nature photonics

Article

https://doi.org/10.1038/s41566-024-01526-8

Modular quantum-to-quantum Bernoulli factory in an integrated photonic processor

Received: 26 June 2023

Accepted: 13 August 2024

Published online: 03 October 2024

Check for updates

Francesco Hoch[1], Taira Giordani[1], Luca Castello[1], Gonzalo Carvacho[1], Nicolò Spagnolo[1], Francesco Ceccarelli[2], Ciro Pentangelo[2,3], Simone Piacentini[2], Andrea Crespi[2,3], Roberto Osellame[2], Ernesto F. Galvão[4,5] & Fabio Sciarrino[1] ✉

Generation and manipulation of randomness is a relevant task for several applications of information technology. It has been shown that quantum mechanics offers some advantages for this type of task. A promising model for randomness manipulation is provided by Bernoulli factories—protocols capable of changing the bias of Bernoulli random processes in a controlled way. At first, this framework was proposed and investigated in a fully classical regime. Recent extensions of this model to the quantum case showed the possibility of implementing a wider class of randomness manipulation functions. We propose a Bernoulli factory scheme with quantum states as the input and output, using a photonic-path-encoding approach. Our scheme is modular and universal and its functioning is truly oblivious of the input bias—characteristics that were missing in earlier work. We report on experimental implementations using an integrated and fully programmable photonic platform, thereby demonstrating the viability of our approach. These results open new paths for randomness manipulation with integrated quantum technologies.

Randomness plays an essential role in several research fields and daily life applications, such as those connected to sensitive data protection. There are several deterministic techniques that can be exploited to generate randomness, whose security and efficiency depend on the precise algorithm used. Quantum mechanics provides intrinsic randomness, which is unbreakable from the theoretical point of view, but hard to ensure from the experimental one, due to the inevitable noise and imperfect control over devices. This peculiar property of quantum theory leads to several advantages in the manipulation, communication and processing of information, which are shown by various quantum communication protocols[1–3] and quantum computational algorithms[2,4–8]. The generation and manipulation of quantum randomness have been studied in depth, resulting in implementations using different platforms[9–12], degrees of freedom[13–16] and protocols[17–21].

A recent proposal aims at using quantum resources to manipulate randomness in Bernoulli processes. Classical Bernoulli factories were first introduced in ref. 22 to address the problem of how to process instances of a Bernoulli variable (flips of a biased coin) with the goal of generating an output Bernoulli variable whose bias is a desired function of the (unknown) input bias. This task was called a classical-to-classical Bernoulli factory (CCBF), since both input and output are classical coins, and finds applications in several fields ranging from Markov chain Monte Carlo simulation[23] to economy[24]. In ref. 22, the space of simulable functions was also characterized, and a method was proposed to construct them.

In recent years, the problem has been extended to the quantum domain by analysing the possibility of replacing the input and/or output Bernoulli variables with quantum counterparts. In refs. 25,26, the first quantum version of this process, named quantum-to-classical

[1]Dipartimento di Fisica, Sapienza Università di Roma, Roma, Italy. [2]Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR), Milano, Italy. [3]Dipartimento di Fisica, Politecnico di Milano, Milano, Italy. [4]International Iberian Nanotechnology Laboratory (INL), Braga, Portugal. [5]Instituto de Física, Universidade Federal Fluminense, Niterói, Brazil. ✉e-mail: fabio.sciarrino@uniroma1.it

Bernoulli factory (QCBF), was defined by considering a quantum input and a classical output. This QCBF extension simulates a Bernoulli variable given a quantum coin (or quoin) as an input parameter. A quoin is a qubit in a pure state that—when measured in the computational basis—returns a classical Bernoulli variable. It was observed that all the functions simulable by a CCBF can also be implemented as a QCBF. Indeed, it is enough to measure the quoin in the computational basis to recover a Bernoulli variable with the same parameter. In ref. 25, the authors characterized the space of simulable functions with a quantum input and showed that a change in the basis is the only necessary quantum operation required to implement the complete set of simulable functions. In fact, a Bernoulli factory that uses quoins as inputs can implement a strictly larger set of bias manipulation functions than the fully classical case. Moreover, there is experimental evidence that a quantum advantage can be achieved[27,28] with respect to the required number of inputs, even for the class of classically simulable functions.

A more complex quantum extension of the Bernoulli factory was later proposed[29], now having quoins as both input and output and aptly named a quantum-to-quantum Bernoulli factory (QQBF). In ref. 29, the set of simulable functions by a QQBF was completely characterized, and a procedure to construct them was defined. For any version of the Bernoulli factory, it is important that the implementation is the same independent of the input bias, that is, the protocol should not use any information on the bias. Furthermore, any experimental scheme should aim at the possibility of concatenating different operations in a modular fashion without the knowledge of the output state from the prior step. All previous attempts to experimentally implement QQBFs[30,31] were unable to simultaneously enforce these conditions. Once all the features of the QQBF are verified, the quantum input and output enable its use as a subroutine in quantum algorithms. For example, QQBF-like operations have been used for delegated quantum computing[32] to obtain genuine secure quantum-state preparation.

In this work, we propose a modular approach to implement a genuine QQBF and we report its experimental realization using integrated quantum photonics. In detail, we use a six-mode, fully programmable, integrated photonic processor (IPP) to manipulate photonic qubits generated by spontaneous parametric down conversion. Our approach provides a viable route for computational tasks involving Bernoulli processes, within a programmable platform that is highly stable, reliable and compact.

This paper is structured as follows. In the 'Bernoulli factory' section, we review the theory of Bernoulli factory processes. Then, in the 'Modular scheme for a photonic QQBF' section, we describe our proposed modular approach. In the 'Implementation' and 'Experimental results' sections, we discuss our experimental apparatus and we demonstrate both individual and concatenated modules corresponding to the various operations that lead to a universal QQBF capable of, in principle, implementing any quantum simulable function.

Bernoulli factory

Different types of Bernoulli factory are proposed in the literature, which may take either classical or quantum resources as inputs and outputs (Fig. 1).

A Bernoulli factory, in a classical context, is an algorithm for the manipulation of random processes that follow a Bernoulli distribution $\mathcal{B}(p)$, described by the bias parameter p. More specifically, a Bernoulli factory aims at constructing a function G_f: $\{0,1\}^\infty \to \{0,1\}$, associated with a function $f : \mathcal{D} \subseteq [0,1] \to [0,1]$, such that its application to a sample following a Bernoulli distribution with parameter p is equivalent to sampling exactly from a different Bernoulli distribution with bias parameter $f(p)$. Formally, this corresponds to searching for a function G_f satisfying $G_f(\mathcal{B}(p)^\infty) = \mathcal{B}(f(p))$. An essential requirement is that the function G_f must not depend on p, which reflects the assumed ignorance of the user about the value of the input bias. In ref. 22, a necessary and sufficient condition for a Bernoulli factory to exist for a given function f was identified. In particular, it was shown that not all functions are exactly implementable as a Bernoulli factory.

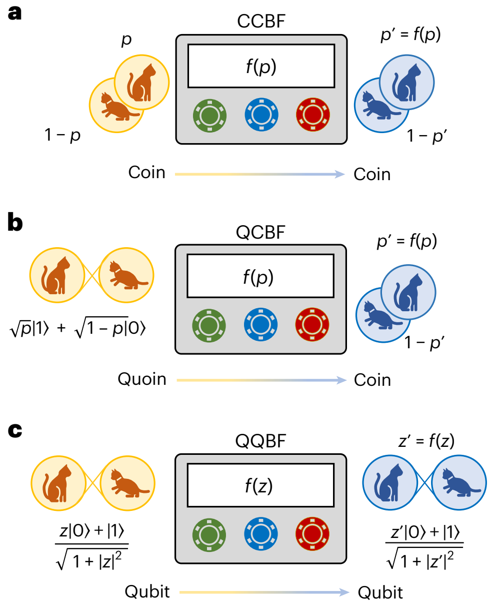
a
CCBF
p
f(p)
p′ = f(p)
1 − p
1 − p′
Coin
Coin
b
QCBF
f(p)
p′ = f(p)
$\sqrt{p}|1\rangle + \sqrt{1-p}|0\rangle$
1 − p′
Quoin
Coin
c
QQBF
z′ = f(z)
f(z)
$\frac{z|0\rangle + |1\rangle}{\sqrt{1+|z|^2}}$
$\frac{z'|0\rangle + |1\rangle}{\sqrt{1+|z'|^2}}$
Qubit
Qubit

Fig. 1 | Conceptual scheme of a Bernoulli factory. a, CCBF where a sequence of classical coins with unknown bias p are processed for producing a new coin with bias $f(p)$ (refs. 22,44). **b**, QCBF in which a quoin serves as the input to synthesize a classical one[25,26]. **c**, Fully quantum version where both input and output are general quantum states[29].

The concept of a Bernoulli factory has been extended to the quantum domain by exploiting a new fundamental resource, namely, a quoin, of parameter p. In detail, a quoin is a qubit in the pure state $|C_p\rangle := \sqrt{1-p}\,|0\rangle + \sqrt{p}\,|1\rangle$. A QCBF, first proposed in ref. 25, has quoins as inputs with bias parameter p, and—at the output—produces a series of classical bits that follow a Bernoulli distribution with parameter $f(p)$. The set of functions f for which a CCBF can be constructed was shown[25,26] to be strictly included in the set that can be implemented via a QCBF.

On the other hand, in the QQBF[29], both input and output are quantum states. In detail, a QQBF takes a set of quoins as the input, all with the same bias parameter p, and returns a quoin with parameter $f(p) : \mathcal{D} \subseteq [0,1] \to [0,1]$. In general, we furthermore define the following parameterization of single-qubit states proved to be helpful in the analysis of Bernoulli factories:

$$|\mathbf{z}\rangle := \frac{z\,|0\rangle + |1\rangle}{\sqrt{1+|z|^2}}, \qquad (1)$$

where z is a complex variable; this can be seen as a stereographic projection of the Bloch sphere onto the complex plane. For a general input qubit $|\mathbf{z}\rangle$, a QQBF associated to a complex function $g(z) : \mathbb{C} \to \mathbb{C}$ is a process that generates a qubit in the state $|\mathbf{g(z)}\rangle$ at the output. In ref. 29, it was demonstrated that a necessary and sufficient condition for a QQBF to exist is that the associated function belongs to the complex field generated by element z, that is, $g(z)$ is a complex rational function in the parameter z. Using the previous result and the algebraic theory of the field, the necessary and sufficient condition to demonstrate the feasibility of implementing all the complex rational functions (that is, all the simulable QQBF) relies on showing the possibility of implementing the quantum version of the field operations, which are inversion, addition and product, as well as the possibility to combine them.

Modular scheme for a photonic QQBF

To demonstrate the feasibility of a generic QQBF using integrated photonics, we will explicitly construct an appropriate scheme to implement the field operations with photons. Previous attempts to experimentally implement the field operations[30,31] were limited, as they substantially relied on prior knowledge of the input state (Supplementary Note 1). This is in stark contrast to the fundamental requirement for a correct implementation of the protocol, that is, full ignorance of the input state. Here we present three interferometers (Fig. 2), each of them implementing a particular field operation that can be concatenated at will. These schemes use the usual dual-rail encoding for photonic qubits, where logical states $|0\rangle$ and $|1\rangle$ are encoded as the presence of a photon in one of two possible optical paths. This choice is motivated by the current state of the art in integrated photonic technology, which allows the implementation of complex architectures[33] based on beamsplitters (BSs) and phase shifters. Let us now discuss the implementation of each field operation building block.

The inversion operation, corresponding to the transformation $|\mathbf{z}\rangle \to \left|\frac{\mathbf{1}}{\mathbf{z}}\right\rangle$, is performed by swapping the two modes of the dual-rail qubit (Fig. 2a). It should be noted that this is the only unitary operation among the three, thereby having a success probability equal to 1.

The product operation corresponds to the transformation $|\mathbf{z_1}\rangle|\mathbf{z_2}\rangle \to |\mathbf{z_1 z_2}\rangle$ and can be implemented as shown in Fig. 2b. Two photons are injected in the interferometer, one for each dual-rail qubit mode pair ($|0\rangle_1$, $|1\rangle_1$) and ($|0\rangle_2$, $|1\rangle_2$). Then, the modes representing states $|1\rangle_1$ and $|0\rangle_2$ of the two dual-rail qubits are routed as the input modes of a balanced BS. The output modes after the BS are then measured by using the two detectors labelled '+' and '−' (Fig. 2b). Conditioned on the detection of a single photon in one of the two outputs of the BS, the output state on the remaining modes $|0\rangle_o$ and $|1\rangle_o$, after inserting a relative π/2 phase shift, is found to be $|\pm\mathbf{z_1 z_2}\rangle_o = \frac{|1\rangle_o \pm z_1 z_2 |0\rangle_o}{\sqrt{1+|z_1 z_2|^2}}$, where the '+' or '−' sign depends on which detector clicks. Hence, the conditional output is found in the product state, up to a state-independent phase factor of π. The success probabilities P_+ and P_- of the two post-selected outputs are given by

$$P_+ = P_- = \frac{1+|z_1|^2|z_2|^2}{2\left(1+|z_1|^2\right)\left(1+|z_2|^2\right)}. \tag{2}$$

We observe that the success probability is greater than zero for all the inputs, except for the pairs ($z_1 = 0, z_2 = \infty$) and ($z_1 = \infty, z_2 = 0$). Indeed, for these pairs, the product operation returns an indeterminate form. In Supplementary Note 2, we provide some further analysis of the behaviour of the success probability.

Finally, the addition operation, corresponding to the transformation $|\mathbf{z_1}\rangle|\mathbf{z_2}\rangle \to |\mathbf{z_1} + \mathbf{z_2}\rangle$, can be implemented with the interferometer shown in Fig. 2c. Two photons are injected in the interferometer, one for each mode pair ($|0\rangle_1$, $|1\rangle_1$) and ($|0\rangle_2$, $|1\rangle_2$). Two identical BSs are used to mix the mode pairs representing the same logical state for the two qubits, combining $|0\rangle_1$ with $|0\rangle_2$ and $|1\rangle_1$ with $|1\rangle_2$. After the mixing process, one output port of each BS is measured via the two detectors labelled as S and I (Fig. 2c), whereas a π/2 phase shift is added in mode $|1\rangle_o$. Conditioned on the detection of a single photon in S, the output state is found to be $\left|(\mathbf{z_1} + \mathbf{z_2})\sqrt{\mathbf{RT}}/(\mathbf{R}-\mathbf{T})\right\rangle_o$, where R and T are the reflectivity and transmissivity of the BSs, respectively. If a single photon is detected at I instead, the corresponding output state is $\left|-\mathbf{z_1 z_2}/(\mathbf{z_1}+\mathbf{z_2})(\mathbf{R}-\mathbf{T})/\sqrt{\mathbf{RT}}\right\rangle_o$. The numerical multiplicative factor $\sqrt{RT}/(R-T)$ can be set to 1 by choosing the reflectivity of both BSs to be $R = \frac{5+\sqrt{5}}{10}$. For this choice of R, the output conditioned on a click in detector S is the sum state $|\mathbf{z_1} + \mathbf{z_2}\rangle_o$, whereas the one conditioned on a click in detector I is the harmonic mean state $|-\mathbf{z_1 z_2}/(\mathbf{z_1} + \mathbf{z_2})\rangle_o$. The corresponding success probabilities are found to be

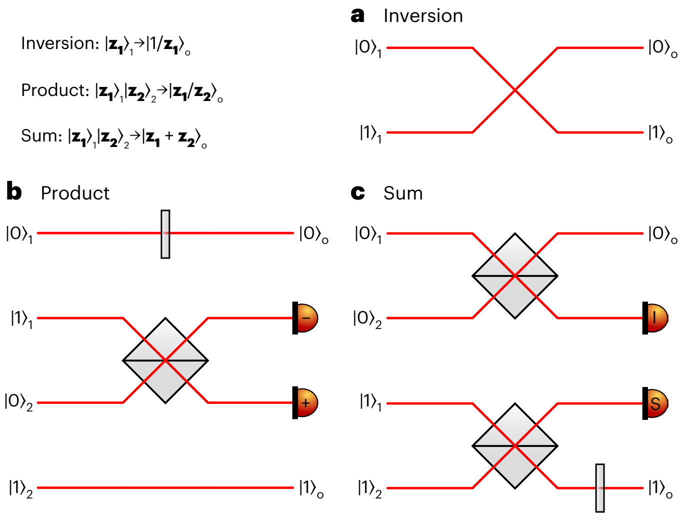
Inversion: $|\mathbf{z_1}\rangle_1 \to |1/\mathbf{z_1}\rangle_o$
Product: $|\mathbf{z_1}\rangle_1|\mathbf{z_2}\rangle_2 \to |\mathbf{z_1}/\mathbf{z_2}\rangle_o$
Sum: $|\mathbf{z_1}\rangle_1|\mathbf{z_2}\rangle_2 \to |\mathbf{z_1} + \mathbf{z_2}\rangle_o$
a Inversion
$|0\rangle_1$
$|1\rangle_1$
$|0\rangle_o$
$|1\rangle_o$
b Product
$|0\rangle_1$
$|1\rangle_1$
$|0\rangle_2$
$|1\rangle_2$
$|0\rangle_o$
$|1\rangle_o$
−
+
c Sum
$|0\rangle_1$
$|0\rangle_2$
$|1\rangle_1$
$|1\rangle_2$
$|0\rangle_o$
$|1\rangle_o$
I
S

Fig. 2 | Building blocks for a generic QQBF. Interferometric schemes that implement the basic operations to build a generic QQBF with dual-rail encoded qubits are shown. The inputs of the interferometers are labelled by numbers 1 and 2, and the outputs are labelled as 'o'. **a**, Inversion operation is performed by swapping the two modes of the input dual-rail qubit. **b**, Product operation is performed by sending one waveguide from each dual-rail qubit ($|1\rangle_1$ and $|0\rangle_2$) into a balanced BS, and measuring the outgoing modes. Detection of a single photon in the modes labelled '+' or '−' signals success (up to a global phase). **c**, Addition operation is implemented by directing the modes, representing the same state of the two qubits, to equally unbalanced BSs, and measuring one output mode for each BS. When one photon is found in the detector labelled S, and the other photon is in output mode $|0\rangle_o$ or $|1\rangle_o$, the output state is the sum of the input ones (up to a global phase).

$$P_S = \frac{|z_1+z_2|^2+1}{5\left(1+|z_1|^2\right)\left(1+|z_2|^2\right)}, \tag{3}$$

$$P_I = \frac{|z_1+z_2|^2+|z_1 z_2|^2}{5\left(1+|z_1|^2\right)\left(1+|z_2|^2\right)}. \tag{4}$$

The probability of success is non-zero for all the inputs, except for the pairs ($z_1 = \infty, z_2 = \infty$) for addition and ($z_1 = 0, z_2 = 0$) for harmonic mean, since the results of the corresponding operations for these pairs are an indeterminate form.

Our implementation, involving linear optics and dual-rail encoding, is, thus, based on a post-selection process. More specifically, the schemes for the product and addition operations, involving the minimum cost in terms of the number of photons and modes, are found to be probabilistic. Furthermore, the success probability is then found to be dependent on the transformation *f* being implemented by the scheme and on the input state $|\mathbf{z_1}\rangle|\mathbf{z_2}\rangle$. However, we observe that such probabilistic nature is unavoidable within the protocol due to the intrinsic nature of the Bernoulli process. In Supplementary Note 3, we show that our proposed interferometer designs for the implementation of the field operations are essentially unique if we use only four modes.

After the definition of the building blocks for the presented scheme, we now discuss the possibility of concatenating the field operations. This is an important characteristic feature of our approach, and fundamentally different from previous realizations[30,31]. Our modular scheme allows for a sequential application of the operations. This is possible owing to the common encoding strategy for the input and output states of the building blocks. Thus, to concatenate two operations, it is sufficient to apply the respective modules in sequence,

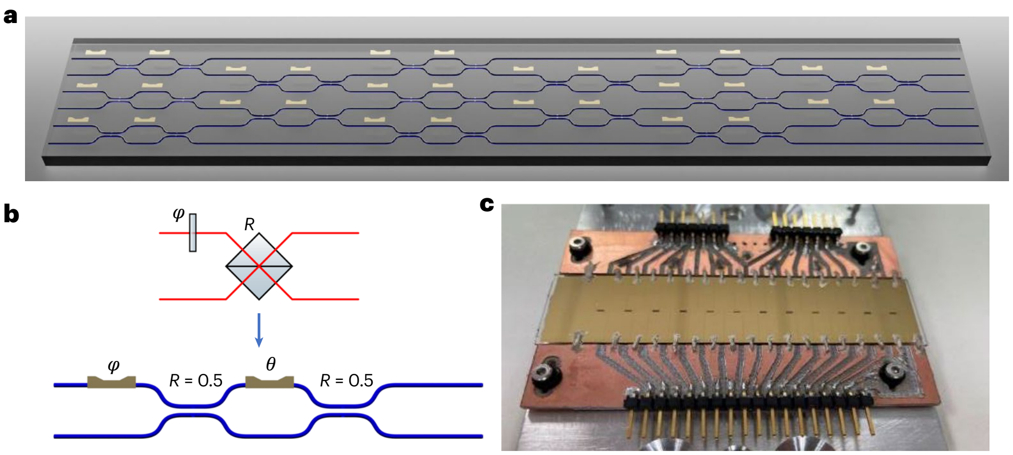

Fig. 3 | Scheme of the six-mode IPP. a, Interferometer layout. The device is a six-mode fully programmable interferometer based on the universal rectangular architecture[45], allowing the implementation of arbitrary linear optical transformations. **b**, Each BS of arbitrary reflectivity *R*, required in the scheme described elsewhere[45], is implemented via a module composed of a Mach–Zehnder interferometer with symmetric 50/50 directional couplers, and two tunable phase shifts *θ* and *φ*. The programmable phases are implemented via thermo-optic phase shifters. **c**, Picture of the actual device. The footprint of the circuit is 82 × 20 mm^2.

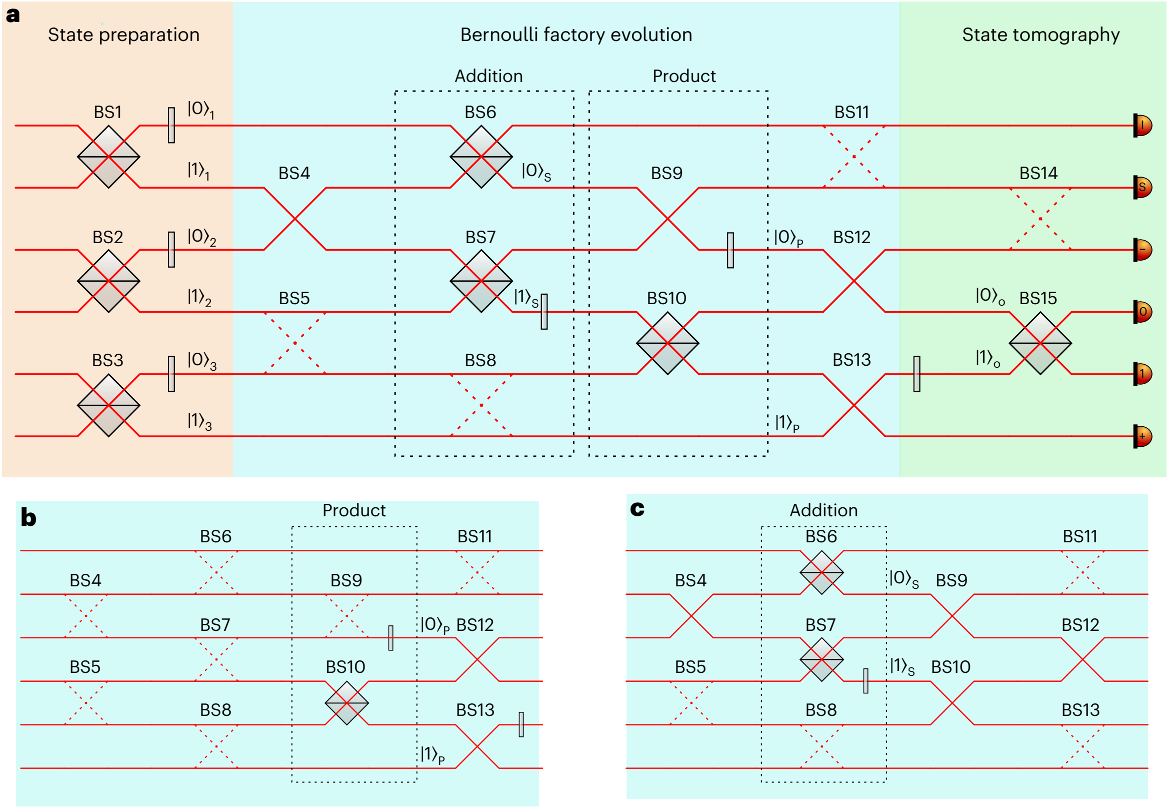

Fig. 4 | Circuit representation of the IPP programmed to implement a complete Bernoulli factory and the building blocks. a, Depiction of the full device highlighting stages for state preparation, Bernoulli factory evolution and state characterization. In particular, the Bernoulli factory evolution shown here corresponds to the settings required to implement the concatenation of an addition followed by a product. In this case, BS5, BS8, BS11 and BS14 are represented with dotted lines since their reflectivities are set to 1; the reflectivities of BS4, BS9, BS12 and BS13 are set to 0, whereas the reflectivities of BS6, BS7 and BS10 are tuned to match the value required for the desired operation. BS1, BS2, BS3 and BS15 are controlled during the experiment to generate the input state and reconstruct the output state. **b**, Settings of the internal evolution required to implement the building block corresponding to the product operation. **c**, Setting corresponding to the required configuration for the addition operation.

using the output of one operation as the input of the subsequent one. Importantly, for each product and addition, an additional photon must be added due to the post-selection process required by these operations.

Implementation

The experimental certification of our modular QQBF was implemented by using up to three photonic qubits in a six-mode IPP (Fig. 3). The IPP was fabricated in-house in a glass substrate by femtosecond laser

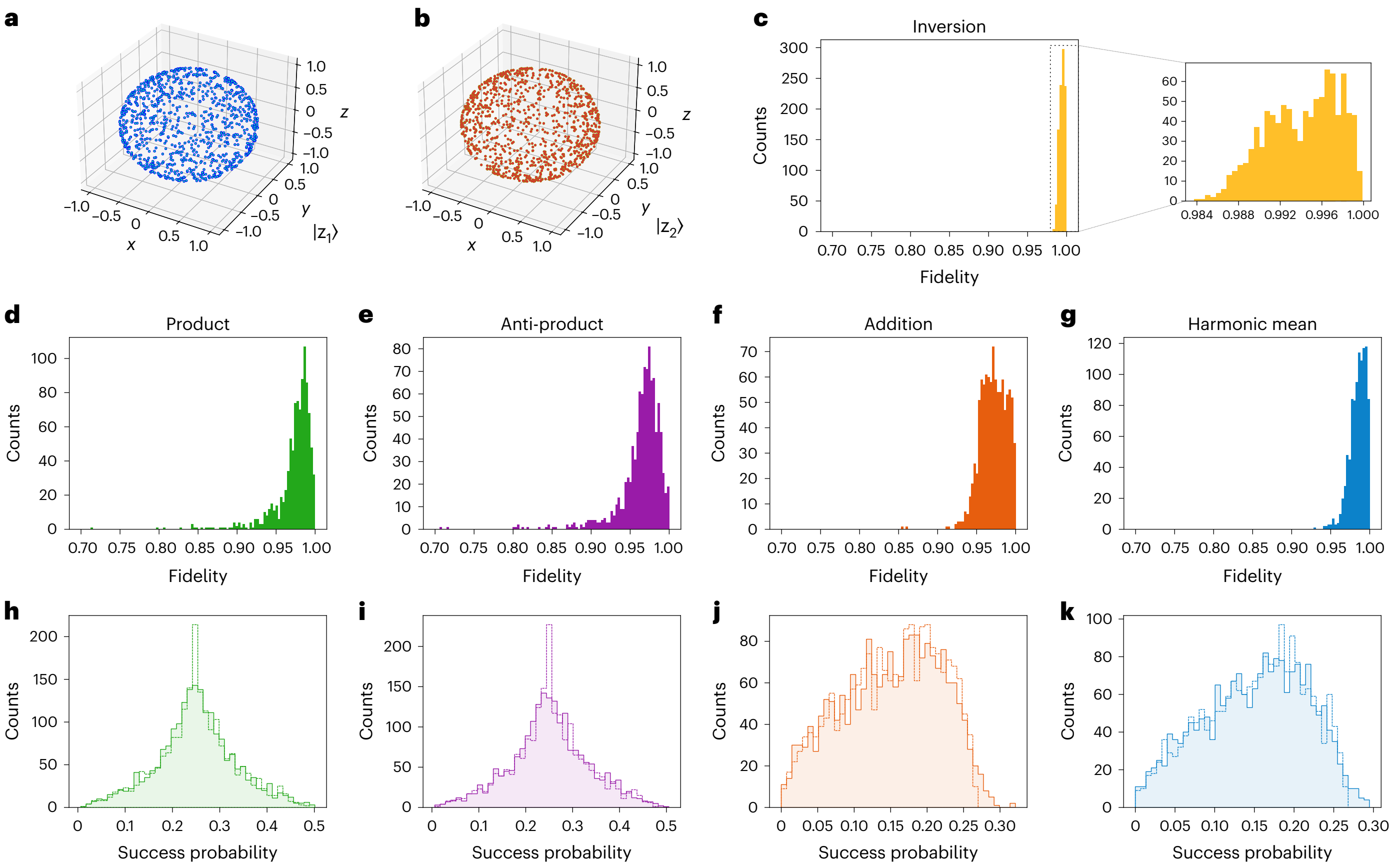

Fig. 5 | Experimental results of the building block operations. Characterization of the building blocks is performed by generating a set of 1,000 pairs of random states ($|\mathbf{z_1}\rangle$ and $|\mathbf{z_2}\rangle$) sampled uniformly from the Bloch sphere. **a**,**b**, Representation of the sampled states for $|\mathbf{z_1}\rangle$ (**a**) and $|\mathbf{z_2}\rangle$ (**b**). The fidelity of the output state after the evolution is measured by projecting it onto the known target state. **c**–**g**, Distribution of the measured fidelities for each operation, for the set of sampled states. **h**–**k**, Comparison of the distribution of success probability for each operation (solid lines) with the corresponding theoretical expectation (dashed lines) for the set of sampled states.

micromachining[34,35]. A complete scheme of the experimental apparatus used for the experiment is described in the Methods and Supplementary Note 4. We discuss now, in detail, how to implement a QQBF in our six-mode integrated interferometer, and specifically how to achieve the different required operations by suitably programming the BS network according to the block scheme shown in Fig. 4a. Note that this approach, demonstrated here for six modes and thus accommodating three dual-rail qubits, could be extended to arbitrary dimensions by scaling up the architecture. Our six-mode device is composed of six layers of BSs with arbitrary reflectivities, and phases in the [0, 2π) interval. The functionality of the different layers can be divided into three main stages, corresponding to state preparation, Bernoulli factory evolution (implementing the linear optical elements for the desired operation) and state characterization.

In the state preparation stage, the six input modes are mixed in pairs by using three different BSs. For each BS, a phase shifter is present in one of the two output ports. This configuration allows the preparation of a set of generic input qubits in the dual-rail encoding (Supplementary Note 5).

In the second stage of the device, the actual evolution for the desired Bernoulli factory operation is applied. More specifically, the reflectivity of the BSs and the phase applied by the phase shifters are appropriately tuned depending on the unitary evolution to be implemented. In particular, the scheme shown in Fig. 4a represents the implementation of an addition operation followed by a product operation, whereas Fig. 4b,c represents the optical elements required for the implementation of each operation individually (configurations for the other operations are reported in Supplementary Note 6). Note that the addition operation is similar but not equal to the one represented in Fig. 2, since here the first two waveguides are exchanged. This change is inserted to reduce the number of layers required for the concatenation of two operations and is implemented by replacing the reflectivity of BS6 with its complement, thereby making BS6 and BS7 complementary.

The final stage performs the necessary operations to characterize the output state. The system can be used to perform either tomography or direct measurement of the fidelity compared with a target state. State tomography for a single qubit requires three projective measurements on mutually orthogonal bases, from which we can reconstruct the output state[36]. On the other hand, to estimate the fidelity, the characterization stage is tuned to act as the projector onto the target state (Supplementary Note 5). In such a way, the verification of the protocol does not require full tomographic reconstruction of the output state. Note that if the output state is used as an input for additional calculations, the output modes $|0\rangle_o$ and $|1\rangle_o$ are not detected and can be routed to subsequent manipulation modules.

Experimental results

The first step towards characterizing the modular QQBF described above involves the demonstration of the individual building blocks by using the six-mode integrated processor. In particular, according to the required interferometric schemes (Fig. 4b,c), the current inside the thermo-optic phase shifters of the IPP is tuned to provide the required BS reflectivities and phase shifts.

Table 1 | Characterization of single operations

Operation	Operation	Measured	Corrected
		mean fidelity	mean fidelity
		F_M	F_C
Inversion	$1/z$	0.989±0.003	1.000±0.003
Product	z_1z_2	0.95±0.02	0.99±0.02
Anti-product	$-z_1z_2$	0.95±0.03	0.99±0.02
Addition	z_1+z_2	0.90±0.05	0.99±0.02
Harmonic mean	$z_1z_2/(z_1+z_2)$	0.92±0.05	0.99±0.02

F_M is estimated by averaging over an ensemble of 1,000 input sets of states uniformly sampled from the Bloch sphere.

Table 2 | Characterization of concatenated operations

Input	Output	Corrected fidelity	Theoretical fidelity
(z_1, z_2, z_3)		F_C	F_D
Concatenation product–addition[a]			
(0, 0, 0)	0	0.993±0.005	1
(∞, ∞, 0)	∞	0.993±0.005	1
(1, 1, 0)	1	0.95±0.02	0.96±0.01
(0, 0, 1)	1	0.80±0.02	0.79±0.05
(1, 1, 1)	2	0.93±0.01	0.92±0.03
Concatenation addition–product[b]			
(0, 0, 1)	0	0.98±0.01	1
(∞, 0, 1)	∞	1±0.01	1
(1, 0, 1)	1	0.87±0.02	0.88±0.02
(0, 1, 1)	1	0.88±0.02	0.88±0.02
(1, 1, 1)	2	0.85±0.02	0.88±0.02

[a] Results obtained from the concatenation of a product followed by an addition. [b] Results for the concatenation of an addition, followed by a product. The measured F_M value is directly estimated from the raw experimental data. F_C is the fidelity measured at the output of the IPP by subtracting the dark counts and accidental coincidences. Conversely, F_D is calculated by taking into account the partial distinguishability of the input photons. More details on the data analysis are provided in Supplementary Notes 7 and 8. All the errors are estimated from the propagation of the Poisson statistic proper of single-photon counts.

The operation of every single block is characterized by preparing (in the first stage of the circuit) a set of random input states ($|\mathbf{z_1}\rangle$ and $|\mathbf{z_2}\rangle$) sampled from a uniform distribution on the Bloch sphere (Fig. 5a,b). Each pair of states is generated in the state preparation stage of the circuit by setting the phase and reflectivity of the first layer of the interferometer. After the transformation, the output is validated by measuring the success probability of the post-selection used and the fidelity reached with respect to the target state. The overall figure of merit defining the quality of implementation is provided by the mean fidelity over the set of sampled states. In Fig. 5c–g, we report the results of the measured output fidelities between the output state and target state of the operation, for all the three building blocks (inversion, product and addition). The average results are summarized in Table 1. Furthermore, in Fig. 5h–k, we report the histograms showing the output distribution of the success probabilities for the two operations implemented probabilistically (product and addition). From a direct comparison of the obtained results with the theoretical expectations, we find that the operations implemented by the circuit are performed with fidelities close to a unitary value, thereby demonstrating the realization of the building blocks of a QQBF. In this case, corresponding to the verification of each stand-alone operation, the effect of experimental noise due to photon distinguishability is almost negligible. Indeed, the inversion operation scheme does not rely on photon interference, whereas both product and addition implementations are verified via two-photon experiments, which, in our source, belong to the same generated pair and thus possess a high degree of indistinguishability.

As the second step, we demonstrate the modularity of our scheme by showing the possibility of concatenating the individual operations. This aspect is necessary to fulfil all the requirements for the correct implementation of a complete Bernoulli factory. To test the concatenation of an addition, followed by a product [$(z_1+z_2)z_3$], the circuit operation is programmed according to the layout shown in Fig. 4a. This requires three input photons. The first two photons, impinging on BS1 and BS2, encode the input states for the addition. The third photon impinging on BS3, together with the output state from the first operation, encode the inputs of the product operation. Finally, the output of both concatenated blocks is validated by direct projection onto the target state in the final stage of the device for an estimation of fidelity.

To test the correctness of the concatenation, we measure the output fidelity for a particular set of states corresponding to relevant choices of the input. All the results are summarized in Table 2, where we report the obtained output-state fidelities. Being a three-photon experiment, this implementation requires the injection of photons generated by the source from different pairs. To compare the experimental data with the theoretical prediction, partial photon distinguishability between the input photons has to be taken into account. Thus, the fidelity F_C, after the subtraction of dark counts and accidental coincidences, has to be compared with a theoretical model that calculates F_D by taking into account only the partial distinguishability between the input photons (Supplementary Note 7). We note that this effect is due to the used photon source, and not to the QQBF implementation itself. The obtained results show a high degree of compatibility between F_C and F_D, thereby demonstrating the correct implementation of the concatenation of building blocks. Additionally, we have performed the QQBF implementation of a different function, obtained by exchanging the order of the addition and product operations (Supplementary Note 6). Also, for this different configuration, we obtain a high degree of compatibility with the theoretical predictions. All these results are summarized in Table 2.

Discussion

In this work, we have devised and demonstrated experimentally a full Bernoulli factory working with quantum states both at input and output (that is, a QQBF). In particular, we have proposed three interferometer designs implementing the basic operations of a field on qubit states. These act as building blocks for the implementation of the Bernoulli factory and, remarkably, can also be concatenated in different orders. This shows the modularity of our approach, making it capable, in principle, of implementing the complete set of functions known to be theoretically simulable. In addition, our methodology guarantees an important ingredient at the core of the Bernoulli factory problem, that is, manipulations that are truly oblivious to the input-state biases. Here we have implemented our scheme by means of a fully programmable six-mode IPP, manipulating three photonic qubits. We report a high degree of control in the optical operation of the IPP and a very high fidelity in the obtained results.

We note that the same device settings allow the implementation of more than one function depending on the post-selection event detected. Further investigation can be foreseen to investigate which functions can be implemented simultaneously with our devices. Moreover, the exploitation of fast reconfiguration would enable the application of feed-forward techniques, to allow the programming of subsequent stages depending on measurements and detections performed in previous ones. The feed-forward process could enable the active control of phase in the product module, thereby converting the anti-product operation into the product one and enhancing the success probability of the operation by a factor 2. Additionally, further investigation involves verifying whether the success probability can be boosted by adding ancillary photons and modes.

The successful integration of the algorithm within innovative integrated devices, as reported in this Article, opens the way to QQBF implementations as subroutine algorithms in compact platforms, which exploit the stability of the overall process. Indeed, current developments in photonic integrated technologies already facilitate the realization of systems with progressively increasing sizes. The use of photonic platforms to build a fundamental subroutine allows its natural integration at the interface between quantum computation and quantum communication networks, thereby enabling the possibility to exploit the substrate of photonic communication technology, which is presently at a high level of technological and commercial maturity. In this scenario, the femtosecond laser micromachining technology used to fabricate the IPP may play a relevant role in providing custom-tailored photonic components. In particular, its unique three-dimensional capabilities may be beneficial in compactifying circuit designs[37,38] and in enabling random transformations[39,40]. Moreover, the compatibility of our IPP with different types of photon source such as demultiplexed quantum dot sources[41] allows the possibility to scale up the used number of photons in coincidence. In addition, we can also implement protocols of error mitigation to deal with the experimental imperfection present in the apparatus such as the partial distinguishability between photons[42] or imperfect BSs[43]. The reliability, modularity and accuracy of our platform indeed pave the way towards the implementation of more complex protocols in which Bernoulli factories represent a key ingredient. Nevertheless, it is worth noting that Bernoulli factories are not limited to photonic implementations, and hence, this class of protocols could find application in different platforms ranging from ions to superconducting qubits.

Online content

Any methods, additional references, Nature Portfolio reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41566-024-01526-8.

References

1. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
2. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
3. Harrow, A. W. & Montanaro, A. Quantum computational supremacy. *Nature* **549**, 203–209 (2017).
4. Feynman, R. P. Simulating physics with computers. *Int. J. Theor. Phys.* **21**, 467–488 (1982).
5. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2009).
6. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
7. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proc. Twenty-Eighth Annual ACM Symposium on Theory of Computing—STOC'96* 212–219 (ACM Press, 1996).
8. David Deutsch, R. J. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A* **439**, 553–558 (1992).
9. Blok, M. S., Kalb, N., Reiserer, A., Taminiau, T. H. & Hanson, R. Towards quantum networks of single spins: analysis of a quantum memory with an optical interface in diamond. *Faraday Discuss.* **184**, 173–182 (2015).
10. Willett, R. L., Nayak, C., Shtengel, K., Pfeiffer, L. N. & West, K. W. Magnetic-field-tuned Aharonov-Bohm oscillations and evidence for non-Abelian anyons at ν=5/2. *Phys. Rev. Lett.* **111**, 186401 (2013).
11. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
12. Polino, E., Valeri, M., Spagnolo, N. & Sciarrino, F. Photonic quantum metrology. *AVS Quantum Sci.* **2**, 024703 (2020).
13. Agresti, I. et al. Experimental device-independent certified randomness generation with an instrumental causal structure. *Commun. Phys.* **3**, 110 (2020).
14. Zahidy, M. et al. Quantum randomness generation via orbital angular momentum modes crosstalk in a ring-core fiber. *AVS Quantum Sci.* **4**, 011402 (2022).
15. Guo, X. et al. Parallel real-time quantum random number generator. *Opt. Lett.* **44**, 5566–5569 (2019).
16. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004 (2017).
17. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. *Theory Comput.* **9**, 143–252 (2013).
18. Boixo, S. et al. Characterizing quantum supremacy in near-term devices. *Nat. Phys.* **14**, 595–600 (2018).
19. Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
20. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A: Math. Theor.* **44**, 095305 (2011).
21. Hamilton, C. S. et al. Gaussian boson sampling. *Phys. Rev. Lett.* **119**, 170501 (2017).
22. Keane, M. S. & O'Brien, G. L. A Bernoulli factory. *ACM Trans. Model. Comput. Simul.* **4**, 213–219 (1994).
23. Vats, D., Gonçalves, F. B., Łatuszyński, K. & Roberts, G. O. Efficient Bernoulli factory Markov chain Monte Carlo for intractable posteriors. *Biometrika* **109**, 369–385 (2021).
24. Dughmi, S., Hartline, J. D., Kleinberg, R. & Niazadeh, R. Bernoulli factories and black-box reductions in mechanism design. *ACM SIGecom Exch.* **16**, 60–73 (2017).
25. Dale, H., Jennings, D. & Rudolph, T. Provable quantum advantage in randomness processing. *Nat. Commun.* **6**, 8203 (2015).
26. Dale, H. *Quantum Coins and Quantum Sampling*. PhD thesis, Imperial College London (2016).
27. Yuan, X. et al. Experimental quantum randomness processing using superconducting qubits. *Phys. Rev. Lett.* **117**, 010502 (2016).
28. Patel, R. B., Rudolph, T. & Pryde, G. J. An experimental quantum Bernoulli factory. *Sci. Adv.* **5**, eaau6668 (2019).
29. Jiang, J., Zhang, J. & Sun, X. Quantum-to-quantum Bernoulli factory problem. *Phys. Rev. A* **97**, 032303 (2018).
30. Liu, Y. et al. General quantum Bernoulli factory: framework analysis and experiments. *Quantum Sci. Technol.* **6**, 045025 (2021).
31. Zhan, X., Wang, K., Xiao, L., Bian, Z. & Xue, P. Experimental demonstration of quantum-to-quantum Bernoulli factory. *Phys. Rev. A* **102**, 012605 (2020).
32. Kashefi, E. & Pappa, A. Multiparty delegated quantum computing. *Cryptography* **1**, 12 (2017).
33. Wang, J., Sciarrino, F., Laing, A. & Thompson, M. G. Integrated photonic quantum technologies. *Nat. Photon.* **14**, 273–284 (2020).
34. Meany, T. et al. Laser written circuits for quantum photonics. *Laser Photon. Rev.* **9**, 363–384 (2015).
35. Corrielli, G., Crespi, A. & Osellame, R. Femtosecond laser micromachining for integrated quantum photonics. *Nanophotonics* **10**, 3789–3812 (2021).
36. James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of qubits. *Phys. Rev. A* **64**, 052312 (2001).
37. Meany, T. et al. Engineering integrated photonics for heralded quantum gates. *Sci. Rep.* **6**, 25126 (2016).
38. Crespi, A. et al. Suppression law of quantum states in a 3D photonic fast Fourier transform chip. *Nat. Commun.* **7**, 10469 (2016).
39. Hoch, F. et al. Reconfigurable continuously-coupled 3D photonic circuit for boson sampling experiments. *npj Quantum Inf.* **8**, 55 (2022).

40. Tang, H. et al. Generating Haar-uniform randomness using stochastic quantum walks on a photonic chip. *Phys. Rev. Lett.* **128**, 050503 (2022).
41. Rodari, G. et al. Semi-device independent characterization of multiphoton indistinguishability. Preprint at https://arxiv.org/abs/2404.18636 (2024).
42. Marshall, J. Distillation of indistinguishable photons. *Phys. Rev. Lett.* **129**, 213601 (2022).
43. Miller, D. A. B. Perfect optics with imperfect components. *Optica* **2**, 747–750 (2015).
44. Nacu, Ş. & Peres, Y. Fast simulation of new coins from old. *Ann. Appl. Probab.* **15**, 93–115 (2005).
45. Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S. & Walmsley, I. A. Optimal design for universal multiport interferometers. *Optica* **3**, 1460–1465 (2016).

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Methods

Photon source

The photons required for dual-rail encoding are produced by a source based on non-collinear spontaneous parametric down conversion. In particular, two pairs of photons are emitted by the source, which are deterministically separated in four different paths by exploiting their polarization state (using half-wave plates and polarizing BSs and coupled into single-mode fibres). One photon is directly detected by a single-photon avalanche photodiode and acts as a trigger. The other three photons are sent through different paths, where they are made indistinguishable in the polarization and time-of-arrival degrees of freedom, and finally injected into the IPP. Optical fibres are also used to collect light at the outputs of the IPP. The detection stage is composed of six in-fibre BSs, one for each output of the IPP, which feeds 12 single-photon avalanche photodiode detectors. In fact, this system implements six probabilistic photon-number-resolving detectors that are used to characterize the output states.

IPP

The IPP consists of a reconfigurable, six-mode waveguide interferometer[46] realized according to the rectangular layout proposed elsewhere[45] and thus able to produce any linear transformation of six modes. The waveguides follow the optical paths depicted in Fig. 3a, the 15 BSs being actually implemented by tunable Mach–Zehnder interferometers (in Fig. 3b). Each of the latter components, in turn, consists of two cascaded waveguide directional couplers and is equipped with two programmable phase shifters. One of the phase shifters is placed inside the Mach–Zehnder ring, whereas the other one is placed on one of its input ports. By acting on these overall 30 phase shifters, full control of the IPP operation is achieved.

We have fabricated the IPP by femtosecond laser micromachining[34,35] in EagleXG (Corning) glass substrate. The waveguides are directly inscribed in the substrate by laser irradiation, 25 µm deep below the substrate surface, followed by thermal annealing[47,48]. Phase shifters base their functioning on the thermo-optic effect and consist of microheaters realized on the chip surface[49]. The microheaters are resistive paths patterned by laser ablation on a metallic layer, which is deposited on the chip surface. On driving suitable currents into the microheaters, local heating of the substrate is achieved in a precise and controlled way. Such local heating induces, in turn, a refractive index change and thus controlled phase delays in the waveguides due to the thermo-optic effect. The chip surface is further microstructured by femtosecond laser processing, particularly creating thermal insulation trenches at the sides of the microheaters, to increase their efficiency and reduce cross-talk[50]. The full IPP has a footprint of 82 × 20 mm^2. Fibre arrays are glued to the input and output ports to provide optical connections, and fibre-to-fibre optical loss is 3 dB. A careful calibration of the IPP operation with respect to the driving currents in the microheaters was performed using coherent light, yielding an average fidelity of 99.7% to the target operation, calculated using thousands of randomly chosen unitary transformations. The calibration procedure allowed us to independently characterize the effect of each phase shifter on all the Mach–Zehnder interferometers. The measurements showed a full reconfiguration (that is, a 2π phase shift) with a dissipated power of 40.7 ± 5.4 mW per thermal shifter and a cross-talk on first-neighbour interferometers of 19.0 ± 5.2%. More details about the characterization of the processor with classical light can be found elsewhere[46].

Data availability

The raw data that support the findings of this study are available from the corresponding author upon reasonable request.

References

46. Pentangelo, C. et al. High-fidelity and polarization-insensitive universal photonic processors fabricated by femtosecond laser writing. *Nanophotonics* **13**, 2259–2270 (2024).
47. Arriola, A. et al. Low bend loss waveguides enable compact, efficient 3D photonic chips. *Opt. Express* **21**, 2978–2986 (2013).
48. Corrielli, G. et al. Symmetric polarization-insensitive directional couplers fabricated by femtosecond laser writing. *Opt. Express* **26**, 15101–15109 (2018).
49. Flamini, F. et al. Thermally reconfigurable quantum photonic circuits at telecom wavelength by femtosecond laser micromachining. *Light Sci. Appl.* **4**, e354 (2015).
50. Ceccarelli, F. et al. Low power reconfigurability and reduced crosstalk in integrated photonic circuits fabricated by femtosecond laser micromachining. *Laser Photon. Rev.* **14**, 2000024 (2020).

Acknowledgements

This work was supported by the FET project PHOQUSING ('PHOtonic Quantum SamplING machine'—grant agreement no. 899544) (F.H., T.G., G.C., N.S., F.C., C.P., S.P., A.C., R.O. E.F.G. and F.S.); by ICSC—Centro Nazionale di Ricerca in High Performance Computing, Big Data and Quantum Computing, funded by European Union—NextGenerationEU (N.S., R.O. and F.S.); and by FCT—Fundação para a Ciência e a Tecnologia (Portugal) via project CEECINST/00062/2018 (E.F.G.). The IPP was partially fabricated at PoliFAB, the micro- and nanofabrication facility of Politecnico di Milano (https://www.polifab.polimi.it/). C.P., F.C. and R.O. thank the PoliFAB staff for their valuable technical support.

Author contributions

F.H., T.G., L.C., G.C., N.S., R.O., E.F.G. and F.S. conceived the concept and scheme for the QQBF. F.C., C.P., S.P., A.C. and R.O. fabricated the photonic chip and characterized the integrated device using classical optics. F.H., T.G., G.C., N.S. and F.S. carried out the quantum experiments and performed the data analysis. All the authors discussed the results and contributed to the writing of the paper.

Competing interests

F.H., T.G., L.C., G.C., N.S., R.O., E.F.G. and F.S. are listed as inventors on corresponding pending patent applications in Italy (no. 102023000012279) and Portugal (no. 20232005054430), both filed on 15 June 2023 and titled 'Quantum Bernoulli factory photonic circuit independent of input state bias' dealing with schemes for the implementation of the QQBF. F.C. and R.O. are co-founders of the company Ephos. The other authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41566-024-01526-8.

Correspondence and requests for materials should be addressed to Fabio Sciarrino.

Peer review information *Nature Photonics* thanks Stefano Paesani, Jianwei Wang and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Reprints and permissions information is available at www.nature.com/reprints.