,2] · Reo Eriguchi[2] · Shohei Satake[3] · Koji Nuida[2,4]

Received: 13 October 2022 / Revised: 19 June 2023 / Accepted: 15 July 2023 /
Published online: 16 August 2023

Abstract
Private Simultaneous Messages (PSM) model is a minimal model for secure multiparty computation. Feige, Kilian, and Naor (STOC 1994) and Ishai (Cryptology and Information Security Series 2013) constructed PSM protocols based on quadratic residues. In this paper, we define QR-PSM protocols as a generalization of these protocols. A QR-PSM protocol is a PSM protocol whose decoding function outputs the quadratic residuosity modulo p of what is computed from messages. We design a QR-PSM protocol for any symmetric function $f : \{0,1\}^n \to \{0,1\}$ of communication complexity $O(n^2)$. As far as we know, it is the most efficient PSM protocol for symmetric functions since the previously known best PSM protocol was of $O(n^2 \log n)$ (Beimel et al., CRYPTO 2014). We also study the sizes of the underlying finite fields $\mathbb{F}_p$ in the protocols since the communication complexity of a QR-PSM protocol is proportional to the bit length of the prime p. We show that there is a prime $p \leq (1 + o(1))N^2 2^{2N-2}$ such that any length-N pattern of quadratic (non)residues appears modulo p (and hence it can be used for general QR-PSM protocols), which improves the Peralta's known result (Mathematics of Computation 1992) by a constant factor $(1 + \sqrt{2})^2$.

Keywords Secure multiparty computation · Private simultaneous messages · Quadratic residues · Symmetric functions · Paley graphs

Mathematics Subject Classification 94A60 · 11T71 · 14G50 · 05C90

Communicated by O. Ahmadi.

✉ Kazumasa Shinagawa
kazumasa.shinagawa.np92@vc.ibaraki.ac.jp

1 Ibaraki University, 4-12-1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan

2 National Institute of Advanced Industrial Science and Technology (AIST), 2-3-26 Aomi, Koto, Tokyo 135-0064, Japan

3 Kumamoto University, 2-39-1 Kurokami, Chuo, Kumamoto 860-8555, Japan

4 Institute of Mathematics for Industry (IMI), Kyushu University, 744 Motooka, Nishi, Fukuoka 819-0395, Japan

1 Introduction

Private Simultaneous Messages (PSM) model introduced by Feige et al. [19] and named by Ishai and Kushilevitz [22] is a minimal model for non-interactive secure multiparty computation with information-theoretic security. In the PSM model, there are n *players* and a special party called the *referee*. Each player P_i computes a message m_i from P_i's input x_i and a *shared randomness* r, and sends m_i to the referee. Here, the shared randomness r is known by all players but the referee. Given n messages $m_1, m_2, \ldots, m_n$, the referee computes an output value y, which is expected to be $y = f(x_1, x_2, \ldots, x_n)$ for a function f agreed upon by all players and the referee. The security of the protocol ensures that the referee cannot learn anything about the secret inputs beyond what can be inferred from the output value. The efficiency of PSM protocols is mainly measured by the communication complexity $\sum_{i=1}^{n} |m_i|$, where $|\cdot|$ denotes the bit length.

1.1 PSM protocols based on quadratic residues

We review two existing PSM protocols based on quadratic residues. Feige et al. [19] proposed such a protocol for comparing two numbers x and y, i.e., deciding whether $x \geq y$ or not. Ishai [23] designed such a protocol for any function $f : \{0,1\}^n \to \{0,1\}$.

1.1.1 Feige–Kilian–Naor's protocol

The protocol based on quadratic residues by Feige et al. [19] is a two-player PSM protocol computing the comparison function $\mathsf{COMP} : \{0,1,2\} \times \{0,1,2\} \to \{-1,0,1\}$ as follows:

$$\mathsf{COMP}(x_1, x_2) = \begin{cases} 1 & \text{if } x_1 > x_2, \\ 0 & \text{if } x_1 = x_2, \\ -1 & \text{if } x_1 < x_2. \end{cases}$$

The shared randomness of the protocol is a pair (r_1, r_2) of an element r_1 of $\mathbb{Z}/7\mathbb{Z}$ and a nonzero quadratic residue r_2 modulo 7. The first player P_1 computes a message $m_1 \in \mathbb{Z}/7\mathbb{Z}$ as $m_1 := r_1 + r_2 x_1 \pmod 7$, and the second player P_2 computes a message $m_2 \in \mathbb{Z}/7\mathbb{Z}$ as $m_2 := -r_1 - r_2 x_2 \pmod 7$. Given m_1, m_2, the referee computes the quadratic residuosity of $m := m_1 + m_2 \pmod 7$, and outputs 1 if m is a non-zero quadratic residue, -1 if m is a quadratic nonresidue, and 0 if $m = 0$.

1.1.2 Ishai's protocol

The protocol based on quadratic residues by Ishai [23] is an n-player PSM protocol computing any function $f : \{0,1\}^n \to \{0,1\}$. Let p be a prime and $0 < a \leq p - 2^n$ an integer such that $a + \sum_{i=1}^{n} 2^{i-1} b_i$ is a quadratic residue modulo p if and only if $f(b_1, b_2, \ldots, b_n) = 1$. From the result by Peralta [25], such a prime p with $p = 2^{O(n)}$ exists. The shared randomness of the protocol is a tuple $(r_0, r_1, r_2, \ldots, r_n)$ of a nonzero quadratic residue r_0 modulo p and $r_1, r_2, \ldots, r_n \in \mathbb{Z}/p\mathbb{Z}$ such that $\sum_{i=1}^{n} r_i \equiv 0 \pmod p$. The player P_i holding $x_i \in \{0,1\}$ computes a message $m_i \in \mathbb{Z}/p\mathbb{Z}$ as $m_i := 2^{i-1} r_0 x_i + r_i \pmod p$ if $2 \leq i \leq n$ and $m_1 := r_0(a + x_1) + r_1 \pmod p$ if $i = 1$. Given $m_1, m_2, \ldots, m_n$, the referee computes the quadratic residuosity of $m := \sum_{i=1}^{n} m_i \pmod p$, and outputs 1 if m is a quadratic residue and -1 otherwise. The communication complexity of this protocol is $O(n \cdot 2^n)$.

Table 1 The communication complexity of QR-PSM protocols (see Sect. 3.2 for the notations)

	function	comm. complexity
Ishai [23]	any function	$O(n \cdot 2^n)$
Corollary 7	symmetric function	$O(n^2)$
Corollary 8	weighted threshold function with weight $\boldsymbol{w}$	$O(n \cdot \sum_{i=1}^{n} \lvert w_i \rvert)$
Proposition 20	AND function	$o(n^2)$
Proposition 21	equality (EQ) function	$o(n^2)$

1.2 Our contributions

First, we introduce the notions of *quadratic residue based PSM (QR-PSM) protocols* and *linear QR-PSM (LQR-PSM) protocols*. Let p be a prime. A QR-PSM protocol modulo p is a PSM protocol such that the decoding function of the protocol outputs the quadratic residuosity (Legendre symbol) of $\phi(m_1, m_2, \ldots, m_n)$ modulo p, where ϕ is a function from messages to $\mathbb{Z}/p\mathbb{Z}$, and m_i is the i-th message for $1 \leq i \leq n$. An LQR-PSM protocol modulo p is a QR-PSM protocol modulo p such that $\phi(m_1, m_2, \ldots, m_n) = \sum_{i=1}^{n} m_i \pmod{p}$. We remark that Feige-Kilian-Naor's protocol and Ishai's protocol are LQR-PSM protocols.

Next, we construct new QR-PSM and LQR-PSM protocols. For any symmetric function $f : \{0,1\}^n \to \{0,1\}$, which is a function whose value is independent of the order of the inputs, we obtain an LQR-PSM protocol of communication complexity $O(n^2)$. We note that this is the most efficient PSM protocol for symmetric functions so far since the previously known best protocol was of $O(n^2 \log n)$ proposed by Beimel et al. [9]. (We note that some concrete symmetric function can have more efficient LQR-PSM protocols. Indeed, we obtain LQR-PSM protocols with communication complexity $o(n^2)$ for AND and equality (EQ) functions.) For any weighted threshold function $f : \{0,1\}^n \to \{0,1\}$ with weight vector $\boldsymbol{w}$ and threshold t, we also obtain an LQR-PSM protocol of communication complexity $O(n \cdot \sum_{i=1}^{n} \lvert w_i \rvert)$. We remark that these protocols are more efficient than the protocols obtained by applying Ishai's protocol to these specific functions (see Table 1 for efficiency comparison). In addition, we show that QR-PSM protocols can be obtained from decomposable randomized encodings (DRE). In particular, we show that if a function f is "embedded" into another function g and g admits a DRE of output length s, we have a QR-PSM protocol with communication complexity $O(s \cdot l(g))$, where $l(g)$ is the "embedding length" of g (see Sect. 3.2 for the definition of the embedding). This construction can be viewed as a generalization of our LQR-PSM protocols since it admits not only linear polynomials but also higher-degree polynomials.

In QR-PSM protocols, the communication complexity is dominated by the size of modulus p. Thus, it is important to give upper and lower bounds on the primes. We study two kinds of primes which we name the *Peralta primes* and the *LQR-PSM primes*: the n-th Peralta prime P_n is the smallest prime p such that every n-bit string appears in the "quadratic residue sequence modulo p" as a subsequence; and the n-th LQR-PSM prime L_n is the smallest prime p such that every function $f : \{0,1\}^n \to \{0,1\}$ has an LQR-PSM protocol modulo p. We first show that $L_n \leq P_{2^{n-1}}$ and $L_n \geq 2^{\frac{2^n-2}{n}}$. We show that $P_n \leq (1 + o(1))n^2 2^{2n-2}$, an upper bound on the Peralta primes, by using graph theory. As a result, we also obtain a lower bound on the LQR-PSM primes. We note that our upper bound on the Peralta primes is tighter than that implied from the result by Peralta [25].

1.3 Related work

The PSM model was firstly introduced by Feige et al. [19]. Besides the QR-PSM protocol described in Sect. 1.1.1, they also constructed a two-player PSM protocol for any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ of complexity $O(2^n)$. Beimel, Ishai, Kumaresan, and Kushilevitz [10] improved it to $O(2^{n/2})$ by introducing a decomposable private information retrieval protocol. This is still the state-of-the-art two-player PSM protocol among those applicable to arbitrary function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. As an impossibility result, Applebaum, Holenstein, Mishra, and Shayevitz [4] showed that any two-player PSM protocol computing a random function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ requires the complexity $3n - O(\log n)$. Narrowing this exponential gap between the upper and lower bounds is an important open problem in cryptography [27].

For the case of k players for $k \geq 3$, Beimel et al. [11] constructed a k-player PSM protocol for any function $f : (\{0,1\}^n)^k \to \{0,1\}$ of complexity $O(poly(k) \cdot 2^{nk/2})$. Assouline and Liu [5] improved it to $O(2^{n(k-1)/2})$ for infinitely many k's and conjectured that it holds for any k.

For a specific class of functions, Ishai and Kushilevitz [22] constructed a PSM protocol for a Boolean modulo-p branching program $BP : \{0,1\}^n \to \{0,1\}$ of size a with communication complexity $O(\log p \cdot n \cdot a^2)$.

Ball, Holmgren, Ishai, Liu, and Malkin [7] and Ball and Randolph [8] showed lower bounds of the communication complexity of PSM protocols for certain functions. They also designed LQR-PSM protocols for "computing quadratic residuosity" as pseudorandom functions.

1.4 Organization

In Sect. 2, we introduce the basic notations (Sect. 2.1), PSM protocols (Sect. 2.2), decomposable randomized encodings (Sect. 2.3), and the notations related to quadratic residues (Sect. 2.4). In Sect. 3, we define QR-PSM protocols (Sect. 3.1), construct LQR-PSM protocols for symmetric functions and weighted threshold functions (Sect. 3.2), and construct QR-PSM protocols from decomposable randomized encodings (Sect. 3.3). In Sect. 4, we show upper and lower bounds on the LQR-PSM primes (Sect. 4.1), define Paley graphs and tournaments (Sect. 4.2), and give an upper bound on Peralta primes (Sect. 4.3). In Appendix, we show that AND and EQ functions have LQR-PSM protocols with communication complexity $o(n^2)$.

2 Preliminaries

2.1 Notations

For an integer $n \geq 2$, we denote $[n] := \{1, 2, \ldots, n\}$ and $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$. For a set S, we denote by $\#S$ the cardinality of S. For a bit string $m \in \{0,1\}^*$, we denote by $|m|$ the bit length of m. For an integer $a \in \mathbb{Z}$, we denote by $|a|$ the absolute value of a.

Let A be a ring. An *arithmetic formula* over A is a rooted binary tree, where each leaf is labeled by either an input variable x_i $(1 \leq i \leq n)$ or a constant $c \in A$, and each intermediate node called a *gate* is labeled by either addition or multiplication. Its *depth* is defined by the length of the longest path from the root to a leaf. An arithmetic formula can be regarded as a function $f : A^n \to A$ naturally. A *Boolean formula* is an arithmetic formula over $A = \mathbb{Z}_2$. In this paper, the basis of Boolean formulas is always $\{\wedge, \oplus\}$.

A *polynomial* over A is a polynomial whose coefficients are elements of A. A polynomial can be regarded as a function $f : A^n \to A$ naturally. Every arithmetic formula over A can be represented by a polynomial over A. In particular, every Boolean formula $f : \{0,1\}^n \to \{0,1\}$ can be represented by a polynomial over $\mathbb{Z}_2$ (over the basis $\{\wedge, \oplus\}$), which is called the *Reed-Muller canonical form* of f.

2.2 PSM protocols

Definition 1 (*PSM protocol*) Let $n \geq 2$ be an integer, and $X_1, X_2, \ldots, X_n, Y, R, M_1, M_2, \ldots, M_n$ finite sets. Set $X = \prod_{1 \leq i \leq n} X_i$ and $M = \prod_{1 \leq i \leq n} M_i$. Let $\mathsf{Enc}_i : X_i \times R \to M_i$ $(1 \leq i \leq n)$ and $\mathsf{Dec} : M \to Y$ be functions. Here, $X_i, Y, R, M_i, \mathsf{Enc}_i, \mathsf{Dec}$ $(1 \leq i \leq n)$ are called the *i-th input space*, the *output space*, the *randomness space*, the *i-th message space*, the *i-th encoding function*, and the *decoding function*, respectively. A *private simultaneous messages (PSM) protocol* Π for a function $f : X \to Y$ is a 7-tuple

$$\Pi = (n, X, Y, R, M, (\mathsf{Enc}_i)_{1 \leq i \leq n}, \mathsf{Dec}),$$

satisfying the following conditions:

Correctness. For any $(x_1, \ldots, x_n) \in X$ and any $r \in R$, it holds that

$$\mathsf{Dec}((\mathsf{Enc}_1(x_1, r), \ldots, \mathsf{Enc}_n(x_n, r)) = f(x_1, \ldots, x_n).$$

Security. For any $m \in M$ and $x = (x_1, \ldots, x_n), x' = (x'_1, \ldots, x'_n) \in X$ with $f(x) = f(x')$, it holds that

$$\Pr_{r \in R}\big[(\mathsf{Enc}_1(x_1, r), \ldots, \mathsf{Enc}_n(x_n, r)) = m\big] = \Pr_{r \in R}\big[(\mathsf{Enc}_1(x'_1, r), \ldots, \mathsf{Enc}_n(x'_n, r)) = m\big],$$

where $r \in R$ is chosen uniformly at random.

The communication complexity is defined by $\sum_{i=1}^{n} \log_2(\#M_i)$ and the randomness complexity is defined by $\log_2(\#R)$.

2.3 Decomposable randomized encodings

In this section, we define the notions of *randomized encodings* and *decomposable randomized encodings (DRE)*. A DRE over $\mathbb{Z}_p$ for a prime p is used as a building block for constructing QR-PSM protocols.

Definition 2 (*Randomized encoding*) Let $X, Y, \hat{Y}, R$ be finite sets, and $f : X \to Y$ a function. A *randomized encoding* $\hat{f} : X \times R \to \hat{Y}$ is a function satisfying the following conditions:

Correctness. There exists a function $\mathsf{Dec} : \hat{Y} \to Y$ called a *decoder* such that for any $x \in X$ and $r \in R$, it holds $\mathsf{Dec}(\hat{f}(x, r)) = f(x)$.

Security. For any $\hat{y} \in \hat{Y}$ and $x, x' \in X$ such that $f(x) = f(x')$, it holds that

$$\Pr_{r \in R}\big[\hat{f}(x, r) = \hat{y}\big] = \Pr_{r \in R}\big[\hat{f}(x', r) = \hat{y}\big],$$

where $r \in R$ is chosen uniformly at random.

Definition 3 (*DRE*) Let A be a finite ring, and $f : A^n \to A$ a function. A *decomposable randomized encoding (DRE)* of f is a randomized encoding $\hat{f} : A^n \times A^m \to A^s$ as follows:

$$\hat{f}((x_1, x_2, \ldots, x_n), r) = (\hat{f}_0(r), \hat{f}_1(x_1, r), \hat{f}_2(x_2, r), \ldots, \hat{f}_n(x_n, r))$$

where $\hat{f}_0 : A^m \to A^{s_0}$ and $\hat{f}_i : A \times A^m \to A^{s_i}$ $(1 \leq i \leq n)$ are functions such that $\sum_{i=0}^{n} s_i = s$. The integer s is called the *output length* of the DRE.

For a function $f : \mathbb{Z}^n \to \mathbb{Z}$, we define the *DRE complexity* of f.

Definition 4 (*DRE complexity*) Let $f : \mathbb{Z}^n \to \mathbb{Z}$ be a function. For a prime p, define $f_p : \mathbb{Z}_p^n \to \mathbb{Z}_p$ as the function such that $f_p \equiv f \pmod{p}$. The *DRE complexity* of f, denoted by $\mathsf{D}(f)$, is defined by the minimum integer s such that for every prime p, there exists a DRE of f_p with output length at most s.

Based on Cleve's result [16] on straight-line programs, Cramer, Fehr, Ishai, and Kushilevitz designed a constant-round multiparty computation protocol for arithmetic formulas [18, Theorem 3]. This construction can be viewed as a DRE of arithmetic formulas.

Theorem 1 (Cramer-Fehr-Ishai-Kushilevitz [18]) *Let $f : A^n \to A$ be an arithmetic formula of depth d. Then, there exists a DRE of f with output length $2^{d+O(\sqrt{d})}$.*

Corollary 2 *Let $f : \mathbb{Z}^n \to \mathbb{Z}$ be an arithmetic formula of depth d. Then, we have $\mathsf{D}(f) \leq 2^{d+O(\sqrt{d})}$.*

Based on Theorem 1, we have a DRE of polynomials.

Theorem 3 *Let $f : A^n \to A$ be a degree-k polynomial having m terms. Then, there exists a DRE of f with output length $m \cdot k \cdot 2^{O(\sqrt{\log k})}$.*

Proof Let $g : A^{k+1} \to A$ be a function such that $g(y_0, y_1, \ldots, y_k) = y_0 + \prod_{i=1}^{k} y_i$. Since g can be represented by an arithmetic formula of depth $d = \lceil \log_2 k \rceil + 1$, it has a DRE with output length $2^{d+O(\sqrt{d})} = k \cdot 2^{O(\sqrt{\log k})}$ from Theorem 1. Suppose that the i-th term of f is a degree-k' term of the form $c x_{j_1} x_{j_2} \cdots x_{j_{k'}}$ $(c \in A, k' \leq k)$. Let $r_1, r_2, \ldots, r_m \in A$ be random numbers such that $\sum_{i=1}^{m} r_i = 0$. Then, we have a DRE of $c x_{j_1} x_{j_2} \cdots x_{j_{k'}} + r_i$ from the DRE of g, by setting

$$(y_0, y_1, y_2, \ldots, y_{k'}, y_{k'+1}, y_{k'+2}, \ldots, y_k) \leftarrow (r_i, c x_{j_1}, x_{j_2}, \ldots, x_{j_{k'}}, 1, 1, \ldots, 1).$$

Juxtaposing them for each term, we obtain the DRE of f with output length $m \cdot k \cdot 2^{O(\sqrt{\log k})}$. □

Let $f : A^n \to A$ be a degree-k polynomial having m terms. Since f can be represented by an arithmetic formula of depth $d = \lceil \log_2 k \rceil + \lceil \log_2 m \rceil$, Theorem 1 results in a DRE of f with output length $2^{\log_2 d + O(\sqrt{d})} = m \cdot k \cdot 2^{O(\sqrt{\log k + \log m})}$. On the other hand, Theorem 3 results in a DRE of f with output length $m \cdot k \cdot 2^{O(\sqrt{\log k})}$. Thus, Theorem 3 is more efficient than Theorem 1 by the factor $2^{O(\sqrt{\log m})}$ in this case.

2.4 Quadratic residues

We denote by $\mathcal{R}_p \subset \mathbb{Z}_p$ the set of non-zero quadratic residues modulo p and by $\mathcal{N}_p \subset \mathbb{Z}_p$ the set of quadratic nonresidues modulo p. For an integer $a \in \mathbb{Z}$, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if a} \not\equiv 0 \pmod{p} \text{ is a quadratic residue modulo p,} \\ 0 & \text{if a} \equiv 0 \pmod{p}, \\ -1 & \text{if a is a quadratic nonresidue modulo p.} \end{cases}$$

For a prime p, we define *the quadratic residue sequence modulo* p as the string $\mathsf{S}_p \in \{0,1\}^{p-1}$ such that for every $i \in [p-1]$, the i-th bit (from the left) of S_p is equal to 1 if $\left(\frac{i}{p}\right) = 1$ and 0 otherwise. If a string $t \in \{0,1\}^*$ is a substring of S_p, then we say that S_p *contains* t. The quadratic residue sequences modulo primes from 2 to 19 are shown as follows:

p	S_p
2	1
3	10
5	1001
7	110100
11	1011100010
13	101100001101
17	1101000110001011
19	1001111010100001 10

By Weil's character sum estimation over finite fields, Peralta [25] gave a sufficient condition on primes for containing every n-bit string $t \in \{0,1\}^n$.

Theorem 4 (Peralta [25]) *Let p be a prime. If $p \cdot \left(\frac{1}{2}\right)^n > n(\sqrt{p}+3)$, then S_p contains every n-bit string $t \in \{0,1\}^n$.*

We say that a prime p is *n-Peralta* if S_p contains every n-bit string $t \in \{0,1\}^n$. We define *the n-th Peralta prime* P_n as the smallest n-Peralta prime. The n-th Peralta primes for $1 \le n \le 8$ obtained by computer experiments are shown as follows:

n	1	2	3	4	5	6	7	8
P_n	3	7	11	37	67	181	367	1091

Applying the Baker-Harman-Pintz theorem on prime gaps in [6], we obtain the following corollary.

Corollary 5 *For any sufficiently large n, there exists an n-Peralta prime p with $p \le c + c^{0.525}$, where $c = (1+\sqrt{2})^2 n^2 2^{2n-2}$. Hence, $\log P_n = O(n)$ holds.*

Proof From Theorem 4, any prime p satisfying

$$\sqrt{p} > n2^{n-1} + \sqrt{n^2 2^{2n-2} + 3n2^n}$$

is n-Peralta. As $\sqrt{2}n2^{n-1} > \sqrt{n^2 2^{2n-2} + 3n2^n}$ for all $n \geq 3$, any prime p satisfying

$$\sqrt{p} > (1 + \sqrt{2})n2^{n-1}$$

is also n-Peralta. By the Baker-Harman-Pintz theorem on prime gaps, there exists a prime p in $[c, c + c^{0.525}]$ for $c = (1 + \sqrt{2})^2 n^2 2^{2n-2}$, as desired. □

In Sect. 4.3, we improve the upper bound on Peralta primes by a constant factor $(1+\sqrt{2})^2$.

3 QR-PSM protocols

3.1 Definition of QR-PSM protocols

We define quadratic residue based PSM protocols. It is a PSM protocol whose decoding function outputs the Legendre symbol of an element of $\mathbb{Z}_p$ which is computed from messages.

Definition 5 (*QR-PSM protocol*) Let $\Pi = (n, X, Y, R, M, (\mathsf{Enc}_i)_{1 \leq i \leq n}, \mathsf{Dec})$ be a PSM protocol such that $Y = \{-1, 0, 1\}$. Let p be a prime. We say that Π is a *quadratic residue based PSM (QR-PSM) protocol modulo p* if there exists a function $\phi : M \to \mathbb{Z}_p$ such that for any $(m_1, \ldots, m_n) \in M$,

$$\mathsf{Dec}(m_1, m_2, \ldots, m_n) = \left(\frac{\phi(m_1, m_2, \ldots, m_n)}{p}\right).$$

We remark that Feige-Kilian-Naor's protocol (see Sect. 1.1.1) is a QR-PSM protocol modulo 7. We also point out that Ishai's protocol (see Sect. 1.1.2) is a QR-PSM protocol modulo a prime p.

Let $f : \{0, 1\}^n \to \{0, 1\}$ be a Boolean function. We say that a QR-PSM protocol computes f if it outputs $(-1)^{f(x)}$. Throughout this paper, we focus on the QR-PSM protocols for Boolean functions in this sense.

3.2 LQR-PSM protocols

We say that a function $f : \{0, 1\}^n \to \{0, 1\}$ is *embedded* into a function $g : \mathbb{Z}^n \to \mathbb{Z}$ if $g(x) = g(x')$ implies $f(x) = f(x')$ for any $x, x' \in \{0, 1\}^n$. The function g is called an *embedding of f*. The *embedding length* of g, denoted by $l(g)$, is defined as follows:

$$l(g) := \max_{x \in \{0,1\}^n} (g(x)) - \min_{x \in \{0,1\}^n} (g(x)) + 1.$$

If a function $f : \{0, 1\}^n \to \{0, 1\}$ can be embedded into a linear function $g = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$, we obtain an efficient QR-PSM protocol which we call a *linear QR-PSM (LQR-PSM) protocol*.

Definition 6 (*Linear QR-PSM protocol*) Let p be a prime and $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Z}_p$. *A linear QR-PSM (LQR-PSM) protocol modulo p*, denoted by $[a_0, a_1, a_2, \ldots, a_n]_p$, is a QR-PSM protocol $\Pi = (n, \{0, 1\}^n, \{-1, 0, 1\}, R, \mathbb{Z}_p^n, (\mathsf{Enc}_i)_{1 \leq i \leq n}, \mathsf{Dec})$ modulo p in the following.

- The randomness space R is

$$R = \left\{ (r_0, r_1, r_2, \ldots, r_n) \in \mathbb{Z}_p^{n+1} \;\middle|\; r_0 \in \mathcal{R}_p,\ \sum_{i=1}^{n} r_i \equiv 0 \pmod{p} \right\}.$$

- The encoding function $\mathsf{Enc}_i : \{0,1\} \times R \to \mathbb{Z}_p$ is

$$\mathsf{Enc}_i(x_i, r) = \begin{cases} r_0(a_0 + a_i x_i) + r_i \pmod{p} & \text{if } i = 1, \\ r_0 a_i x_i + r_i \pmod{p} & \text{otherwise,} \end{cases}$$

  where $r = (r_0, r_1, r_2, \ldots, r_n) \in R$ and $x_i \in \{0,1\}$.
- The decoding function $\mathsf{Dec} : (\mathbb{Z}_p)^n \to \{-1, 0, 1\}$ is

$$\mathsf{Dec}(m_1, m_2, \ldots, m_n) = \left(\frac{\sum_{i=1}^{n} m_i}{p} \right).$$

Remark 1 Let $[a_0, a_1, a_2, \ldots, a_n]_p$ be an LQR-PSM protocol for a function $f : \{0,1\}^n \to \{0,1\}$. Then for any quadratic nonresidue $a' \in \mathcal{N}_p$, $[a_0, a'a_1, a'a_2, \ldots, a'a_n]_p$ is an LQR-PSM protocol for the negated function f' such that $f'(x) = f(x) \oplus 1$ for all $x \in \{0,1\}^n$. Thus, in general, an LQR-PSM protocol for a function implies an LQR-PSM protocol for the negated function with the same efficiency.

Theorem 6 *Let $f : \{0,1\}^n \to \{0,1\}$ be a function. Let $g : \mathbb{Z}^n \to \mathbb{Z}$ be an embedding of f such that $g = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ for some $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Then, there exists an LQR-PSM protocol for f with communication complexity $n \cdot \log_2 P_{l(g)}$, where $P_{l(g)}$ is the $l(g)$-th Peralta prime.*

Proof Set $p := P_{l(g)}$. Since p is the $l(g)$-th Peralta prime, there exists $a_0 \in \mathbb{Z}_p$ such that $\left(\frac{a_0 + g(x)}{p} \right) = (-1)^{f(x)}$ for all $x \in \{0,1\}^n$. We claim that $[a_0, a_1, a_2, \ldots, a_n]_p$ is an LQR-PSM protocol for f. By setting $m_i := \mathsf{Enc}_i(x_i, r)$, we have

$$(m_1, m_2, \ldots, m_n) = (r_0(a_0 + a_1x_1) + r_1, r_0a_2x_2 + r_2, \ldots, r_0a_nx_n + r_n).$$

Since r_0 is a nonzero quadratic residue, we have

$$\left(\frac{\sum_{i=1}^{n} m_i}{p} \right) = \left(\frac{r_0(a_0 + a_1x_1 + \cdots + a_nx_n)}{p} \right) = \left(\frac{r_0(a_0 + g(x))}{p} \right) = \left(\frac{a_0 + g(x)}{p} \right).$$

Thus, it correctly computes f. The communication complexity of the protocol is $n \cdot \log_2 P_{l(g)}$. □

Theorem 6 implies a protocol for any symmetric function.

Corollary 7 *For any symmetric function $f : \{0,1\}^n \to \{0,1\}$, there exists an LQR-PSM protocol with communication complexity $n \cdot \log_2 P_{n+1} = O(n^2)$.*

Proof It follows from Theorem 6 since any symmetric function is embedded to a linear function $g(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \cdots + x_n$ of embedding length $n + 1$. □

A weighted threshold function $f_{\boldsymbol{w},t}$ associated with $\boldsymbol{w} = (w_1, w_2, \ldots, w_n) \in \mathbb{Z}^n$ and $t \in \mathbb{N}$ is defined as

$$f_{\boldsymbol{w},t}(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & \text{if } \sum_{i=1}^{n} w_i x_i \geq t, \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 8 *For any $\boldsymbol{w} \in \mathbb{Z}^n$ and $t \in \mathbb{N}$, there exists an LQR-PSM protocol for the weighted threshold function $f_{\boldsymbol{w},t} : \{0,1\}^n \to \{0,1\}$ associated with $\boldsymbol{w}, t$ with communication complexity $n \cdot \log_2 P_{W+1} = O(n \cdot W)$ for $W = \sum_{i=1}^n |w_i|$.*

Proof It follows from Theorem 6 since a weighted threshold function associated with $\boldsymbol{w}, t$ is embedded to a linear function $g(x_1, x_2, \ldots, x_n) = w_1x_1 + w_2x_2 + \cdots + w_nx_n$ of embedding length $\sum_{i=1}^n |w_i| + 1$. □

Theorem 6 also implies Ishai's protocol (see Subsect. 1.1.2).

Corollary 9 (Ishai [23]) *For any function $f : \{0,1\}^n \to \{0,1\}$, there exists an LQR-PSM protocol with communication complexity $n \cdot \log_2 P_{2^n} = O(n \cdot 2^n)$.*

Proof It follows from Theorem 6 since any function $f : \{0,1\}^n \to \{0,1\}$ is embedded to a linear function $g(x_1, x_2, \ldots, x_n) = x_1 + 2x_2 + \cdots 2^{i-1}x_i + \cdots + 2^{n-1}x_n$ of embedding length 2^n. □

We also obtain an LQR-PSM protocol for a composition of symmetric functions.

Corollary 10 *Let $h : \{0,1\}^m \to \{0,1\}$ be any function and $g_i : \{0,1\}^k \to \{0,1\}$ $(1 \le i \le m)$ be symmetric functions. Set $n = mk$. Define a function $f : \{0,1\}^n \to \{0,1\}$ as follows:*

$$f(x_1, x_2, \ldots, x_n) = h(g_1(x_1, \ldots, x_k), g_2(x_{k+1}, \ldots, x_{2k}), \ldots, g_m(x_{n-k+1}, \ldots, x_n)).$$

Then, there exists an LQR-PSM protocol for f with communication complexity $n \cdot \log_2 P_L = O(n \cdot L)$ for $L = (k+1)^{n/k}$.

Proof We can observe that the function f can be embedded to a linear function $g : \mathbb{Z}^n \to \mathbb{Z}$ in the following:

$$g(x_1, \ldots, x_n) = \sum_{i=1}^{k} x_i + \sum_{i=k+1}^{2k} (k+1)x_i + \sum_{i=2k+1}^{3k} (k+1)^2 x_i + \cdots + \sum_{i=(m-1)k+1}^{mk} (k+1)^{m-1} x_i.$$

We have

$$l(g) = 1 + k + (k+1)k + (k+1)^2 k + \cdots + (k+1)^{m-1}k = (k+1)^{n/k}.$$

From Theorem 6, we have an LQR-PSM protocol with communication complexity $n \cdot \log_2 P_L = O(n \cdot L)$ for $L = (k+1)^{n/k}$. □

Remark 2 By setting $(m, k) = (1, n)$, we obtain Corollary 7. By setting $(m, k) = (n, 1)$, we obtain Corollary 9. In this sense, Corollary 10 is a generalization of Corollaries 7 and 9.

By computer experiment, it is possible to enumerate all LQR-PSM protocols for small prime numbers, thereby identifying a minimal LQR-PSM protocol for computing a specific function. By this way, we obtain LQR-PSM protocols for several symmetric functions with minimum communication complexity in Table 2: AND is the logical AND function, XOR is the logical exclusive OR function, EQ is a function that outputs 1 if and only if all bits are equal, and MAJ is a function which outputs 1 if and only if half or more bits are 1. Note that these protocols are more efficient than those of Corollary 7.

Table 2 The list of LQR-PSM protocols for AND, XOR, EQ, and MAJ

n AND	XOR	EQ	MAJ
2	$[2, 1, 1]_5$	$[2, 2, 4]_5$	$[1, 1, 2]_5$	$[2, 2, 2]_5$
3	$[6, 1, 1, 1]_{11}$	$[6, 3, 3, 3]_7$	$[1, 1, 1, 1]_5$	$[3, 3, 3, 2]_7$
4	$[5, 1, 1, 1, 1]_{13}$	$[12, 1, 1, 1, 7]_{17}$	$[5, 1, 1, 1, 1]_{11}$	$[6, 2, 2, 2, 2]_{11}$
5	$[11, 1, 1, 1, 1, 1]_{41}$	$[14, 2, 2, 2, 2, 2]_{19}$	$[4, 1, 1, 1, 1, 1]_{13}$	$[6, 2, 2, 2, 2, 2]_{11}$
6	$[18, 1, 1, 1, 1, 1, 1]_{53}$	$[15, 1, 1, 1, 1, 1, 6]_{41}$	$[10, 1, 1, 1, 1, 1, 1]_{41}$	$[21, 3, 3, 3, 3, 3, 3]_{31}$
7	$[52, 1, 1, 1, 1, 1, 1, 1]_{83}$	$[35, 1, 1, 1, 1, 1, 1, 1]_{79}$	$[17, 1, 1, 1, 1, 1, 1, 1]_{53}$	$[21, 3, 3, 3, 3, 3, 3, 2]_{31}$

3.3 QR-PSM protocols from DREs

In this subsection, we construct QR-PSM protocols from DREs.

Theorem 11 *Let $f : \{0,1\}^n \to \{0,1\}$ be a function, and $g : \mathbb{Z}^n \to \mathbb{Z}$ an embedding of f. Let $h : \mathbb{Z}^{n+2} \to \mathbb{Z}$ be a function such that $h(x_1, x_2, \ldots, x_{n+2}) := (g(x_1, x_2, \ldots, x_n) + x_{n+1}) \cdot x_{n+2}$. Then, there exists a QR-PSM protocol computing f with communication complexity $O(\mathsf{D}(h) \cdot l(g))$.*

Proof From Theorem 4 and Corollary 5, there exists a prime p with $\log_2 p = O(l(g))$ containing every $l(g)$-bit string. Since $g(x) = g(x')$ implies $f(x) = f(x')$, we can take an offset $a_0 \in \mathbb{Z}_p$ such that $\left(\frac{a_0 + g(x)}{p}\right) = (-1)^{f(x)}$ for all $x \in \{0,1\}^n$.

From the assumption of the statement, there exists a DRE of $h = (g + x_{n+1}) \cdot x_{n+2}$ with output length $\mathsf{D}(h)$. Set $s := \mathsf{D}(h)$. Let $\hat{h} : \mathbb{Z}_p^{n+2} \times \mathbb{Z}_p^m \to \mathbb{Z}_p^s$ be the DRE of $h = (g + x_{n+1}) \cdot x_{n+2}$ with output complexity s. It has the following form:

$$\hat{h}((x_1, x_2, \ldots, x_{n+2}), r) = (\hat{h}_0(r), \hat{h}_1(x_1, r), \hat{h}_2(x_2, r), \ldots, \hat{h}_{n+2}(x_{n+2}, r))$$

where $\hat{h}_0 : \mathbb{Z}_p^m \to \mathbb{Z}_p^{s_0}$ and $\hat{h}_i : \mathbb{Z}_p \times \mathbb{Z}_p^m \to \mathbb{Z}_p^{s_i}$ $(1 \le i \le n+2)$ are functions such that $\sum_{i=0}^{n+2} s_i = s$. Let $\mathsf{dec} : \mathbb{Z}_p^s \to \mathbb{Z}_p$ be the decryption function of the DRE.

The QR-PSM protocol $\Pi = (n, \{0,1\}^n, \{-1, 0, 1\}, R, M, (\mathsf{Enc}_i)_{1 \le i \le n}, \mathsf{Dec})$ modulo p is defined as follows:

- $M_1 = \mathbb{Z}_p^{s_0 + s_1 + s_{n+1} + s_{n+2}}$ and $M_i = \mathbb{Z}_p^{s_i}$ for all $2 \le i \le n$.
- $R = \mathbb{Z}_p^m \times \mathcal{R}_p$. (Recall that $\mathcal{R}_p$ is the set of nonzero quadratic residues modulo p).
- $\mathsf{Enc}_1(x_1, (r, r')) = (\hat{h}_0(r), \hat{h}_1(r' \cdot x_1, r), \hat{h}_{n+1}(a_0, r), \hat{h}_{n+2}(r', r))$ and $\mathsf{Enc}_i(x_i, (r, r')) = \hat{h}_i(x_i, r)$ for $2 \le i \le n$, where $r \in \mathbb{Z}_p^m$ and $r' \in \mathcal{R}_p$.
- $\mathsf{Dec}(m_1, m_2, \ldots, m_n) = \left(\frac{\mathsf{dec}(m_1, m_2, \ldots, m_n)}{p}\right)$.

The correctness of the protocol follows from the correctness of the DRE, i.e., $\mathsf{dec}(m_1, m_2, \ldots, m_n) = (g(x) + a_0) \cdot r'$. The security of the protocol follows from the security of the DRE $\hat{h}$ directly. The communication complexity of the protocol is $s \log_2 p = O(\mathsf{D}(h) \cdot l(g))$. □

Corollary 12 *Let $f : \{0,1\}^n \to \{0,1\}$ be a function which is embedded into a degree-d polynomial $g : \mathbb{Z}^n \to \mathbb{Z}$ having m terms. Then, there exists a QR-PSM protocol computing f with communication complexity $m^2 \cdot d \cdot 2^{O(\sqrt{\log d})}$.*

Proof Let $h : \mathbb{Z}^{n+2} \to \mathbb{Z}$ be a function defined by $h := (g + x_{n+1}) \cdot x_{n+2}$. By expanding the formula, h can be regarded as a degree-$(d+1)$ polynomial having $m+1$ terms. From Theorem 3, we have a DRE of h with output length $m \cdot d \cdot 2^{O(\sqrt{\log d})}$. From Theorem 11, we have a QR-PSM protocol computing f with communication complexity $O(\mathsf{D}(h) \cdot l(g)) = m^2 \cdot d \cdot 2^{O(\sqrt{\log d})}$ since the embedding length of g is $l(g) = m+1$. □

4 Upper bound on primes for QR-PSM protocols

4.1 LQR-PSM primes

We define *the n-th linear QR-PSM (LQR-PSM) prime* L_n as the smallest prime p such that for any function $f : \{0,1\}^n \to \{0,1\}$, there exists a linear QR-PSM protocol modulo p computing f. The n-th LQR-PSM prime for $1 \le n \le 4$ are: $L_1 = 3, L_2 = 7, L_3 = 11$, and $L_4 = 37$. Although $P_i = L_i$ for $1 \le n \le 4$, it does not hold in general. Indeed, from Theorem 14 and Corollary 5, we have $L_n > P_n$ for sufficiently large n.

An LQR-PSM prime is upper bounded by a Peralta prime. A trivial bound is $L_n \le P_{2^n}$ since the length of the truth table is 2^n. The following lemma gives a somewhat non-trivial bound on LQR-PSM primes.

Lemma 13 *We have* $L_n \le P_{2^{n-1}}$.

Proof Set $p = P_{2^{n-1}}$. Let $f : \{0,1\}^n \to \{0,1\}$ be any function. For a bit $b \in \{0,1\}$, let $f_b : \{0,1\}^{n-1} \to \{0,1\}$ be a function such that $f_b(x_1, x_2, \ldots, x_{n-1}) = f(x_1, x_2, \ldots, x_{n-1}, b)$, and $t_b \in \{0,1\}^{2^{n-1}}$ a string such that the i-th bit ($0 \le i < 2^{n-1}$) of t_b is $f_b(i_1, i_2, \ldots, i_{n-1})$ if $i = \sum_{j=1}^{n-1} 2^{j-1} i_j$, i.e., t_b is the truth table of f_b. From the property of Peralta prime, S_p contains both t_0 and t_1. Let $b_0, b_1 \in \mathbb{Z}_p$ be the offset of the truth tables t_0, t_1, i.e., t_0 (resp. t_1) starts at the b_0-th (resp. the b_1-th) bit of S_p. Without loss of generality, we can assume $b_0 \le b_1$. Now we have a LQR-PSM protocol $[a_0, a_1, a_2, \ldots, a_n]_p$ computing f, where $a_0 = b_0$, $a_i = 2^{n-1-i}$ for $1 \le i \le n-1$, and $a_n = b_1 - b_0$. Therefore, we have $L_n \le P_{2^{n-1}}$. □

We obtain a lower bound on LQR-PSM primes via counting the number of LQR-PSM protocols.

Theorem 14 *We have* $L_n \ge 2^{\frac{2^n-2}{n}}$.

Proof We say that two protocols $[a_0, a_1, \ldots, a_n]_p$ and $[b_0, b_1, \ldots, b_n]_p$ are *conjugate* if there exists a quadratic residue $s \in \mathcal{R}_p$ such that $b_i = s a_i$ for $0 \le i \le n$. Note that if two protocols are conjugate, they compute the same function. Since the number of n-variable Boolean functions 2^{2^n} is a lower bound on the number of protocols $\frac{2p^{n+1}}{p-1}$ (up to conjugate), we have $\frac{2p^{n+1}}{p-1} \ge 2^{2^n}$. Since it holds $4 \ge \frac{2p}{p-1}$ for every prime p, we have $4p^n \ge 2^{2^n}$. Taking logarithms, we have $p \ge 2^{\frac{2^n-2}{n}}$. □

4.2 Paley graphs and Paley tournaments

We introduce Paley graphs and Paley tournaments, which play important roles in many areas, such as graph theory and additive combinatorics. In this paper, a *graph* is an undirected graph without multiple edges and loops, and a *tournament* is an oriented complete graph.

Fig. 1 G_{17}

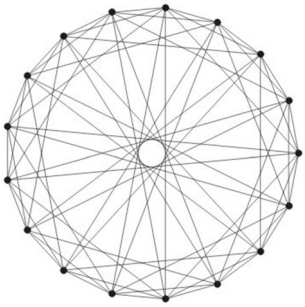
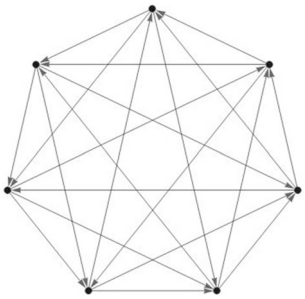


Fig. 2 T_7



Definition 7 (*Paley graph*) Let $p \equiv 1 \pmod 4$ be a prime. Then, the *Paley graph* G_p with p vertices is a graph with vertex set $\mathbb{Z}_p$ in which two distinct vertices x and y are adjacent if and only if $x - y \in \mathcal{R}_p$.

Note that the adjacency of x, y is independent of the order of x, y since $\left(\frac{-1}{p}\right) = 1$, which follows from the assumption of p.

Definition 8 (*Paley tournament*) Let $p \equiv 3 \pmod 4$ be a prime. Then, the *Paley tournament* T_p with p vertices is a tournament with vertex set $\mathbb{Z}_p$ in which for two distinct vertices x and y, there is a directed edge from x to y if and only if $x - y \in \mathcal{R}_p$.

Note that the Paley tournament is a tournament, i.e., every distinct vertex x, y have either a directed edge from x to y or a directed edge from y to x since $\left(\frac{-1}{p}\right) = -1$ holds, which follows from the assumption of p.

Figure 1 shows Paley graph G_{17} and Fig. 2 shows Paley tournament T_7 as examples.

Paley graph (tournament) is known as a typical example of graphs (tournaments) satisfying various "random-like" properties, which means properties that random graphs (tournaments) realize with high probability [1, Chapter 9], [14, 26].

The following property is one of such random-like properties.

Definition 9 Let $n \geq 1$ be an integer. Then, a graph G with vertex set $\mathbb{Z}_p$ is said to have the property $(*)_n$ if for any set S of n consecutive elements of $\mathbb{Z}_p$ and any pair of disjoint (possibly empty) sets of elements, say A and B, with $A \cup B = S$, there exists a vertex $z_{A,B} \notin S$ such that $z_{A,B}$ is adjacent to all vertices in A, but none in B. Similarly, a tournament T with vertex set $\mathbb{Z}_p$ is said to have the property $(*)_n$ if for any set S of n consecutive elements of $\mathbb{Z}_p$ and any pair of disjoint (possibly empty) sets of elements A and B with $A \cup B = S$, there exists a vertex $z_{A,B} \notin S$ such that for every vertex $a \in A$ and $b \in B$, there exist an edge from $z_{A,B}$ to a and an edge from b to $z_{A,B}$.

Remark 3 The property $(*)_n$ is a weaker version of the n-existentially closed (n-e.c.) property which is known as a finite-analogue of the axiom of the countable random graph (a.k.a. the Rado graph, see, e.g., [15]). The details of the n-e.c. property and its application to constructing circulant almost orthogonal arrays can be found in [14] and [28].

4.3 Upper bound on Peralta primes

The following theorem establishes a connection between Paley graphs, tournaments and Peralta primes. The fundamental idea to prove this theorem can be found in [28].

Theorem 15 *Let $n \geq 1$ be an integer and $p > n$ denote an odd prime. When $p \equiv 1 \pmod 4$, p is n-Peralta if and only if G_p has the property $(*)_n$. Similarly, when $p \equiv 3 \pmod 4$, p is n-Peralta if and only if T_p has the property $(*)_n$.*

Proof Let $n \geq 1$ and assume that $p \equiv 1 \pmod 4$ is a prime with $p > n$; the discussion below works for the case of a prime $p \equiv 3 \pmod 4$ as well. Suppose that the Paley graph G_p has the property $(*)_n$. Let $t := (t_1, t_2, \ldots, t_n) \in \{0, 1\}^n$ be an arbitrarily given sequence. Set $A := \{i \in \{1, 2, \ldots, n\} \mid t_i = 1\}$ and $B := \{i \in \{1, 2, \ldots, n\} \mid t_i = 0\}$. Notice that $A \cup B = \{1, 2, \ldots, n\}$. Then, from the assumption of G_p, there exists some $z = z_{A,B} \in \mathbb{Z}_p \backslash \{1, 2, \ldots, n\}$ such that $(\frac{i-z}{p}) = 1$ if and only if $i \in A$. Here notice that for any $i \in \{1, 2, \ldots, n\}$ we have $(\frac{i-z}{p}) \neq 0$ since $z \notin \{1, 2, \ldots, n\}$. Now consider the sequence

$$\mathsf{S}_z := \left(\frac{1}{2} + \frac{1}{2}\left(\frac{1-z}{p}\right), \frac{1}{2} + \frac{1}{2}\left(\frac{2-z}{p}\right), \ldots, \frac{1}{2} + \frac{1}{2}\left(\frac{n-z}{p}\right)\right).$$

Since $z \notin \{1, 2, \ldots, n\}$, S_z forms a consecutive subsequence of S_p, and we now have $\mathsf{S}_z = t$. Conversely if p is an n-peralta prime, then S_p contains any sequence $t \in \{0, 1\}^n$. Since the permutation $x \mapsto x + 1$ on $\mathbb{Z}_p$ is an automorphism of G_p, to prove that G_p has the property $(*)_n$, it suffices to check that there exists $z_{A,B}$ with respect to the subsets A, B defined above, which is obvious from the assumption of p. □

Thus, we immediately obtain the following corollary.

Corollary 16 *For $n \geq 1$, let $m_n^{(G)}$ be the least prime $p \equiv 1 \pmod 4$ such that G_p has the property $(*)_n$, and similarly, $m_n^{(T)}$ denotes the least prime $p \equiv 3 \pmod 4$ such that T_p has the property $(*)_n$. Set $m_n := \min\{m_n^{(G)}, m_n^{(T)}\}$. Then, we have $P_n = m_n$.*

Substantially, the following theorem was proved by Graham and Spencer [21], Blass, Exoo and Harary [12], Bollobás and Thomason [13] in the context of graph theory.

Theorem 17 ([12, 13, 21]) *For $n \geq 1$ and every prime $p > n^2 2^{2n-2}$, both G_p and T_p have the property $(*)_n$. In particular, $m_n > n^2 2^{2n-2}$ for $n \geq 1$.*

Furthermore, it was proved in [2, 3] that for an odd prime p, both G_p and T_p have the property $(*)_n$ if $p > \{(n-3)2^{n-1} + 2\}\sqrt{p} + (n+1)2^{n-1} - 1$.

The following corollary is a direct consequence of Theorems 15, 17 and Corollary 16, which improves Corollary 5 by a constant factor $(1 + \sqrt{2})^2 \fallingdotseq 5.828$.

Corollary 18 *If an odd prime p satisfies that $p > n^2 2^{2n-2}$, then p is n-Peralta. As a consequence, we have $P_n < n^2 2^{2n-2}$ for $n \geq 1$.*

Applying the Baker-Harman-Pintz theorem on prime gaps in [6], we obtain the following corollary.

Corollary 19 *For any sufficiently large n, there exists an n-Peralta prime p with $p \in [n^2 2^{2n-2}, n^2 2^{2n-2} + (n^2 2^{2n-2})^{0.525}]$, which means that $p = (1 + o(1))n^2 2^{2n-2}$.*

Remark 4 A modification of the proof of [17, Theorem 4.1] shows that for each $n \geq 1$ there is a graph (and tournament) with vertex set $\mathbb{Z}_p$ such that $p = O(n2^n)$ satisfying the property $(*)_n$, where such a graph can be constructed from random Cayley graphs over $\mathbb{Z}_p$. Since it is known that the Paley graph G_p has various properties that random Cayley graphs over $\mathbb{Z}_p$ satisfy with high probability, we guess that in fact $m_n = P_n = o(n^2 2^{2n})$. Although at present there seems to be no known direct approach toward this conjecture, it may be possible to obtain some supporting evidences by considering the following "random" graph, for example. Suppose that $p \equiv 1 \pmod 4$ is a prime and $1/2 \leq q \leq 1$ is a real number. Then the set $\mathcal{R}_p$ can be partitioned into two non-empty sets $\mathcal{R}_p^+$ and $\mathcal{R}_p^-$ with same size such that $\mathcal{R}_p^- = \{-r \mid r \in \mathcal{R}_p^+\}$. Then for each $r \in \mathcal{R}_p^+$ choose a pair $\{r, -r\}$ independently with probability q and form the set $U_p \subseteq \mathcal{R}_p$ consisting of all chosen quadratic residues in $\mathcal{R}_p^+$ and their additive inverses in $\mathcal{R}_p^-$. Then construct a graph (denoted by $G_p(q)$) with vertex set $\mathbb{Z}_p$ and connect two vertices x and y if and only if $x - y \in U_p$. (A similar construction for primes $p \equiv 3 \pmod 4$ can be established as well.) Notice that $G_p(q)$ is a spanning subgraph of G_p, and the "closer" $G_p(q)$ is to G_p, the closer q is to 1 (in particular $G_p(q) = G_p$ if $q = 1$). We believe that for $q = 1 - \varepsilon$ with *any* $\varepsilon > 0$ the probability that $G_p(q)$ with $p = o(n^2 2^{2n})$ has the property $(*)_n$ tends to 1 (as $n \to \infty$). At present it is possible to confirm this claim for $q < 3/4$. Indeed by the union bound the probability that $G_p(q)$ does not have the property $(*)_n$ is at most $2^n(1 - (1 - q)^n)^{p-n}$, which is $o(1)$ if $q < 3/4$ and $p = o(n^2 2^{2n})$.

Acknowledgements The first author was supported during this work by JSPS KAKENHI Grant Numbers JP21K17702 and JP23H00479, and JST CREST Grant Number JPMJCR22M1. The second author was supported during this work by JSPS KAKENHI Grant Number JP20J20797. The third author was supported during this work by JSPS KAKENHI Grant Number JP20J00469. The last author was supported during this work by JSPS KAKENHI Grant Number JP19H01109, JST CREST Grant Number JPMJCR2113, and JST AIP Acceleration Research JPMJCR22U5.

Declarations

Competing interests The authors declare no conflicts of interest associated with this manuscript.

Appendix

LQR-PSM protocols for AND and EQ functions

In this section, we discuss LQR-PSM protocols for some particular symmetric functions, namely, AND and EQ functions. Recall that Corollary 7 shows that for any symmetric function $f : \{0,1\}^n \to \{0,1\}$ there exists an LQR-PSM protocol with communication complexity $O(n^2)$. It is natural to ask whether this upper bound could be improved or not. The following two propositions show that it is possible to improve the bound of communication complexity for AND and EQ functions by choosing appropriate primes.

Proposition 20 *Let* $\mathsf{AND}_n : \{0,1\}^n \to \{0,1\}$ *be the n-bit AND function. Then for any positive integer n there exists an LQR-PSM protocol for* AND_n *with communication complexity* $o(n^2)$.

Proposition 21 *Let* $\mathsf{EQ}_n : \{0,1\}^n \to \{0,1\}$ *be the n-bit EQ function. Then for infinitely many n there exists an LQR-PSM protocol for* EQ_n *with communication complexity* $o(n^2)$.

To prove these propositions we introduce the following theorem and corollary from analytic number theory.

Theorem 22 (Graham–Ringrose [20]) *For an odd prime p let* n_p *denote the least positive integer that is a quadratic non-residue modulo p. Then there exist infinitely many primes p with* $n_p = \Omega(\log p \cdot \log\log\log p)$.

Corollary 23 *There exist infinitely many primes p such that* $n_p = \Omega(\log p \cdot \log\log\log p)$ *and all integers in the interval* $(n_p, 2n_p)$ *are quadratic residues modulo p.*

Proof First notice that n_p is a prime and $2n_p$ is the least composite number of which n_p is a prime factor. Hence all composite numbers in $(n_p, 2n_p)$ are quadratic residues modulo p because all primes less than n_p are quadratic residues modulo p. Since there exists at least one prime in $(n_p, 2n_p)$ by Bertrand's postulate, it suffices to prove that all *primes* in $(n_p, 2n_p)$ are quadratic residues. To that end we use the following discussion which is a slight modification of the proof of Theorem 22 in [20]. Let y be a prime and let $\mathbf{P}_{2y}$ be the set of primes p such that $\left(\frac{y}{p}\right) = -1$ and for all primes $p_1 \le 2y$ with $p_1 \ne y$ we have $\left(\frac{p_1}{p}\right) = 1$. For a prime y and a real number $x > 0$ consider the following weighted sum.

$$S_{x,2y} := \sum_{\substack{p \in \mathbf{P}_{2y} \\ x^{1/2} < p \le x^2}} (\log p)\left(\exp\left(-\frac{p}{2x}\right) - \exp\left(-\frac{p}{x}\right)\right).$$

Notice that $(\log p)(\exp(-p/2x) - \exp(-p/x)) > 0$ whenever $x > 0$ and $p \ge 2$. Hence for given x and y we have $S_{x,2y} > 0$ if and only if there exists a prime $p \in \mathbf{P}_{2y}$ with $x^{1/2} < p \le x^2$. By this fact it suffices to prove that there exists $x_0 > 0$ such that for any $x > x_0$ we have $S_{x,2y} > 0$ when $y \ge c_1 \log x \cdot \log\log\log x$ for some $c_1 > 0$. Indeed if $p \in \mathbf{P}_{2y}$ satisfies that $x^{1/2} < p \le x^2$ then we have $y = n_p$ and the inequality $y \ge c_1 \log x \cdot \log\log\log x$ implies that $y \ge c_2 \log p \cdot \log\log\log p$ for some $c_2 > 0$, proving the corollary. It is not difficult to obtain that

$$S_{x,2y} = \sum_{x^{1/2} < p \le x^2} (\log p)\left(\exp\left(-\frac{p}{2x}\right) - \exp\left(-\frac{p}{x}\right)\right) \cdot T_{p,2y}$$

where

$$T_{p,2y} := 2^{-\pi(2y)}\left(1-\left(\frac{y}{p}\right)\right)\prod_{\substack{p_1\le 2y\\ p_1\neq y}}\left(1+\left(\frac{p_1}{p}\right)\right)$$

and $\pi(\cdot)$ denotes the prime-counting function. Indeed by the definition of $\mathbf{P}_{2y}$ we have

$$T_{p,2y} = \begin{cases} 1 & p\in\mathbf{P}_{2y};\\ 0 & \text{otherwise.}\end{cases}$$

Hereafter for two integers a and b the notation $a|b$ means that a is a divisor of b. Let Q_{2y} be the product of all primes $p_1\le 2y$, and for an integer m with $m|Q_{2y}$ define ε_m as

$$\varepsilon_m := \begin{cases} -1 & y|m;\\ 1 & \text{otherwise.}\end{cases}$$

Then expanding $T_{p,2y}$ implies that

$$S_{x,2y} = 2^{-\pi(2y)}\sum_{m|Q_{2y}}\varepsilon_m\sum_{x^{1/2}<p\le x^2}(\log p)\left(\exp\left(-\frac{p}{2x}\right)-\exp\left(-\frac{p}{x}\right)\right)\prod_{p_1|m}\left(\frac{p_1}{p}\right).$$

Now we can use the same discussion in [20]. Indeed there exists $x_0>0$ such that for any $x>x_0$ the last sum is at least $c_3\cdot x2^{-\pi(2y)}$ for some $c_3>0$ when $y\ge c_1\log x\cdot\log\log\log x$ with sufficiently small constant $c_1>0$, which follows from Theorems 2 and 4 in [20] and (2.5) in [20], together with the discussion in Section 9 in [20]. In summary for any $x>x_0$ we have $S_{x,2y}>0$ when $x^{1/2}<p\le x^2$ and $y\ge c_2\log p\cdot\log\log\log p$. □

Now we are ready to prove Propositions 20 and 21.

Proof of Proposition 20 Let n be a given positive integer. By Theorem 22, it is possible to choose a prime p with $n\le n_p$ and $n\ge c\log p\cdot\log\log\log p$ (with sufficiently small constant $c>0$). Since $\log\log\log(\cdot)$ is unbounded and monotonically increasing it must hold that $p=2^{o(n)}$, implying that $\log_2 p=o(n)$. Since S_p contains 1^n0 as subsequence, we have an LQR-PSM protocol for the n-bit NAND function. By Remark 1, we have an LQR-PSM protocol for AND_n. □

Proof of Proposition 21 By Corollary 23, there exist infinitely many primes p with $n_p=\Omega(\log p\cdot\log\log\log p)$ and all integers $0<x<2n_p$ except n_p are quadratic residues modulo p. Let n'_p be the second least quadratic nonresidue modulo p. Then S_p contains $01^{n'_p-n_p-1}0$ as a subsequence. By Remark 1, we have an LQR-PSM protocol for $\mathsf{EQ}_{n'_p-n_p-1}$.

Remark 5 There are known PSM protocols for AND and EQ functions with communication complexity $O(n\log n)$ [19]. Hence LQR-PSM protocols in Propositions 20 and 21 would not realize the best known complexity. On the other hand these propositions suggest that the communication complexity of LQR-PSM protocols in Corollary 7 could be reduced for other symmetric functions.

Remark 6 If the generalized Riemann hypothesis is true then the lower bound of n_p in Theorem 22 and Corollary 23 can be improved to $n_p=\Omega(\log p\cdot\log\log p)$ [24, Chapter 13].

References

1. Alon N., Spencer J.H.: The Probabilistic Method. Wiley, New York (2016).
2. Ananchuen W., Caccetta L.: On the adjacency properties of Paley graphs. Networks **23**(4), 227–236 (1993).
3. Ananchuen W., Caccetta L.: On tournaments with a prescribed property. Ars Combinatoria **36**, 89–96 (1993).
4. Applebaum B., Holenstein T., Mishra M., Shayevitz O.: The communication complexity of private simultaneous messages, revisited. J. Cryptol. **33**(3), 917–953 (2020).
5. Assouline, L., Liu, T.: Multi-party PSM, revisited. In: TCC 2021, pp. 194–223 (2021). Springer
6. Baker R.C., Harman G., Pintz J.: The difference between consecutive primes, II. Proc. London Math. Soc. **83**(3), 532–562 (2001).
7. Ball, M., Holmgren, J., Ishai, Y., Liu, T., Malkin, T.: On the complexity of decomposable randomized encodings, or: how friendly can a garbling-friendly PRF be? In: 11th Innovations in Theoretical Computer Science Conference (ITCS 2020) (2020). Schloss Dagstuhl-Leibniz-Zentrum für Informatik
8. Ball, M., Randolph, T.: A note on the complexity of private simultaneous messages with many parties. In: 3rd Conference on Information-Theoretic Cryptography (ITC 2022) (2022). Schloss Dagstuhl-Leibniz-Zentrum für Informatik
9. Beimel, A., Gabizon, A., Ishai, Y., Kushilevitz, E., Meldgaard, S., Paskin-Cherniavsky, A.: Non-interactive secure multiparty computation. In: CRYPTO 2014, pp. 387–404 (2014). Springer
10. Beimel, A., Ishai, Y., Kumaresan, R., Kushilevitz, E.: On the cryptographic complexity of the worst functions. In: TCC 2014, pp. 317–342 (2014). Springer
11. Beimel, A., Kushilevitz, E., Nissim, P.: The complexity of multiparty PSM protocols and related models. In: EUROCRYPT 2018, pp. 287–318 (2018). Springer
12. Blass A., Exoo G., Harary F.: Paley graphs satisfy all first-order adjacency axioms. J. Graph Theory **5**(4), 435–439 (1981).
13. Bollobás B., Thomason A.: Graphs which contain all small graphs. Eur. J. Combinatorics **2**(1), 13–15 (1981).
14. Bonato A.: The search for n-e.c. graphs. Contrib. Discret. Math. (2009). https://doi.org/10.11575/cdm.v4i1.61874.
15. Cameron, P.J.: The random graph. The Mathematics of Paul Erdös II, 333–351 (1997)
16. Cleve, R.: Towards optimal simulations of formulas by bounded-width programs. In: Proceedings of the 22nd ACM STOC, pp. 271–277 (1990)
17. Costea, A.: Computational and theoretical aspects of n-e.c. graphs. Master's thesis, Wilfrid Laurier University (2010)
18. Cramer, R., Fehr, S., Ishai, Y., Kushilevitz, E.: Efficient multi-party computation over rings. In: EUROCRYPT 2003, pp. 596–613 (2003). Springer
19. Feige, U., Killian, J., Naor, M.: A minimal model for secure computation. In: Proceedings of the 26th ACM STOC, pp. 554–563 (1994)
20. Graham S.W., Ringrose C.J.: Lower bounds for least quadratic non-residues. In: Berndt B.C., Diamond H.G., Halberstam H., Hildebrand A. (eds.) Analytic Number Theory, pp. 269–309. Springer, Heidelberg (1990).
21. Graham R.L., Spencer J.H.: A constructive solution to a tournament problem. Can. Math. Bull. **14**(1), 45–48 (1971).
22. Ishai, Y., Kushilevitz, E.: Private simultaneous messages protocols with applications. In: Proceedings of the 5th Israeli Symposium on Theory of Computing and Systems (ISTCS 1997), pp. 174–183 (1997). IEEE
23. Ishai Y.: Randomization techniques for secure computation. Secur. Multi-Party Comput. **10**, 222 (2013).
24. Montgomery H.L.: Topics in Multiplicative Number Theory, vol. 227. Springer, Heidelberg (2006).
25. Peralta R.: On the distribution of quadratic residues and nonresidues modulo a prime number. Math. Comput. **58**(197), 433–440 (1992).
26. Satake S.: On explicit random-like tournaments. Graphs Combinatorics **37**(4), 1451–1463 (2021).
27. Vaikuntanathan, V.: Some open problems in information-theoretic cryptography. In: 37th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2017) (2018). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik
28. Yoshida, K., Satake, S., Phoa, F., Sawa, M.: Circulant almost-orthogonal arrays with strength 3 and bandwidth 1: constructions and existence. preprint