SCIENTIFIC REPORTS

OPEN

Physical implementation of oblivious transfer using optical correlated randomness

Received: 6 February 2017
Accepted: 10 July 2017
Published online: 16 August 2017

Tomohiro Ito[1], Hayato Koizumi[1], Nobumitsu Suzuki[1], Izumi Kakesu[1], Kento Iwakawa[1], Atsushi Uchida[1], Takeshi Koshiba[1], Jun Muramatsu[2], Kazuyuki Yoshimura[3], Masanobu Inubushi[2] & Peter Davis[4]

We demonstrate physical implementation of information-theoretic secure oblivious transfer based on bounded observability using optical correlated randomness in semiconductor lasers driven by common random light broadcast over optical fibers. We demonstrate that the scheme can achieve one-out-of-two oblivious transfer with effective key generation rate of 110 kb/s. The results show that this scheme is a promising approach to achieve information-theoretic secure oblivious transfer over long distances for future applications of secure computation such as privacy-preserving database mining, auctions and electronic-voting.

With the rapid evolution of big data and cloud computing systems there is increasing interest in practical schemes for secure operations on information on large scales. One example is secure computation which would allow computation of functions over data without revealing the data[1–15]. Practical large scale implementations of secure computation are needed to realize applications such as private information retrieval, privacy preserving database mining, auctions, and electronic voting systems.

A key component for secure computation is oblivious transfer. Oblivious transfer is message transfer in which a sender sends encoded messages in such a way that the receiver can only decode some of the messages and the sender does not know which messages were decoded. The original notion of oblivious transfer using an erasure channel was given by Rabin[16]. Later, one-out-of-two oblivious transfer was considered by Even *et al.*[17]. Naor and Pinkas[18,19] gave an oblivious transfer protocol based on the Diffie-Hellman assumption, where the protocol relies on computational complexity. It has been known that the Naor-Pinkas protocol is time-consuming, and large amount of computation is required. The oblivious transfer extension technique of Ishai *et al.*[20] and follow up work has been aimed at achieving faster and more efficient oblivious transfer.

Various schemes for oblivious transfer based on information-theoretic security have also been proposed. Information-theoretic oblivious transfer can be secure with respect to adversaries that are computationally unbounded. Moreover, information-theoretic oblivious transfer can be future proof in the sense that secrets will not be revealed by future advances in computational power. Information-theoretic schemes are based on the idea of distilling a secret bit, or string of secret bits, from a statistical advantage in correlation of bits acquired from a probabilistic system. Different models can be distinguished based on specific features of the probabilistic model of the system. Following the original notion of the erasure channel[16], there have been schemes proposed based on noisy channels[21–24], bounded storage[25], wireless communication systems[26], quantum mechanical systems[27–30], and network behaviors[31,32]. In the noisy channel model, users observe a random sequence from a common source (such as a broadcast satellite), but the detected bits are different with a certain probability due to noise in the channel. In this case, sets of matching bits can be identified ("distilled") by techniques such as comparing results of hash functions. The bounded storage model assumes that users observe the same random sequence but some observations are randomly dropped due to storage limits. Matching bits can be identified by exchanging sequence labels of stored bits. Quantum schemes for oblivious transfer are based on a random choice

[1]Department of Information and Computer Sciences, Saitama University, 255 Shimo-okubo,Sakura-ku, Saitama City, Saitama, 338-8570, Japan. [2]NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato, Wakamiya, Atsugi-Shi, Kanagawa, 243-0198, Japan. [3]Department of Information and Electronics, Graduate school of Engineering, Tottori University 4-101 Koyama-Minami, Tottori, 680-8552, Japan. [4]Telecognix Corporation, Japan, 58-13 Shimooji-cho, Yoshida, Sakyo-ku, Kyoto, 606-8314, Japan. Correspondence and requests for materials should be addressed to A.U. (email: auchida@mail.saitama-u.ac.jp)

of observation function in a quantum mechanical system. Matching bits can be identified by transmitting observation parameter information together with observation sequence labels.

However, feasible schemes for physical implementation of information-theoretic oblivious transfer over long distance with high bit rate, which is necessary for practical use, are still lacking. Information-theoretic schemes are difficult to implement because of the difficulty of generating large volumes of entropy in a way that corresponds to a reliable probabilistic model such as an erasure channel[16] or a binary symmetric channel[21] and its variant[22]. Entropy sources based on analog physical signals depend on the bandwidth and dynamic ranges of analog-to-digital detectors, as can be seen for example in the ongoing efforts to build non-deterministic random number generators operating above Gigabit per second (Gbps)[33–35]. Implementation of channel models such as Gaussian or wireless channels[23–25] rely on assumptions about the stochastic state of the channel which are difficult to guarantee in practice, especially in open environments.

Recently, it has been shown that a correlated random source suitable for information-theoretic security applications can be implemented using random light transmitted large distances over optical fiber and injected into semiconductor lasers[36, 37]. The parameter-dependent synchronization properties of complex dynamical systems driven by a common random signal[38–41] are used to realize a correlated random source for secure key distribution based on information-theoretic security[42]. The scheme assumes a random choice of observation function in a classical optical system where the same choices result in detecting identical bits, and different choices result in uncorrelated bits. Matching bits can be identified by communicating information about observation choices over an open communication channel. The correlated randomness required for information-theoretic security relies on the property of bounded observability[43–45], whereby the number of simultaneous observations of a system by a single user is limited and the state of the observed system cannot be known by any other means. These properties can be feasible due to technological limits of observing a physical system. The proposal in refs 36 and 37 was based on the technological difficulty of completely observing broadband random light. The physical system was implemented using common broadband random light transmitted over optical fiber. Users observe the received light by injecting it into a laser device and detect the output to obtain binary bits. Random choice of observation function was implemented with a random choice of a laser parameter, so that identical choices result in detecting identical bits, and different choices result in uncorrelated bits. Secure key distribution using this scheme has been demonstrated experimentally for nodes separated by over 120-km of optical fiber at a key generation rate of 64 kb/s[37].

The bounded observability scheme is similar to a quantum scheme in the sense of generating a sequence of parameter-bit pairs. However, the difficulty of transmitting quantum states over large distances currently limits the separation distance to tens of kilometers. The optical implementation is feasible for generating correlated randomness over hundreds of kilometers using conventional optical amplifiers, since the scheme uses a classical optical state rather than a quantum optical state.

This physical implementation of a source of correlated randomness in an optical fiber system was a breakthrough in both speed and reliability over large distances, bringing information-theoretic schemes closer to the regime of practical feasibility. The work in this paper builds on this breakthrough and shows how to harness it for information-theoretic oblivious transfer. Specifically, we present the first experimental demonstration of information-theoretic oblivious transfer using an optical correlated random source based on the bounded observability model.

Correlated random optical source

Figure 1 shows the proposed scheme for oblivious transfer using optical correlated randomness. A common random signal can be broadcast through optical fibers or free space (Fig. 1(a)). Two legitimate users Alice and Bob each have optical nodes (Fig. 1(b)) consisting of an optical device (Fig. 1(c)) driven by the common random optical signal. Alice and Bob independently acquire and record many observations at their respective optical nodes, where each observation consists of the values of the random observation parameters and the corresponding observed bits (Fig. 1(b)). The bits are highly correlated if the observation parameters are identical and uncorrelated if the observation parameters do not match. After recording their observations, Alice and Bob execute an oblivious transfer protocol over an open channel, and use oblivious transfer to execute secure computation. Note that the common random broadcast signal can be provided by either Alice or a trusted third party, but not by Bob.

First we describe the scheme for acquiring random sequences from the laser optical system. Alice and Bob each have a semiconductor laser with an external cavity containing a phase modulator (Fig. 1(c)). Each laser has a variable parameter v (e.g., optical-feedback phase) with different values (e.g., 0 and 1, corresponding to zero- and π-phase shift, respectively). A random broadband light S is broadcast to the users. They each inject the received light S into their laser. Each laser generates an optical output, which depends on both S and v and has the following property of correlated randomness: the temporal waveforms of the laser outputs are strongly correlated if the parameter values of Alice and Bob are the same ($v_A = v_B$), and mutually uncorrelated if the parameter values are different ($v_A \neq v_B$). Alice and Bob independently select their parameter values v_A and v_B at random. Alice and Bob simultaneously sample and quantize their laser outputs to extract bits x_A and x_B (0 or 1), respectively. Alice and Bob then store the parameter-bit pairs (v_A, x_A) and (v_B, x_B) in their data recorders (Fig. 1(b)). They repeat this procedure many times, injecting the continuously varying nonrepeating random light S to their lasers with parameters randomly selected each time t, to acquire sequences of the parameter-bit pairs $(v_A(t), x_A(t))$ and $(v_B(t), x_B(t))$, $t = 1, 2, \ldots, m$, respectively. Due to the synchronization properties of the two lasers, the same bits are obtained $(x_A(t) = x_B(t))$ between Alice and Bob when the parameters are the same $(v_A(t) = v_B(t))$, but when the parameters are different $(v_A(t) \neq v_B(t))$, the probability of the bits being equal is just 0.5.

The security of the oblivious transfer scheme with regard to malicious attacks relies on two physical limitations on observations in the optical system[36, 37]. (i) No one can continuously measure and record the entire common random light in order to repeat the observations of Alice or Bob *after* the parameter settings have been exchanged. (ii) No one can simultaneously observe the outputs for all possible parameter values while the common random

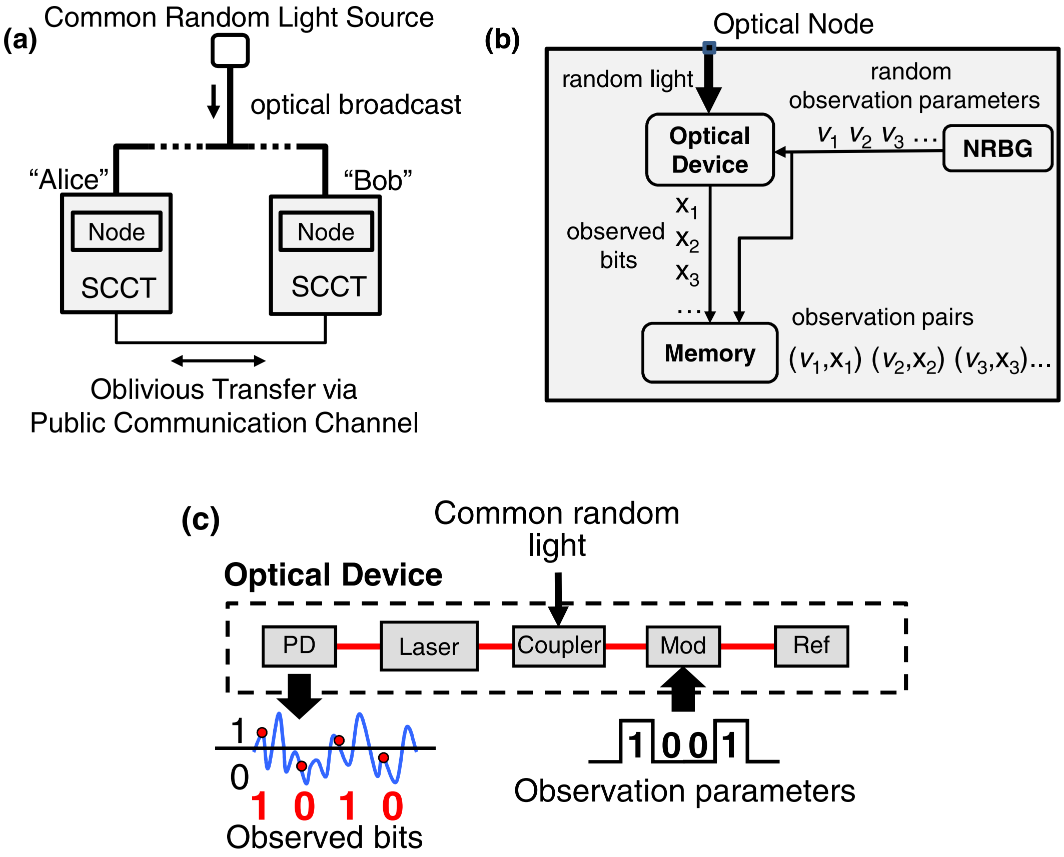

Figure 1. Schematic diagram of system for oblivious transfer using optical correlated randomness. (**a**) Total system, (**b**) optical node, and (**c**) optical device. (**a**) SCCT: secure communication and computation terminal. (**b**) NRBG: non-deterministic random bit generator. (**c**) Mod: optical phase modulator, PD: photodetector, and Ref: optical reflector.

light is being broadcast. The limitation (i) can be achieved by delaying the parameter exchange long enough to make it impossible to store the entire length of common random signal in an optical delay line or ring buffer, and by using broadband random light with a fluctuation bandwidth which is too broad to accurately and continuously electronically observe and record its fast temporal variation with current technology. The second limitation (ii) can be achieved by increasing the number of possible parameter values of the receiver optical device, to make it practically infeasible to prepare the number of devices required to simultaneously observe all possible cases. An example of a scalable receiver device based on cascaded laser systems is described in the supplementary material.

We note that in order to realize information-theoretic security, it is not necessary to prevent the attacker from obtaining some information, or to know which information they obtain. It is only necessary to estimate the amount of information that they might obtain, and apply a suitable privacy amplification procedure. There is a fundamental trade-off between the amount of partial information leak that is allowed and the rate at which secure keys can be generated for oblivious transfer.

One-out-of-two oblivious transfer protocol. One-out-of-two oblivious transfer means the following conditions hold for legitimate users Alice and Bob communicating through an authenticated public channel. (i) Alice sends two encoded messages to Bob, and Bob can only decode one of them, but not the other one. (ii) Alice cannot know which message Bob has decoded.

We propose the following protocol for one-out-of-two oblivious transfer (Fig. 2). Consider Alice has two messages, M_0 and M_1, to send to Bob, and Bob decides a binary value $b = 0$ or 1 according to which message M_b he intends to decode. First, Bob sends the following parameter set $\{c_B(t)\}^m{}_{t=1}$ to Alice,

$$c_B(t) = v_B(t) + b \tag{1}$$

where + denotes bitwise exclusive-OR (XOR) operation. That is, Bob sends his parameter set $\{c_B(t)\}^m{}_{t=1} = \{v_B(t)\}^m{}_{t=1}$ as it is to Alice if he intends to obtain M_0, or sends the inverted values $\{c_B(t)\}^m{}_{t=1} = \{v_B(t) + 1\}^m{}_{t=1}$ if he intends to obtain M_1. After Alice receives Bob's parameter set $\{c_B(t)\}^m{}_{t=1}$, Alice creates two cryptographic keys k_0 and k_1, using observed bits $x_A(t)$ corresponding to the parameter matches $v_A(t) = c_B(t)$ and $v_A(t) = c_B(t) + 1$ respectively. That is, for the key k_0, Alice uses the bits $x_A(t)$ observed at times t when $v_A(t) = c_B(t)$, and for the key k_1, Alice uses the bits $x_A(t)$ observed at times t when $v_A(t) = c_B(t) + 1$. Then Alice encrypts the message M_0 with the key k_0 and the message M_1 with the key k_1, and sends the two encrypted messages and her original parameter set $\{v_A(t)\}^m{}_t$

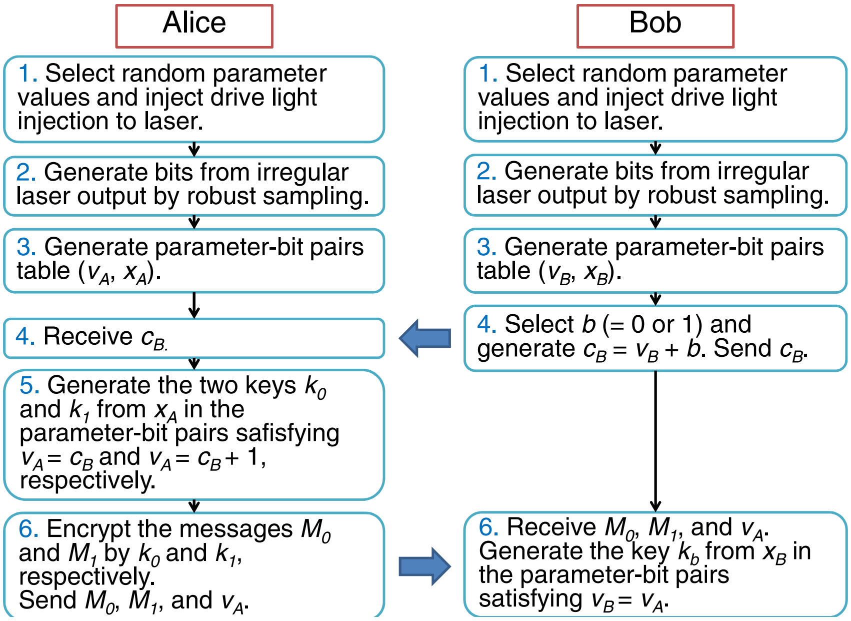
Alice
Bob
1. Select random parameter values and inject drive light injection to laser.
2. Generate bits from irregular laser output by robust sampling.
3. Generate parameter-bit pairs table (v_A, x_A).
4. Receive c_B.
5. Generate the two keys k_0 and k_1 from x_A in the parameter-bit pairs safisfying $v_A = c_B$ and $v_A = c_B + 1$, respectively.
6. Encrypt the messages M_0 and M_1 by k_0 and k_1, respectively.
Send M_0, M_1, and v_A.
1. Select random parameter values and inject drive light injection to laser.
2. Generate bits from irregular laser output by robust sampling.
3. Generate parameter-bit pairs table (v_B, x_B).
4. Select b (= 0 or 1) and generate $c_B = v_B + b$. Send c_B.
6. Receive M_0, M_1, and v_A.
Generate the key k_b from x_B in the parameter-bit pairs satisfying $v_B = v_A$.

Figure 2. Protocol of one-out-of-two oblivious transfer. +Denotes bitwise exclusive-OR operation. $\nu_{A,B}$: random observation parameters for Alice and Bob. $x_{A,B}$: observed bits for Alice and Bob.

$_{=1}$ to Bob. Finally, Bob creates a key using the bits $x_B(t)$ for the sampling time t such that $\nu_B(t) = \nu_A(t)$. Bob's key will be identical to Alice's key k_b, where $b = 0$ or 1 is the value Bob initially decided. Thus Bob is able to decode the message M_b that he intended but not the other message, and Alice does not know which of the two messages Bob can decode.

This protocol can be extended to include privacy amplification to make it robust against statistical bias in bits and secure against malicious attacks that might learn partial information about the observations of other users. Details are given in the Methods section.

Results

Experimental implementation of oblivious transfer.

The components of the optical system are feasible for practical optical fiber communication (See Methods for details). The lasers are semiconductor lasers operating at wavelengths used for long range optical communication, 1.5 microns. The common random optical signal is generated using a laser with phase modulated by a random noise generator[38], and sent to Alice and Bob over optical fiber. In the optical nodes of Alice and Bob, the received common random signal is injected into a laser with an external cavity under conditions for so-called generalized synchronization[35,39], such that after a transitory evolution the fluctuating dynamical state of the laser is determined by the combination of drive signal and the optical feedback phase[38,46]. The optical feedback phase can be controlled by an external electrical signal and is used as the observation parameter for the oblivious transfer protocol.

Figure 3(a) and (b) show examples of correlation plots between temporal waveforms of the output from the lasers of Alice and Bob. The temporal waveforms are correlated when the parameters of Alice and Bob are matched, and uncorrelated when the parameters are mismatched. Figure 3(c) shows the change of short-term cross correlation of the temporal waveforms between the two laser outputs for Alice and Bob when the parameters are repeatedly shifted (0 and 1 correspond to zero and π phase shift, respectively) in independent random sequences. The feedback phase of the lasers is modulated with a return-to-zero (RZ) format at a frequency of 2 MHz to ensure the transient time of synchronization. After a short transient time of each switch, the correlation settles to a steady value. High values of the short-term cross correlation are obtained when the phase parameters match, and low correlation values are observed when the parameters do not match. The intensity of the fluctuating laser output is sampled with a 1-bit digitizer at a fixed time after the parameter switch longer than the correlation relaxation time. In order to reduce the effect of noise and synchronization errors, we implemented a method known as robust sampling for the 1-bit sampler[36,37]. This method uses two intensity thresholds - a value above the upper threshold is detected as 1, a value below the lower threshold is detected as 0, and the sample is discarded otherwise. Repeated switching and sampling at the rate of 2 MHz result in fast generation of a sequence of parameter-bit pairs including timestamps that are stored in the user's memory.

Next we examine the oblivious transfer using the parameter-bit pairs. Alice sends two messages M_0 and M_1 that are random bits encrypted with the keys k_0 and k_1, respectively. We assume that Bob selects $b = 1$ and generates key k_1 to decode the message M_1. Table 1 shows a typical result of the oblivious transfer in the case where Alice and Bob generate a 3,600-bit key, and Bob recovers the message M_1 correctly without errors. In this case, we

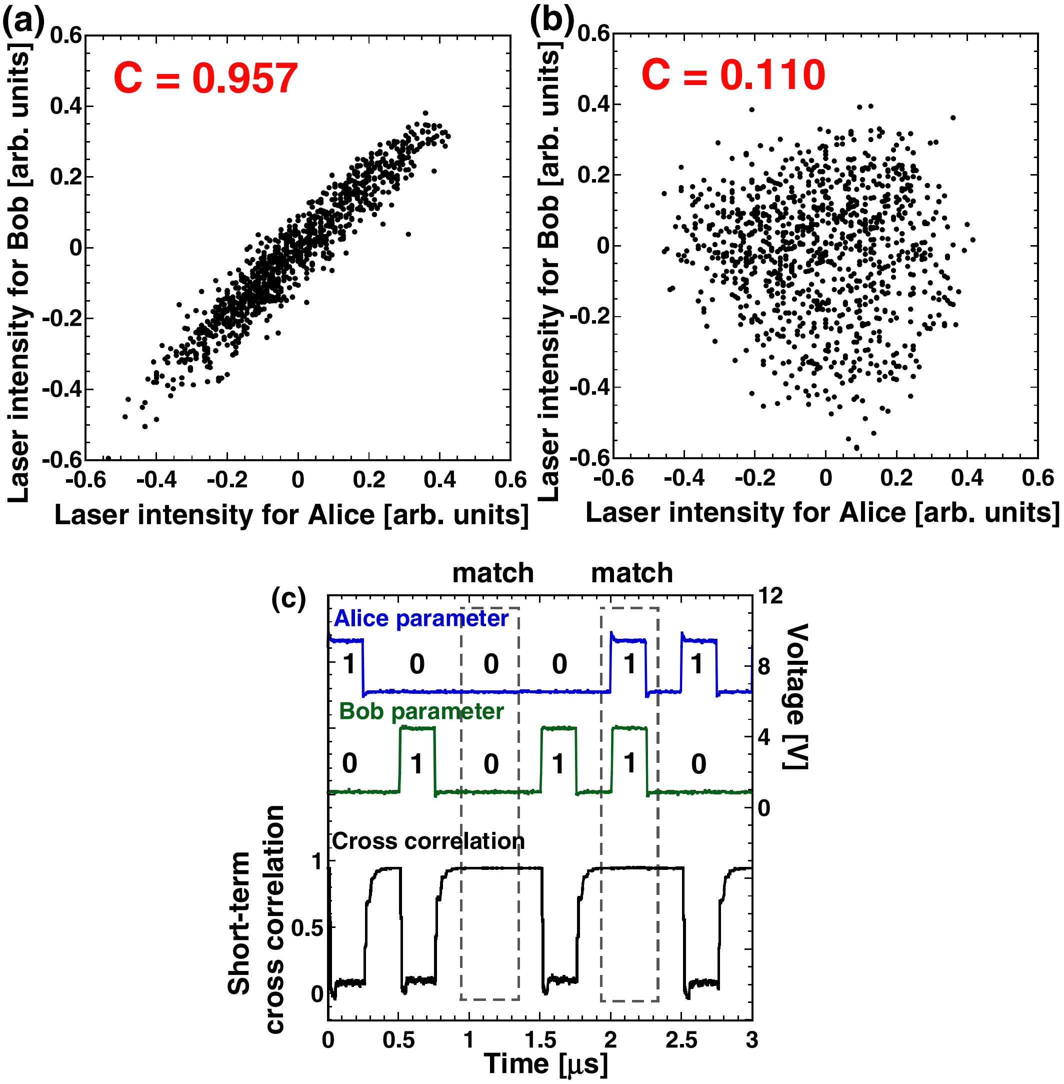

Figure 3. Experimental result of optical correlated randomness. (**a**,**b**) Correlation plots of temporal waveforms of Alice's and Bob's laser outputs. *C* indicates cross-correlation value. (**a**) Same parameter selection, and (**b**) different parameter selection. (**c**) Example of parameter switching. Alice's and Bob's parameter values and the short-term cross-correlation between Alice's and Bob's temporal waveforms are shown.

also evaluate the randomness of the generated binary key k_1. The ratio of '0' bits in k_1 is 0.4933, which satisfies the criterion of the bit bias for random bits, $0.5 \pm 3/(2\sqrt{N})$, where N is the number of bits[47].

We consider two possible attacks by Bob to decode the other message M_0, under the assumption of a semi-honest user: (i) Bob uses his key k_1 to estimate Alice's key k_0, (ii) Bob generates a new key (called k_2) using the bits that he observed at the timestamps t of observations used by Alice for k_0. (From v_A and v_B Bob knows the timestamps t of observations used by Alice for k_0 as well as k_1). These results are also shown in Table 1. For both of the attacks, the bit error rates (BERs) between Alice's k_0 and Bob's k_1 (or k_2) are close to 0.5, indicating that Bob cannot decode the message M_0. It is found that the second attack is more effective than the first one, since BER is slightly lower (BER = 0.386). The mutual information between Alice's k_0 and Bob's k_1 and k_2 generated in the two attacks are 0.0002 and 0.0269, respectively. Similarly, the second attack is more effective since there is a small correlation (see Fig. 3(b)) between the temporal waveforms used for generating the keys k_0 and k_2. The small information leakage in these attacks can be reduced by privacy amplification[48,49] (See the Methods section for details).

Next, we evaluate the key error ratio, the ratio of cases where Alice's key k_1 and Bob's key k_1 do not match due to bit errors in the optical samples. The proportion of bit errors of the optical samples depends on the two threshold values of the robust sampling - larger threshold separation results in lower BER and lower observation-pair (bit) generation rate[36,37]. Measured values of BER and bit generation rate (BGR) are shown in Fig. 4. With 2 MHz sampling clock and robust sampling with BGR of 1 Mb/s or less, the BER is less than 10^{-4}. The results in Table 1 were obtained with BGR of 220 kb/s, for which the BER is much less than 10^{-4}. Considering a match probability of 0.5, and a negligible bit error, the maximum key generation rate can be estimated as 110 kb/s.

	Legitimate users	Bob's attack 1	Bob's attack 2
	Alice k_1, Bob k_1	Alice k_0, Bob k_1	Alice k_0, Bob k_2
Number of generated bits	3600	3600	3600
Bit error rate	0	0.491	0.386
Ratio of 0	0.4933	0.4933	0.3883
Mutual information between Alice and Bob	1	0.0002	0.0269

Table 1. Result of oblivious transfer at the bit generation rate of 110 kb/s. Left column: legitimate users (comparison between Alice's key k_1 and Bob's key k_1). Middle column: Bob's attack 1 (comparison between Alice's k_0 and Bob's k_1). Right column: Bob's attack 2 (comparison between Alice's k_0 and Bob's k_2). Bob generates k_2 using the bits that he observed at the timestamps t of observations used by Alice for k_0.

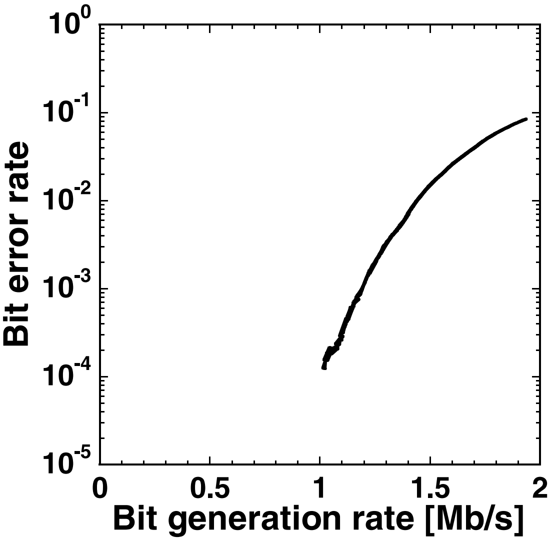

Figure 4. Relation between bit error rate (BER) and bit generation rate (BGR) for parameter-bit observation pairs of optical correlated random source for oblivious transfer. The two threshold values of the robust sampling are changed.

Secure computation. Next we demonstrate the use of oblivious transfer to implement two-party secure computation, using the one-out-of-two oblivious transfer and Yao's garbled circuit[1,2,7]. Technical details are provided in the Methods section and the supplementary material. Our purpose here is to experimentally demonstrate one way of operating the oblivious transfer system in the context of secure computation, and to evaluate the latency of the oblivious transfer system in this context.

The secure computation implemented is a comparison of two numbers, (This is known as the millionaire problem[1,2], as it corresponds to Alice and Bob comparing two numbers representing their respective wealth, to determine which is larger, without revealing their numbers to each other). The multi-bit digital comparison is translated into an encrypted Boolean circuit, called a "garbled circuit", which can be evaluated without the evaluator knowing all the inputs by making use of oblivious transfer. In the garbled circuit protocol, one of the users (Alice) encrypts each logical gate operation as an encrypted "garbled" logical table with logical values of input wires replaced by random bit strings (called labels), and sends the garbled circuit to the other user (Bob) together with the random labels corresponding to her input bits. Using one-out-of-two oblivious transfer for each input bit, Bob is able to get from Alice the label corresponding to the value of his input bit without learning the other label and without Alice knowing what his bit is. Then Bob is able to evaluate the garbled circuit to obtain the labels of the circuit output wires, which can be decoded by Alice or Bob.

We simulate the garbled circuit protocol on a personal computer and evaluated the scheme together with the implementation of oblivious transfer. Figure 5(a) shows the total execution time for input-bit lengths of 2-bit to 64-bit. We found that the total execution time is proportional to the input-bit length on the log-log scale. We achieve 32-bit and 64-bit secure comparison in 0.23 and 0.45 seconds, respectively. Figure 5(b) shows the execution time for each procedure in the secure computation. The construction of the garbled circuit (B in Fig. 5(b)) and execution of the oblivious transfer (D in Fig. 5(b)) are the most time-consuming procedures. The execution time of the oblivious transfer is proportional to the input-bit length for large input-bit lengths. The time required for the oblivious transfer procedure is 0.2 seconds for 64-bit secure comparison, and corresponds to 44% of the total execution time (0.45 seconds). The time for the oblivious transfer was measured under the condition where the observation parameter-bit pairs are already stored in the computer. The pairs were generated in advance with the same sampling conditions as for Table 1. Hence, the time to generate the observation parameter-bit pairs required for each 100-bit oblivious transfer can be estimated as 100 bits-per-key/110 kb/s = 0.00091 sec, and the

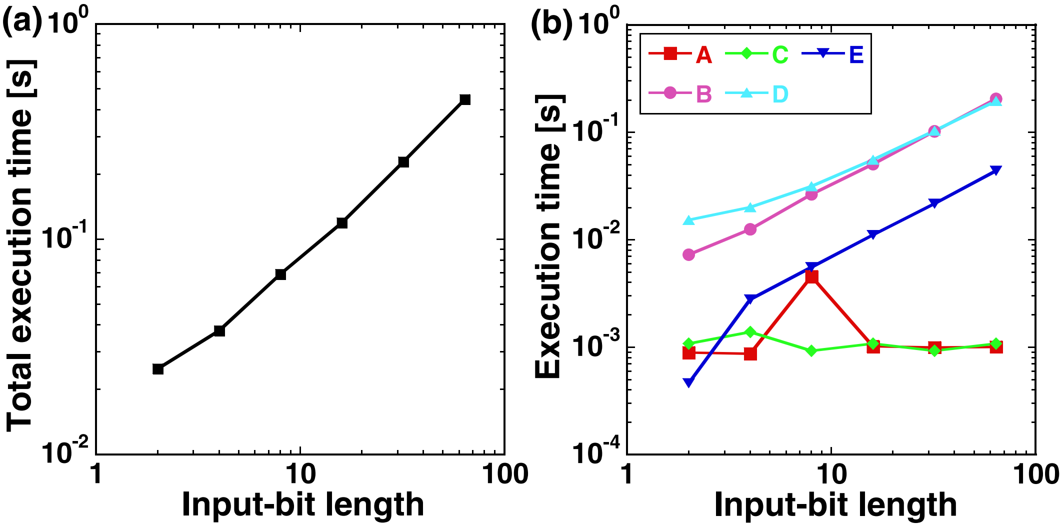

Figure 5. (**a**) Total execution time of secure comparison with garbled circuit for different input-bit lengths of 2-bit to 64-bit. (**b**) Execution time of each procedure for secure comparison. A (red squares): construction of logic circuit, B (pink circles): construction of garbled circuit, C (green diamonds): construction of Alice's garbled input, D (light blue triangles): construction of Bob's garbled input via oblivious transfer, and E (dark blue inverted triangles): execution of garbled circuit.

time to generate the observation parameter-bit pairs required for oblivious transfer of 64 input labels for 64-bit computation can be estimated as 0.058 sec, which is smaller than the oblivious transfer procedure time (0.2 sec).

Discussion

Here we discuss a number of features of the implementation of oblivious transfer and its possible future extensions.

The raw parameter-bit-pair generation rate has an upper limit depending on the parameter switching rate. The parameter switching rate is limited by the transient time of synchronization of the laser outputs after the parameter values are switched. For the lasers used in the experiment, the transient synchronization time is several tens of nanoseconds. The transient time could be reduced by using lasers with shorter external cavity length such as photonic integrated devices[50, 51].

The raw parameter-bit-pair generation rate is comparable with a recent information-theoretic oblivious transfer system based on a quantum scheme[30]. In addition, this oblivious transfer scheme has an advantage of the capability of long optical fiber transmission over hundreds of kilometers, much longer than quantum-based oblivious transfer[30]. It has been reported that no significant degradation of the statistical properties of the optical correlated randomness due to the propagation and amplification operations was observed in an experiment over 120 km of optical fiber with optical amplifiers[36, 37]. This fact indicates that the scheme of optical correlated randomness is feasible for stable operation of oblivious transfer over long distances in large-scale optical fiber networks, which is a practical important advantage over other techniques.

We consider the effect of robust sampling and bit error on the oblivious transfer rate. In the experiment errors were not detected due to the use of robust sampling. If we allow for a message to be resent with new keys when the oblivious transfer fails due to bit error, then it may be feasible to use a less strict robust sampling condition with a higher BER to achieve a higher BGR. The probability of key success for a key of bit-length L, can be estimated as $(1\text{-BER})^L$, and the effective key rate can be estimated as BGR × 0.5 × $(1\text{-BER})^L$, where 0.5 is parameter-match rate. For example, if the key length is 100 bits, the BGR is 1 Mb/s, and BER is 10^{-4}, then the effective key rate is 495 kb/s, which is significantly larger than the value of 110 kb/s reported above for the case analyzed in Table 1.

Next, we consider the effective of bit bias. In the experiment statistically-significant bit bias was not observed. If there was a significant bias, the technique of privacy amplification[48, 49] could be used to generate information-theoretic secure keys with arbitrarily small bit bias. In the Methods section we explain a method of privacy amplification for oblivious transfer and also provide an estimate of the corresponding key generation rate.

Privacy amplification is also essential for achieving security against physical attacks by malicious users that have physical (technological) limits. The experiment in this paper corresponds to the basic case where we assume that Alice and Bob are semi-honest, in the sense that they obey the protocol and do not act maliciously by using other physical measurements to obtain more information about the system that would allow them to know the other user's bits after the parameter exchange. As mentioned earlier, by using privacy amplification, the oblivious transfer can be made information-theoretic secure against a malicious attacker that obtains partial information. It is not necessary to prevent the attacker from obtaining some information or to know which information they obtain. It is only necessary to estimate an upper bound on the amount of information they can obtain.

We consider two types of physical attacks by malicious users. First, an attacker may make multiple simultaneous observations, using multiple devices with different parameter settings (known as "multiple observation attack"[45] or "sampling attack"[43]). To prevent this attack, the number of possible parameter settings needs to be increased so that it exceeds the upper estimate of the number of receiver devices that the malicious user can operate simultaneously. In fact, it is effective to increase the number of the laser stages in the cascaded laser system, because the malicious user needs to increase exponentially the number of his/her cascaded laser systems to perform the perfect multiple observation attack[37] (See the supplementary material for details).

For the second attack, an attacker may reproduce the drive signal after the parameter exchange (known as "replay attack"). To prevent this attack, the bandwidth of the drive signal needs to be increased so that it exceeds the upper estimate of the length of signal that can be recorded by the user for replay after the parameter exchange. In the case of an attack using optical memory, the users can prevent this attack by delaying the parameter exchange longer than the propagation time or decay time of the signal in the optical memory. In the case of heterodyne detection, the attacker would need to record the modulation of the optical drive signal at least within the principal frequency band of the response laser[52, 53]. A successful attack by a malicious user against the laser used in this experiment would require an extremely advanced digitizer and data streaming system able to capture at least 10 GHz of modulation bandwidth[54]. In addition, a method has been proposed to increase the principal frequency band up to much broader bandwidths[52] and this is a challenging area for future theoretical and experimental innovation in laser dynamics.

Finally, we note that as our example implementation of secure computation, we used the Yao's garbled circuit which is based on computational security, rather than information-theoretic security. We note that the fundamental security assumptions of information-theoretic oblivious transfer and computational garbled circuit are different, and a complete implementation of information-theoretic secure computation is an important goal for the future. The scheme proposed by Kolesnikov *et al.* significantly reduces the computational cost of information-theoretic secure computation[55], so this scheme could be feasible if the circuit size is not too large. We consider that this method would be a good candidate for future complete implementation of information-theoretic secure two-party computation.

Conclusion

We demonstrate physical implementation of information-theoretic secure oblivious transfer based on bounded observability with optical correlated randomness. The implementation is realized using semiconductor lasers driven by common random signals broadcast over optical fiber. We experimentally demonstrated oblivious transfer at the effective key generation rate of 110 kb/s for the fundamental case of semi-honest users with a single binary-valued observation parameter and discussed the potential for realizing security against physical observation attacks by malicious users. This scheme is a promising approach to achieve information-theoretic secure oblivious transfer over long distances for future applications of secure computation such as privacy-preserving database mining, auctions and electronic-voting.

Methods

Experimental setup for oblivious transfer.

The experimental setup of the optical correlated random system based on optical fiber components for oblivious transfer is shown in Fig. 6. We use three semiconductor lasers. The lasers are single-mode distributed-feedback (DFB) lasers (NTT Electronics, NLK1C5GAAA, the optical wavelength of 1547 nm) with external optical injection and optical feedback[36, 37]. One laser is used for a common drive signal (called Drive laser) and the other lasers are used for Response lasers. Each legitimate user (Alice or Bob) has a Response laser (called Response 1 and 2 lasers). The injection currents are set to 30.00 mA (2.84 I_{th}), 12.30 mA (1.31 I_{th}), and 12.68 mA (1.34 I_{th}) for the Drive, Response 1, and 2 lasers, respectively, so that the relaxation oscillation frequencies of the Response lasers are as similar as possible, where I_{th} is the injection current at the lasing threshold. The relaxation oscillation frequencies are 5.8, 1.8, and, 1.8 GHz for the Drive, Response 1, and 2 lasers, respectively.

The Response 1 and 2 lasers are subject to a common random drive signal. We use a phase modulator (PM), which is driven by the output of a super-luminescent diode as an optical noise source to generate constant-amplitude and random-phase (CARP) light for the Drive light[38]. The CARP light is divided into two beams at a fiber coupler (FC) and each of the CARP beams is attenuated by an optical attenuator (ATT) to adjust the injection strength. The CARP beams are unidirectionally injected to Response 1 and 2 lasers though optical isolators (ISO). A tracking procedure is required to adjust for the slow variation of the timing offset between the waveform and the sampling clock.

Each of the Response 1 and 2 lasers is subject to optical feedback from a fiber mirror reflector (Ref) forming an external cavity. The external cavity lengths are set to 3.68 m (one-way) for both the Response 1 and 2 lasers, and the corresponding feedback delay time (roundtrip) is 35.4 ns. Precise matching of the external cavity lengths is required to achieve high-quality synchronization between the Response 1 and 2 lasers. The phase of the optical feedback light from each Response laser is shifted by a phase modulator (PM) with a random binary waveform, generated with an arbitrary waveform generator (AWG), with the binary values '0' and '1', corresponding to no and π-phase shift, respectively. Note that each Response laser has an independent phase modulator with random sequences of 0 and 1 generated independently from other chaotic semiconductor lasers[33, 34]. The output of each of the two Response lasers is detected by a photodiode (PD) (New Focus, 1554-B, 12 GHz bandwidth), amplified by an electric amplifier (Amp) (New Focus, 1422-LF, 20 GHz bandwidth), and observed by a digital oscilloscope (Tektronix, DPO71604B, 16 GHz bandwidth, 50 GigaSamples/s) and an RF spectrum analyzer (Agilent, N9010A, 26.5 GHz bandwidth).

We set the optical wavelengths of the Drive and Response lasers by adjusting the temperature of the lasers. Optical injection locking between the Drive and Response lasers is required for common-signal-induced synchronization. It is important to satisfy the following two conditions for oblivious transfer: The correlation between the intensities of the drive and response laser outputs is always low, and the correlation between the intensities of

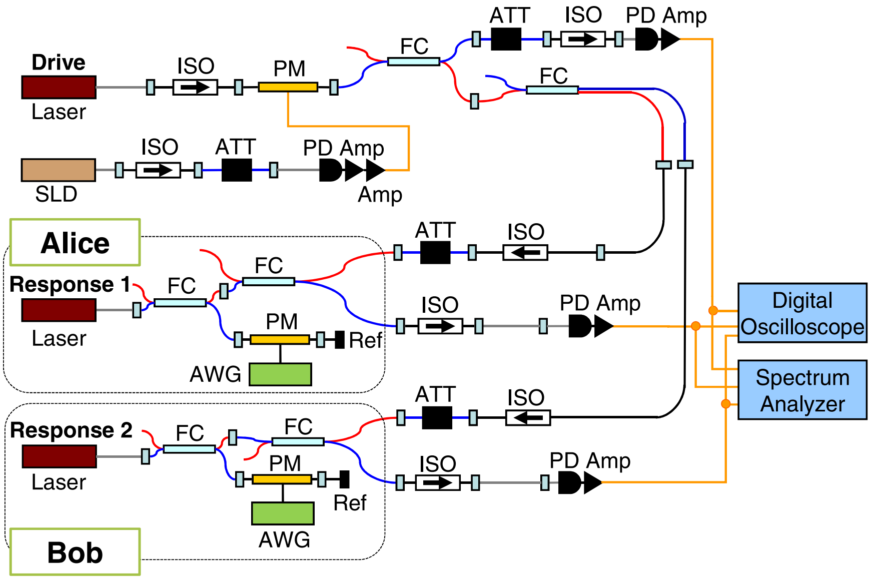

Figure 6. Experimental implementation of optical correlated random system based on optical fiber components for oblivious transfer. Amp: electronic amplifier, ATT: optical attenuator, AWG: arbitrary waveform generator, FC: fiber coupler, ISO: optical isolator, PD: photodetector, PM: phase modulator, Ref: fiber mirror reflector, SLD: super-luminescent diode.

the two response lasers is high when the phase-shift parameter is the same, and low when the phase-shift parameter is different. The former condition is to prevent Bob from estimating the intensity waveform of Alice from the intensity waveform of the common driving light.

Privacy amplification and information reconciliation for oblivious transfer. We explain a method of privacy amplification for oblivious transfer to ensure security with respect to non-ideal probabilities, noise errors or attacks. We also estimate the reduction of the key generation rate by additional procedures, such as privacy amplification and information reconciliation.

In the protocol of oblivious transfer, Alice creates two sequences $\boldsymbol{x}_{A,0}$ and $\boldsymbol{x}_{A,1}$, using observed bits x_A(t) corresponding to the parameter matches $v_A(t) = c_B(t)$ and $v_A(t) = c_B(t) + 1$ respectively. That is, for the sequence $\boldsymbol{x}_{A,0}$, Alice uses the bits $x_A(t)$ observed at times t when $v_A(t) = c_B(t)$, and for the sequence $\boldsymbol{x}_{A,1}$, Alice uses the bits $x_A(t)$ observed at times t when $v_A(t) = c_B(t) + 1$. Then Alice employs the following information reconciliation[56] and privacy amplification[48, 49]. To this end, Alice and Bob share two parity check matrices S_0, S_1 and hashing matrices K_0, K_1 in advance, and Alice calculates following four vectors

$$\boldsymbol{s}_{A,0} = S_0\boldsymbol{x}_{A,0} \tag{2}$$

$$\boldsymbol{s}_{A,1} = S_1\boldsymbol{x}_{A,1} \tag{3}$$

$$\boldsymbol{k}_{A,0} = K_0\boldsymbol{x}_{A,0} \tag{4}$$

$$\boldsymbol{k}_{A,1} = K_1\boldsymbol{x}_{A,1}, \tag{5}$$

where $\boldsymbol{k}_{A,0}$ and $\boldsymbol{k}_{A,1}$ corresponds to two cryptographic keys. Alice encrypts the message M_0 with the key $\boldsymbol{k}_{A,0}$ and the message M_1 with the key $\boldsymbol{k}_{A,1}$, and sends her original parameter set $\{v_A(t)\}^m{}_{t=1}$, two parity check vectors $\boldsymbol{s}_{A,0}$, $\boldsymbol{s}_{A,1}$, and the two encrypted messages to Bob. Finally, Bob obtains a vector $\boldsymbol{x}_{B,b}$ by using the bits $x_B(t)$ for the sampling time t such that $v_B(t) = v_A(t)$, reproduces a vector $\boldsymbol{y}_{B,b}$ by using the relation $S\boldsymbol{y}_{B,b} = \boldsymbol{s}_b$ and $\boldsymbol{x}_{B,b}$, and creates a key as $\boldsymbol{k}_{B,b} = K_0\boldsymbol{y}_{B,b}$, where $b = 0$ or 1 is the value Bob initially decided. Bob's key will be identical to Alice's key $\boldsymbol{k}_{A,b}$ when $\boldsymbol{x}_{A,b} = \boldsymbol{y}_{B,b}$ is satisfied, that is, errors between the bits $x_A(t)$ and $x_A(t)$ for the sampling time t such that $v_B(t) = v_A(t)$ are corrected. Thus Bob is able to decode the message M_b that he intended but not the other message, and Alice does not know which of the two messages Bob can decode. It should be noted that the bias of the frequencies of 0's and 1's in Alice's observed bits $\{x_A(t)\}^m{}_{t=1}$ and the leakage of information of her bits from that of Bob's observed bits $\{x_B(t)\}^m{}_{t=1}$ are eliminated. Following refs 45, 57 and 58, the key generation rate R can be obtained as

$$R = (1/2)(\mathrm{H}(X_{A,b+1}|X_{B,b}) - \mathrm{H}(X_{A,b}|X_{B,b})), \tag{6}$$

where the factor 1/2 corresponds to the probability of the parameter match, $X_{A,b}$ and $X_{B,b}$ denote random variables corresponding to the sample sequences $\boldsymbol{x}_{A,b}$ and $\boldsymbol{x}_{B,b}$, and $\mathrm{H}(X\,|Y)$ represents the entropy of X conditioned on Y.

Secure comparison using Yao's garbled circuit. We implement a multibit secure comparator with a garbled circuit. The detailed protocol of Yao's garbled circuit is shown in the supplementary material. Alice generates the garbled circuit as follows. Alice assigns two randomly generated 100-bit strings (labels) to each wire in the circuit: one for Boolean 0 and one for 1. The random bit strings were generated using a physical random number generator, realized with a semiconductor laser[33, 34]. Next, for each gate in the circuit Alice replaces 0 and 1 in the truth tables with the corresponding 100-bit labels. She then encrypts each output of each truth table with the corresponding two input labels. The Advanced Encryption Standard (AES)[59] block cipher is used for the encryption, and a 28-bit check string (all zeros) is added to each input and output label to test for correct decryption. Given two particular input strings at a gate, only one of the 4 output strings can be decrypted using the input labels as keys. After encrypting the table, Alice randomly permutes the table such that no one can learn the output value based on row position. Alice and Bob use oblivious transfer for each 64-bit input to obtain Bob's garbled input.

In the case of n-bit secure comparison, the number of input bits is n for each user Alice and Bob. The number of gates and wires are given by $5n$-5 and $7n$-5, respectively ($n \geq 2$), so for $n = 64$, the number of gates is 315 and the number of the wires is 443. Assigning 100-bit physical random numbers to each wire of the gates for 0 and 1 requires 88,600 random bits.

The emulation of the Yao's garbled circuit protocol including the one-out-of-two oblivious transfer protocol is executed on a computer with a Intel(R) Core(TM) i7-4770 CPU and 8.2 GB RAM with Windows 7 Professional 64-bit operating system.

References

1. Hazay, C. & Lindell, Y. *Efficient Secure Two-Party Protocols: Techniques and Constructions*. Springer-Verlag, Berlin Heidelberg (2010).
2. Schneider, T. *Engineering Secure Two-Party Computation Protocols, Design, Optimization, and Applications of Efficient Secure Function Evaluation*. Springer-Verlag, Berlin Heidelberg (2012).
3. Damgård, I., Geisler, M. & Krøigård, M. Homomorphic encryption and secure comparison, *Int. J. Applied Cryptography* **1**, 22–31 (2008).
4. Gentry, C. Fully homomorphic encryption using ideal lattices, *Proceedings of 41st ACM Symposium on Theory of Computing (STOC 2009)*, 169–178 (2009).
5. Brakerski, Z., Gentry, C. & Vaikuntanathan, V. Fully homomorphic encryption without bootstrapping, *Innovations in Theoretical Computer Science (ITCS* 2012*), ACM*, 309–325 (2012).
6. Brakerski, Z. & Vaikuntanathan, V. Efficient fully homomorphic encryption from (standard) LWE, *Foundations of Computer Science (FOCS 2011), IEEE*, 97–106 (2011).
7. Yao, A. C. How to generate and exchange secrets. *Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS 1986)*, 162–167 (1986).
8. Malkhi, D., Nisan, N., Pinkas, B. & Sella, Y. Fairplay - A secure two-party computation system. *Proceedings of the 13th conference on USENIX Security Symposium (SSYM 2004)*, 287–302 (2004).
9. Huang, Y., Evans, D., Katz, J. & Malka, L. Faster secure two-party computation using garbled circuits. *Proceedings of the 20th conference on USENIX Security Symposium* (2011).
10. Kolesnikov, V. & Schneider, T. Improved garbled circuit: Free XOR gates and applications. *Proceedings of the 35th international colloquium on Automata, Languages and Proglamming (ICALP 2008), Part II*, 486–498 (2008).
11. Henecka, W., Kogl, S., Sadeghi, A.-R., Schneider, T. & Wehrenberg, I. TASTY: Tool for automating secure two-party computations. *ACM Conference on Computer and Communications Security (CCS 2010)*, 451–462 (2010).
12. Pinkas, B., Schneider, T., Smart, N. P. & Williams, S. C. Secure two-party computation is practical. *Proceedings of ASIACRYPT 2009, Lecture Notes Comput. Sci.* **5912**, 250–267 (2009).
13. Kolesnikov, V. & Mohassel, P. FleXOR: Flexible garbling for XOR gates that beats free-XOR. *Proceedings of CRYPTO 2014, Part II, Lecture Notes Comput. Sci.* **8617**, 440–457 (2014).
14. Zahur, S., Rosulek, M. & Evans, D. Two halves make a whole: Reducing data transfer in garbled circuits using half gates. *Proceedings of EUROCRYPT 2015, Part II, Lecture Notes Comput. Sci.* **9057**, 220–250 (2015).
15. Kempka, C., Kikuchi, R., Kiyoshima, S. & Suzuki, K. Garbling scheme for formulas with constant size of garbled gates. *Proceedings of ASIACRYPT 2015, Part I, Lecture Notes Comput. Sci.* **9452**, 758–782 (2015).
16. Rabin, M. O. How to exchange secrets with oblivious transfer. *Technical Report TR-81*, Aiken Computation Lab, Harvard University (1981).
17. Even, S., Goldreich, O. & Lempel, A. A randomized protocol for signing contracts. *Communications of the ACM* **28**, 637–647 (1985).
18. Naor, M. & Pinkas, B. Efficient oblivious transfer protocols. *Proceedings of the 12th ACM-SIAM Symposium on Discrete Algorithms* (SODA'01), 448–457 (2001).
19. Naor, M. & Pinkas, B. Computationally secure oblivious transfer. *Journal of Cryptology* **18**, 1–35 (2005).
20. Ishai, Y., Kilian, J., Nissim, K. & Petrank, E. Extending oblivious transfers efficiently. *Proceedings of CRYPTO 2003, Lecture Notes Comput. Sci.* **2729**, 145–161 (2003).
21. Crépeau, C. & Killan, J. Achieving oblivious transfer using weakened security assumptions, *Proceedings of the 29th Annual Symposium on Foundations of Computer Science (FOCS 1988)*, 42–52 (1988).
22. Damgård, I., Fehr, S., Morozov, K. & Salvail, L. Unfair noisy channels and oblivious transfer. *Proceedings of Theory of Cryptography Conference (TCC 2004)*, *Lecture Notes Comput. Sci.* **2951**, 355–373 (2004).
23. Wullschleger, J. Oblivious transfer from weak noisy channels. *Proceedings of Theory of Cryptography Conference (TCC 2009), Lecture Notes Comput. Sci.* **5444**, 332–349 (2009).
24. Isaka, M. Oblivious transfer from the additive white Gaussian noise channel. *IEICE Trans. Fundamentals* **E93A**, 516–525 (2010).
25. Cachin, C., Crépeau, C. & Marcil, J. Oblivious transfer with a memory-bounded receiver. *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS 1998)*, 168–173 (1998).
26. Ravi, J., Dey, B. K. & Viterbo, E. Oblivious transfer over wireless channels. *IEEE Transactions on Communications* **64**, 893–905 (2016).
27. Crépeau, C. Quantum oblivious transfer. *Journal of Modern Optics* **41**, 2445–2454 (1994).
28. Fattal, D., Fiorentino, M., Chefles, A. & Beausoleil, R. G. Experimental realization of quantum oblivious transfer. *Conference on Lasers and Electro-Optics and the Quantum Electronics and Laser Science 2008 (CLEO/QELS 2008)* QFB4 (2008).

29. Wehner, S., Curty, M., Schaffner, C. & Lo, H.-K. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A* **81**, 052336 (2010).
30. Erven, C. *et al*. An experimental implementation of oblivious transfer in the noisy storage model. *Nat. Commun.* **5**, 3418 (2014).
31. Palmieri, P. & Pereira, O. Building oblivious transfer on channel delays. *Proceedings of Inscrypt 2010. Lecture Notes Comput. Sci.* **6584**, 125–138 (2010).
32. Palmieri, P. & Pereira, O. Unconditionally secure oblivious transfer from real network behavior. *Proceedings of Advances in Information and Computer Security - 8th International Workshop on Security (IWSEC 2013). Lecture Notes Comput. Sci.* **8231**, 168–182 (2013).
33. Uchida, A. *et al*. Fast physical random bit generation with chaotic semiconductor lasers. *Nat. Photon.* **2**, 728–732 (2008).
34. Akizawa, Y. *et al*. Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 8 × 50 Gb/s. *IEEE Photon. Tech. Lett.* **24**, 1042–1044 (2012).
35. Uchida, A. *Optical Communication with Chaotic Lasers, Applications of Nonlinear Dynamics and Synchronization*. Wiley-VCH, Weinheim (2012).
36. Yoshimura, K. *et al*. A. Secure key distribution using correlated randomness in lasers driven by common random light. *Phys. Rev. Lett.* **108**, 070602 (2012).
37. Koizumi, H. *et al*. Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers. *Opt. Express* **21**, 17869–17893 (2013).
38. Aida, H. *et al*. Experiment on synchronization of semiconductor lasers by common injection of constant-amplitude random-phase light. *Opt. Express* **20**, 11813–11829 (2012).
39. Soriano, M. C., García-Ojalvo, J., Mirasso, C. R. & Fischer, I. Complex photonics: Dynamics and applications of delay-coupled semiconductors lasers. *Rev. Mod. Phys.* **85**, 421–470 (2013).
40. Zhou, B. B. & Roy, R. Isochronal synchrony and bidirectional communication with delay-coupled nonlinear oscillators. *Phys. Rev. E* **75**, 026205 (2007).
41. Brunner, D., Soriano, M. C., Mirasso, C. R. & Fischer, I. Parallel photonic information processing at gigabyte per second data rates using transient states. *Nat. Commun.* **4**, 1364 (2013).
42. Maurer, U. M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **39**, 733–742 (1993).
43. Muramatsu, J., Yoshimura, K., Arai, K. & Davis, P. Secret key capacity for optimally correlated sources under sampling attack. *IEEE Trans. Inf. Theory* **52**, 5140–5151 (2006).
44. Muramatsu, J., Yoshimura, K. & Davis, P. Information theoretic security based on bounded observability. *Lecture Notes Comput. Sci.* **5973**, 128–139 (2010).
45. Muramatsu, J., Yoshimura, K., Davis, P., Uchida, A. & Harayama, T. Secret-key distribution based on bounded observability. *Proceedings of the IEEE* **103**, 1762–1780 (2015).
46. Peil, M., Heil, T., Fischer, I. & Elsäßer, W. Synchronization of chaotic semiconductor laser systems: a vectorial coupling-dependent scenario. *Phys. Rev. Lett.* **88**, 174101 (2002).
47. Rukhin, A. *et al*. National Institute of Standards and Technology, Special Publication 800-22, Revision 1a (2010).
48. Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41**, 1915–1923 (1995).
49. Brassard, G., Crépeau, C. & Wolf, S. Oblivious transfer and privacy amplification. *Journal of Cryptology* **16**, 219–237 (2003).
50. Argyris, A., Deligiannidis, S., Pikasis, E., Bogris, A. & Syvridis, D. Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit. *Opt. Express* **18**, 18763–18768 (2010).
51. Harayama, T. *et al*. A. Fast nondeterministic random-bit generation using on-chip chaos lasers. *Phys. Rev. A* **83**, 031803(R) (2011).
52. Yoshimura, K., Inubushi, M. & Uchida, A. Principal frequency band of cascaded single-mode semiconductor lasers injected with broadband random light, *Proceedings of the 2015 International Symposium on Nonlinear Theory and Its Applications (NOLTA2015)* 257–260 (2015).
53. Suzuki, N. *et al*. Common-signal-induced synchronization in semiconductor lasers with broadband optical noise signal. *IEEE Journal of Selected Topics in Quantum Electronics* **23**, 1800810 (2017).
54. Fontaine, N. K. *et al*. Real-time full-field arbitrary optical waveform measurement. *Nat. Photon.* **4**, 248–254 (2010).
55. Kolesnikov, V. Gate evaluation secret sharing and secure one-round two-party computation. *Proceedings of ASIACRYPT 2005, Lecture Notes Comput. Sci.* **3788**, 136–155 (2005).
56. Brassard, G. & Salvali, L. Secret-key reconciliation by public discussion, *Proceedings of EUROCRYPT 1993, Lecture Notes Comput. Sci.* **765**, 411–423 (1993).
57. Muramatsu, J. Secret-key agreement from correlated source outputs using low density parity check matrices, *IEICE Trans. Fundam.* **E89-A**, 2036–2046 (2006).
58. Muramatsu, J. & Miyake, S. Uniform random number generation and secret key agreement for general sources by using sparse matrices, *Mathematical Modelling for Next-Generation Cryptography*, Springer, Singapore, 177–198 (2017).
59. National Institute of Standards and Technology, *Announcing the Advanced Encryption Standard (AES)*. (2001).

Acknowledgements

A.U. acknowledges support from Grants-in-Aid for Scientific Research from Japan Society for the Promotion of Science (JSPS KAKENHI Grant Number JP16H03878), and Management Expenses Grants from the Ministry of Education, Culture, Sports, Science and Technology in Japan. T.K. acknowledges support in part from JSPS Grant-in-Aids for Scientific Research (A) JP16H01705 and Scientific Research (B) JP17H01695.

Author Contributions

A.U. directed the project. H.K., A.U., J.M., and K.Y. designed the oblivious transfer protocol. T.I., H.K., K.I, and A.U. implemented the oblivious transfer. T.I., N.S. and I.K. conducted the optical experiments. T.I., A.U., and T.K. emulated the secure computation. T.I., H.K., A.U., and P.D. analyzed the data. T.I., A.U., T.K., J.M., K.Y., M.I, and P.D. wrote the paper.

Additional Information

Supplementary information accompanies this paper at doi:10.1038/s41598-017-08229-x

Competing Interests: The authors declare that they have no competing interests.

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