PHYSICAL REVIEW E **71**, 045202(R) (2005)

Encryption with synchronized time-delayed systems

Won-Ho Kye, Muhan Choi, and Chil-Min Kim
National Creative Research Initiative Center for Controlling Optical Chaos, Pai-Chai University, Daejeon 302-735, Korea

Young-Jai Park
Department of Physics, Sogang University, Seoul 121-742, Korea

(Received 12 August 2004; revised manuscript received 26 October 2004; published 15 April 2005)

We propose a new communication scheme that uses time-delayed chaotic systems with delay time modulation. In this method, the transmitter encodes a message as an additional modulation of the delay time and then the receiver decodes the message by tracking the delay time. We demonstrate our communication scheme in a system of coupled logistic maps. Also we discuss the error of the transferred message due to an external noise and present its correction method.

DOI: 10.1103/PhysRevE.71.045202 PACS number(s): 05.45.Xt

The fact that a chaotic system, which intrinsically posseses unpredictability and a broad band spectrum, can be synchronized [1–3] has led people to assume that a chaotic system would provide better security in communication than other cryptographic schemes previously proposed. Since the first demonstration of its possibility in an electronic circuit [4], chaos communication has been extensively investigated and correspondingly various methods for masking the message have been developed [5]. It was shown, however, that the message, when masked by a chaotic signal from a low-dimensional chaotic system, can be extracted [6]. Further, it was reported that even when the message is masked by a hyperchaotic signal, it can be extracted by using nonlinear dynamic forecasting as far as the local dynamics does not reflect more complicated dynamics significantly [7].

A cure for the weakness of the conventional chaos communication was to develop methods using synchronization of time-delayed systems [8–13]. Despite the small number of physical degrees of freedom, the time-delayed system has the advantage of possessing the property of high-dimensional hyperchaos which can be easily implemented electronically [9]. This made the communication using time-delayed systems attract much attention [9,10]. However, it was again reported that delay time τ can be also detected by analyzing the transmitted signal and that in such a case the reconstructed phase space of the time-delayed system collapses into low-dimensional manifold [14]. On this discovery, it was demonstrated that the message masked by the signal of time-delayed system can be extracted even in the presence of message signal of small amplitude [15]. So far almost all of the methods proposed for chaos communication have been broken by their successive counter examples. This fact has spurred a debate on the general assumptions on a chaotic system.

Meanwhile, a time-delayed system with delay time modulation (DTM) in which the delay time is driven by chaotic or stochastic signal for the purpose of making the delay time undetectable was introduced [16]. It was analyzed that a phase space reconstruction is hardly possible in that case [17] because DTM significantly increases the complexity of an attractor and it renders the delay time undeterminable. The report that robust synchronization can be established between two coupled chaotic systems with DTM calls attention to a time-delayed system with DTM as an ideal candidate for communication. In the synchronization with DTM, the system consists of two parties. One is a transmitter, which is a time-delayed system with delay time modulation

$$\dot{x} = f(x(t),x(t-\tau)), \quad \tau = g(x(t),t), \tag{1}$$

where $g(x(t),t)$ is the modulation function. The other is a receiver which is a time-delayed system driven by the signal $x(t-\tau)$ from the transmitter:

$$\dot{x}' = f(x'(t),x(t-\tau)). \tag{2}$$

Even though the modulation works only at the transmitter side, it has been found that the receiver is synchronized with the transmitter by the signal $x(t-\tau)$ [16].

In this paper, we propose a communication method that hides a message into the delay time of time-delayed systems with DTM. In our method the transmitter encodes the message as an additional modulation of the delay time by which we overcome the drawbacks in the previous schemes. The receiver decodes the message by identifying the modulated delay time with a delay buffer.

First, we shall describe the proposed scheme conceptually and demonstrate it in two coupled logistic maps. The transmitter is given by

$$\dot{x} = f(x,x(t-\tilde{\tau})), \quad \tau = g(x), \quad \tilde{\tau} = \tau + m(t), \tag{3}$$

where we call τ the bare delay time which is modulated by the function $g(x)$ and $\tilde{\tau}$ the genuine delay time which includes the message $m(t)$. Here we start by supposing that the $g(x)$ depends only on the state variable x, and that $g(x)$ is announced in public. Even if random people know $g(x)$, they can not get bare delay time τ because for that they also need to know the synchronized state variable x. Now we consider the case that the transmitter and receiver are already synchronized after some transient time. For communication, the transmitter sends $x^* \equiv x(t-\tilde{\tau})$ which includes the encoded message. We emphasize here that our encoding method is fundamentally different from the previous ones. Up to now, in the conventional methods [5] the encoding of the message was usually done by perturbing the real trajectory of the chaotic signal such that $\overline{x}=x+m$. Accordingly, the message could be extracted by identifying the fluctuations of the reconstructed trajectory on phase space or return map [7]. Moreover, because the message plays a role of effective noise which degrades the quality of synchronization, the system should have fast relaxation to the attractor to keep the communication quality, which potentially increases vulnerability [5,6]. On the other hand, in our scheme, the message is encoded as a modulation of the delay time such that $\overline{x}=x(t-(\tau+m))$ which is just the temporal shifting of the original trajectory depending on the message m. Therefore the amplitude of a message needs not to be small. Furthermore, since the delay time including the message changes the genuine characteristics of the attractor such as the embedding dimension and the complexity through the modulation of the delay time [17], the message is constituted into the attractor itself rather than a perturbation.

To decode the message, the receiver should preserve the history of its own trajectory for the time interval $[t-\tau_m,t]$ in the delay buffer which is denoted by the symbol $\{x'[i]\}_{t-\tau_m}^{t}$, where $\tau_m=\max\,\tau(t)$, $i\in[0,N]$. Here $N=[\tau_m/\delta t]$ where δt is a sampling step, and $[x]$ is the largest integer less than x. For tracking the delay time, the receiver defines the delay identification measure:

$$M(i,\epsilon)=\epsilon-|x^{*}-\{x'[i]\}_{t-\tau_m}^{t}|, \tag{4}$$

where ϵ is the predefined threshold for the identification and $|\cdots|$ is the absolute value. The receiver can find the value of $\tilde{\tau}$ by finding the index i^{*}, which maximizes the delay identification measure such that $M(i^{*},\epsilon)\geqslant M(i,\epsilon)$ for $i\in[0,N-1]$. Accordingly, the two delay times, i.e., bare and genuine delay times, can be obtained following the procedure

$$\dot{x}'=f(x',x(t-\tilde{\tau})),\quad \tau'=g(x'),\quad \tilde{\tau}'=\frac{i^{*}}{N}\tau_m, \tag{5}$$

and then the message hidden in the delay time can be decoded at the receiver side such that $m'(t)=\tilde{\tau}'-\tau'$. Since we have supposed that, the two systems in our scheme are synchronized, the state variables and the delay times are coincided with each other, i.e., $x=x'$, $\tau=\tau'$, and $\tilde{\tau}=\tilde{\tau}'$. Thus the decoded message at the receiver side $m'(t)$ is equal to the original message $m(t)$.

In conventional schemes, since the message is encoded as a deviation from the synchronized trajectory, the encoded message can be partly decoded through the synchronized windows in such cases as a different system is located on the intermittently synchronized phase. However, in our scheme, even if a different system is located on the intermittently synchronized phase, the message is completely unknown, because the message is not a deviation from the synchronization manifold. Another strength of this scheme is that the delay time is represented by the integer even if one uses a chaotic flow for transmitter and receiver, because delay time is actually an indicator of a position of the previous state. For that reason, digital data can be directly encoded and decoded in this scheme.

For demonstration, we consider two logistic maps

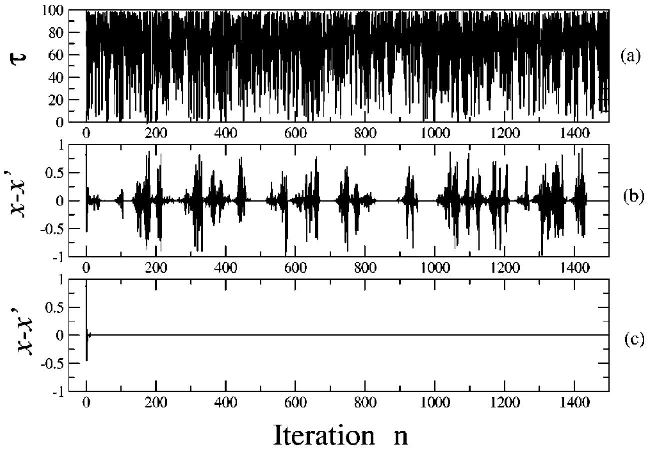

FIG. 1. Temporal behaviors of the coupled systems in Eqs. (6) and (7), when $\Lambda=100$. (a) The modulated delay time. The difference of two state variables: $x-x'$ (b) below the threshold $\alpha=0.28$ and (c) above the threshold $\alpha=0.33$.

$$\left.\begin{array}{l} x_{n+1}=\lambda\overline{x_n}(1-\overline{x_n}),\\ \tau=[\Lambda x_n],\\ \tilde{\tau}=\tau+m \bmod \tau_m, \end{array}\right\}\text{ transmitter}, \tag{6}$$

where we take $g(x)=[\Lambda x]$ and

$$\left.\begin{array}{l} x'_{n+1}=\lambda\overline{x'_n}(1-\overline{x'_n}),\\ \tau'=[\Lambda x'_n],\\ \tilde{\tau}'=i^{*},\\ m'=\tilde{\tau}'-\tau' \bmod \tau_m, \end{array}\right\}\text{ receiver}, \tag{7}$$

where $\overline{x_n}=(1-\alpha)x_n+\alpha x_{n-\tilde{\tau}}$ and $\overline{x'_n}=(1-\alpha)x'_n+\alpha x_{n-\tilde{\tau}}$ and we take $\lambda=4.0$. Here $i\in[0,\tau_m-1]$ and i^{*} is the identified index which maximizes the delay identification measure [Eq. (4)]. Figure 1 shows the temporal behaviors of the two coupled systems with a null message, i.e., $m=0$. While the difference $x-x'$ between the two state variables shows the intermittent chaotic bursting below the synchronization threshold [Fig.

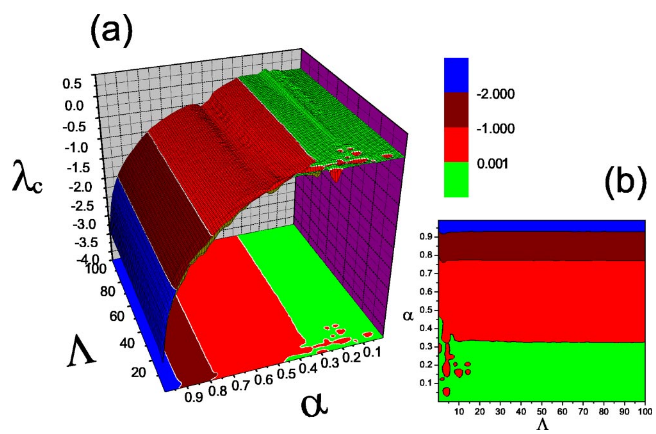

FIG. 2. (Color online) (a) The conditional Lyapunov exponent λ_c as a function of Λ and α. (b) The contour plot in the (Λ,α) space. Here the colors indicate the different values of λ_c.

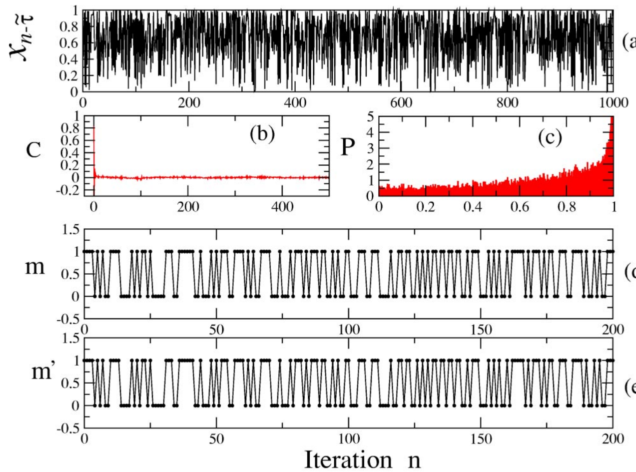

FIG. 3. (Color online) (a) The transmitted signal including the message m at $\alpha=0.7$, $\Lambda=100$, and $\epsilon=10^{-8}$. (b) The autocorrelation of the transmitted signal, which shows δ function shape. (c) The probability distribution function of the transmitted signal $x_{n-\tilde{\tau}}$. (d) The original message at transmitter side. (e) The decoded message at receiver side.

1(b)], it converges fast to the synchronization manifold $x-x'=0$ above the threshold [Fig. 1(c)].

To analyze the critical behaviors of the two coupled chaotic systems we find the difference motion such that $\Delta X_{n+1}=\lambda(1-\alpha)\mathbf{(}1-(\overline{x_n}+\overline{x_n'})\mathbf{)}\Delta X_n$, where $\Delta X_n=x_n-x_n'$. The conditional Lyapunov λ_c, which determines the synchronization threshold, can be found by following the standard procedure: $\lambda_c=\lim_{n\to\infty}(1/n)\ln|\Delta X_n/\Delta X_0|$.

Figure 2 shows conditional Lyapunov exponent as a function of coupling strength α and modulation amplitude Λ. One sees that the conditional Lyapunov exponent becomes negative above $\alpha=0.32$ for all $\Lambda\in[3,100]$ and it means two coupled systems are synchronized in that regime. On the other hand, if the modulation amplitude is relatively small, i.e., $\Lambda<3$, synchronization is established in the stronger coupling, i.e., $\alpha>0.48$ and some synchronization islands appear in the regime $\Lambda\in[3,18]$ and $\alpha\leqslant 0.32$ [see the contour plot in Fig. 2(b)].

Figure 3 shows the temporal behavior and statistical properties of the transmitted signal with an example of the message transfer. The transmitted signal $x_{n-\tilde{\tau}}$ is shown in Fig. 3(a) and the autocorrelation function of the signal is presented in Fig. 3(b). Figure 3(c) shows the probability distribution function P of the transmitted signal $x_{n-\tilde{\tau}}$, which is a normalized histogram of the projected trajectory onto the $x_{n-\tilde{\tau}}$ axis in n versus $x_{n-\tilde{\tau}}$ plot [Fig. 3(a)]. Since the autocorrelation function is δ-correlated, one can see that the system looks random to an eavesdropper. Figure 3(d) is the original message encoded at the transmitter and (e) is the message decoded at the receiver. Consideration of the effects of noise in the transmission channel is essential in regard to real application and implementation.

The noise in the transmission channel ξ_n induces the distortion at receiver side such that $\hat{x}^*=x^*+\xi_n$, $\hat{x}_n'=x_n'+O(\alpha\xi_n)$. The distortion is propagated into the delay identification measure such that $\hat{M}(i,\epsilon)=\epsilon-|\hat{x}^*-\{\hat{x}'[i]\}_{n-\tau_m}^{n}|$. So the possibility exists that the identified index i^* can be determined incorrectly due to the external noise. Figure 4 shows how the external noise has an effect on the message transfer in our scheme. The original message is presented in Fig. 4(a) and the decoded messages with different values of the threshold ϵ for delay time identification are presented in Figs. 4(b)–4(d). One can see that the transferred bits are intermittently flipped as shown in Figs. 4(c) and 4(d) (see the arrows).

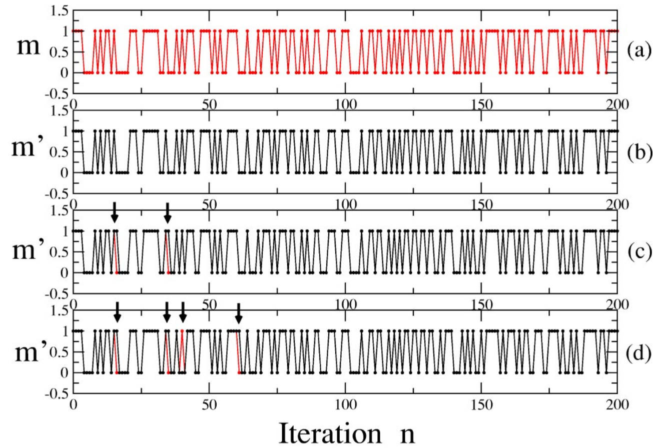

FIG. 4. (Color online) The decoded messages for different values of the threshold ϵ in the presence of noise of $\max(\xi_n)=10^{-6}$. (a) The original message. (b) The decoded message with $\epsilon=2.5\times10^{-5}$. (c) With $\epsilon=2.0\times10^{-5}$. (d) With $\epsilon=1.5\times10^{-5}$. The arrows in (c) and (d) indicate the bit-flipped events in the decoded message.

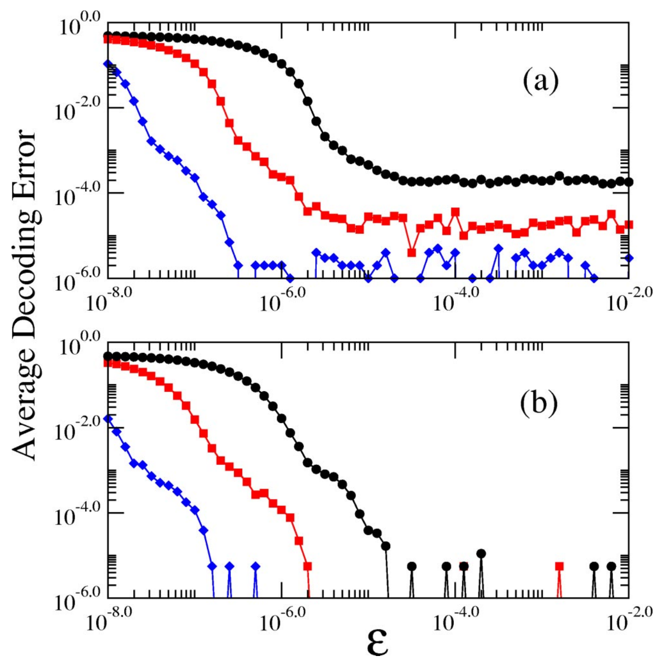

FIG. 5. (Color online) The average decoding errors for different noise amplitudes as a function of the threshold ϵ, where the points below $10^{-6.0}$ are zero. Each datum point is the result of 10^6 bit transfer. Circles: $\max(\xi)=10^{-6}$; squares: $\max(\xi)=10^{-7}$; diamonds: $\max(\xi)=10^{-8}$.
(a) Without the error correction. (b) With the error correction (see Ref. [18]).

To clarify the role of the noise ξ_n in our scheme and the relationship with the threshold ϵ, we evaluate the average decoding error, which is defined by the number of flipped bits divided by the total number of transferred bits. Figure 5(a) shows the decoding error as a function of the threshold ϵ in the presence of external noise. The decoding error is decreased as the threshold is increased. Figure 5(b) shows the data on the application of the error correction method [18]. With the proper threshold, the receiver can decode the message completely even in the presence of external noise.

It is worth discussing the possibility of eavesdropping for the proposed scheme. The eavesdropper can accumulate the transmitted signal $x(t-\tilde{\tau})$, which is the temporally shuffled signal of the synchronized state variable $x(t)$. Accordingly the eavesdropper can not reconstruct the phase space correctly [17], because the information of the phase space is preserved only when the temporal ordering of the signal is kept. Even if one succeeds in reconstructing the phase space, the message is not separable as mentioned above. For the eavesdropper to identify the genuine delay time $\tilde{\tau}$, the construction of the delay buffer is the most essential procedure. The eavesdropper, however, always gets the fake delay buffer $\{\tilde{x}[i]\}_{t-\tau_m}^{t}$ in which the temporal order is mixed. Accordingly the eavesdropper reads the incorrect genuine delay time $\tilde{\tau}$ from it. Furthermore, since the synchronized state variable x is never exposed outside the transmitter or the receiver in our scheme, the eavesdropper cannot find the bare delay time τ also, which is the function of synchronized state variable x.

In conclusion, we have proposed a communication scheme which enables one to encode and decode the desired message using the time-delayed system in the presence of delay time modulation. Our scheme is fundamentally different from the conventional ones in that, in our scheme, since the message is encoded as a modulation of the delay time [Eq. (3)], it does not degrade the quality of the synchronization. The transferred message is decoded just by comparing the transmitted signal with the history of the trajectory stored in the delay buffer [Eqs. (4) and (5)]. We have demonstrated the proposed scheme in coupled simple maps and we have also shown that the scheme works even in the presence of external noise just with a simple algorithm for the error correction. We expect our scheme can be used to implement the real communication system with better performance and enhanced security.

This work is supported by Creative Research Initiatives of the Korean Ministry of Science and Technology.

[1] H. Fujisaka and T. Yamada, Prog. Theor. Phys. **69**, 32 (1983); V. S. Afraimovich, N. N. Verichev, and M. I. Rabinovich, Radiophys. Quantum Electron. **29**, 747 (1986); L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).

[2] S. Boccaletti, J. Kurth, G. Osipov, D. L. Valladares, and C. Zhou, Phys. Rep. **366**, 1 (2002).

[3] A. Pikovsky, M. Rosenblum, and J. Kurths, *Synchronization: a universal concept in nonlinear science* (Cambridge University Press, Cambridge, 2001).

[4] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

[5] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995); J. H. Peng, E. J. Ding, M. Ding, and W. Yang, *ibid.* **76**, 904 (1996); J. H. Xiao, G. Hu, and Z. Qu, *ibid.* **77**, 2818 (1996); S. Boccaletti, A. Farini, and F. T. Arecchi, Phys. Rev. E **55**, 4979 (1997); K. Murali and M. Lakshmanan, *ibid.* **56**, 251 (1997); Z. Liu, S. Chen, and B. Hu, *ibid.* **59**, 2817 (1999); S. Sundar and A. A. Minai, Phys. Rev. Lett. **85**, 5456 (2000); C.-M. Kim, S. Rim, and W.-H. Kye, *ibid.* **88**, 014103 (2002); S. Wang, J. Kuang, J. Li, Y. Luo, H. Lu, and G. Hu, Phys. Rev. E **66**, 065202 (2002); R. Mislovaty, E. Klein, I. Kanter, and W. Kinzel, Phys. Rev. Lett. **91**, 118701 (2003).

[6] G. Pérez and H. A. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).

[7] K. M. Short and A. T. Parker, Phys. Rev. E **58**, 1159 (1998); D.-U. Hwang, C.-M. Kim, and Y.-J. Park, J. Korean Phys. Soc. **42**, 8 (2003).

[8] K. Pyragas, Phys. Rev. E **58**, 3067 (1998); R. He and P. G. Vaidya, *ibid.* **59**, 4048 (1999).

[9] B. Mensour and A. Longtin, Phys. Lett. A **244**, 59 (1998).

[10] J.-P. Goedgebuer, L. Larger, and Henri Porte, Phys. Rev. Lett. **80**, 2249 (1998); L. Yaowen, G. Gguangming, Z. Hong, and W. Yinghai, Phys. Rev. E **62**, 7898 (2000); V. S. Udaltsov, J.-P. Goedgebuer, L. Larger, and W. T. Rhodes, Phys. Rev. Lett. **86**, 1892 (2001).

[11] J. K. Hale, *Theory of Functional Differential Equations* (Springer-Verlag, Berlin, 1997), and references therein.

[12] T. Heil, I. Fischer, W. Elsässer, J. Mulet, and C. R. Mirasso, Phys. Rev. Lett. **86**, 795 (2001).

[13] J. Fort and V. Méndez, Phys. Rev. Lett. **89**, 178101 (2002).

[14] R. Hegger, M. J. Bünner, H. Kantz, and A. Giaquinta, Phys. Rev. Lett. **81**, 558 (1998).

[15] C. Zhou and C.-H. Lai, Phys. Rev. E **60**, 320 (1999); B. P. Bezruchko, A. S. Karavaev, V. I. Ponomarenko, and M. D. Prokhorov, *ibid.* **64**, 056216 (2001); V. I. Ponomarenko and M. D. Prokhorov, *ibid.* **66**, 026215 (2002).

[16] W.-H. Kye, M. Choi, M.-W. Kim, S.-Y. Lee, S. Rim, C.-M. Kim, and Y.-J. Park, Phys. Lett. A **322**, 338 (2004).

[17] W.-H. Kye, M. Choi, S. Rim, M. S. Kurdoglyan, C.-M. Kim, and Y.-J. Park, Phys. Rev. E **69**, 055202(R) (2004).

[18] We have introduced a redundancy of the transferred data. At the transmitter, a bit is represented by five duplicated bits. At the receiver, the bit is read as the value that is duplicated more than two times.