The Novel Rapid Long PN Sequence Acquisition Method Based on Correlation Property*

Hong Wen, Suling Wang, Liang Zhou, Shumin Luo, Zhongpei Zhang

National Key Lab of Communication of University Electronic Science and Technology of China, Chengdu 610054, China
E-mail: sunlike@uestc.edu.cn

*This work is supported by the National Natural Science Foundation of China under Grant No. 60496313

where E_c is the signal energy per chip, $y_t(\boldsymbol{u})$ is the t-th output of the LFSR with initial state $\boldsymbol{u}$ and n_t is additive white Gaussian noise (AWGN) with zero mean and variance $N_0/2$. The model in (2) can be written in vector form as

$$\boldsymbol{Z} = \sqrt{E_c}\boldsymbol{Y}(\boldsymbol{u}) + \boldsymbol{n} \tag{3}$$

where $\boldsymbol{n} = (n_0, n_1, \cdots, n_{M-1})^T$ is a Gaussian vector with zero mean and covariance matrix $N_0/2\mathbf{I}_M$, where $\mathbf{I}_M$ is $M \times M$ the identity matrix.

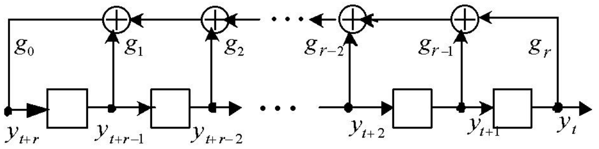

Fig.1. The generator diagram for an r-stage LFSR

III. ACQUISTION METHODS

Though the fast correlation attacks algorithm is an efficient stream cipher attacking algorithm, we can also view it as a decoding algorithm. The system model of fast correlation attacks acquisition is shown in Fig.2. We regard LFSR sequence $\boldsymbol{Y}(\boldsymbol{u})$ as input and Z as the corresponding channel output of $\boldsymbol{Y}(\boldsymbol{u})$. At the receiver, fast correlation attack algorithm is employed to obtain $\boldsymbol{Y}(\boldsymbol{u})$ and hence it recovers the initial state of LFSR.

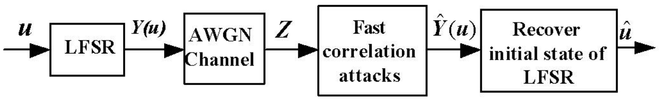

Fig.2. System model

For the purpose of reconstructing the LFSR-sequence $\boldsymbol{Y}(\boldsymbol{u})$ from Z, the following principle[4] is essential to the algorithms: Every digit $y_t(\boldsymbol{u})$ of $\boldsymbol{Y}(\boldsymbol{u})$ satisfies several linear equations derived from the basic feedback relations, all of them involving l other digits of $\boldsymbol{Y}(\boldsymbol{u})$ if there are $l+1$ nonzero coefficients in $g(x)$. By substituting the corresponding digits of Z in these relations, we obtain a group of equations for each digit z_t, which may either hold or not hold. To test whether $z_t = y_t(\boldsymbol{u})$, we count the number of all equations that turn out to hold for z_t. Then the more of these equations hold, the higher the probability is for z_t to agree with $y_t(\boldsymbol{u})$. This can be justified by a statistical model, computing the corresponding conditional probabilities.

By iterating squaring of the generation polynomial, a variety of linear relations is generated for every digit $y_t(\boldsymbol{u})$. The average number M_n of relations obtained in this way can be computed as:

$$M_n = \log(M/2r) \times (l+1) \tag{4}$$

To give a more precise description we list the algorithm for BSC as follows:

Step 1: Determine M_n according to (4).

Step 2: Find the value of $h = h_{\max}$ such that $I(p, M_n, h)$ is maximum, where

$$\begin{aligned} I(p, M_n, h) = &\sum_{i=0}^{h} C_{M_n}^{i} (1-p)(1-S)^i S^{M_n - i} \\ &- \sum_{i=0}^{h} C_{M_n}^{i} pS^i (1-S)^{M_n - i} \end{aligned} . \tag{5}$$

And $S = S(p,t)$ can be computed using the recursion

$$\begin{cases} S(p,t) = pS(p,t-1) + (1-p)(1-S(p,t-1)) \\ S(p,1) = p \end{cases} \tag{6}$$

In (5), p is correlation probability which determined by BSC channel transition probability p_{ec} as:

$$p = 1 - p_{ec}, \tag{7}$$

Step 3: Initialize the iteration counter $i = 0$.

Step 4: For every digit of $\boldsymbol{Z}$ calculate a new probability p^* for $z_t = y_t(\boldsymbol{u})$, given that h of M_n relations are satisfied.

$$p^* = pS^h(1-S)^{M_n - h} / (pS^h(1-S)^{M_n - h} + (1-p)(1-S)^h S^{M_n - h}) \tag{8}$$

Step 5: Calculate the thresholds P_{thr} and N_{thr}, where

$$\begin{cases} P_{thr} = \left(p^*(p, M_n, h_{\max} + 1) + p^*(p, M_n, h_{\max})\right)/2 \\ N_{thr} = U(p, M_n, h_{\max}) \times N \end{cases} \tag{9}$$

where $U(p, M_n, h)$ is the probability that a digit z_t satisfies at most h of M_n relations,

$$U(p, M_n, h) = \sum_{i=0}^{h} C_{M_n}^{i} \left(pS^i(1-S)^{M_n - i} + (1-p)(1-S)^i S^{M_n - i}\right) \tag{10}$$

Step 6: Determine the number of positions N_w with $p^* < P_{thr}$. If $N_w < N_{thr}$ or $i < \alpha$, increase i and go to step 4.

Step 7: Make complement for those binary digits of Z with $p^* < P_{thr}$ and reset the probability of each digit to the original value p.

Step 8: If there exists digit of Z not satisfying the feedback relation then go to step 3.

Step 9: Terminate with $\boldsymbol{Y}(\boldsymbol{u}) = \boldsymbol{Z}$.

IV. SIMULATION RESULTS

To evaluate the performance of our schemes, we have performed some simulations and compared the results of our approach with other three search methods over AWGN channel. We consider the m-sequence generated by an

15-stage LFSR with $g(y)=1+y+y^{15}$. The threshold for serial searches is determined using method in [1].

We do simulations with length M=256, M=512 and M=1024 respectively. As illustrated in Fig.3, when M=256, FCAA with 20 iterations provides approximately 0.4 dB degradation. From Fig.4 the improvement in E_c/N_0 for the FCAA to min-sum iMPA is about 0.5 dB when M=512 with 20 iterations, and more than 1 dB with 50 iterations. As observed in Fig. 5, when M=1024, FCAA with 20 iterations provides more than 0.5 dB improvement to min-sum iMPAs and about 0.8 dB with 50 iterations. It is reasonable to conclude that the length is longer, the performance of FCAA is better

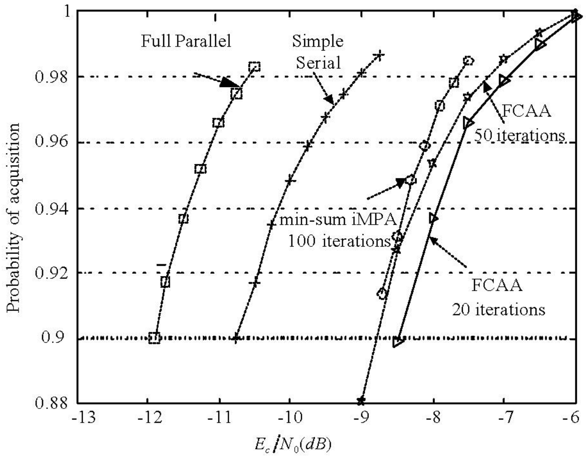

Fig.3. Comparison of acquisition performances of various approaches with $M=256$ total observations

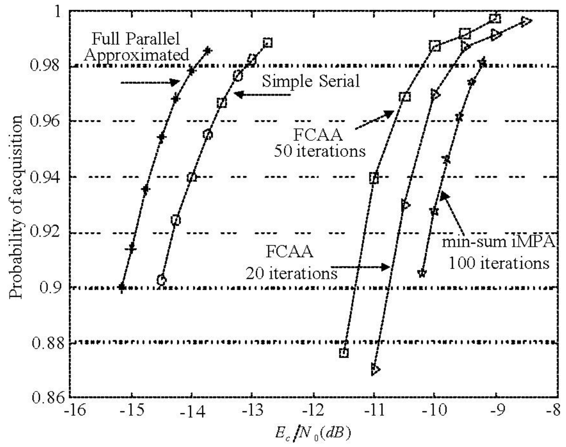

Fig.4. Comparison of acquisition performances of various approaches with $M=512$ total observations

V. CONCLUSIONS

In this paper, we have proposed a new approach for rapid pseudorandom long sequence acquisition using the method that is similar as fast correlation attacks. Simulation results show that new method performs close to that of iMPAs search method. Compared with full parallel and serial search, this approach also provides significant complexity reduction. Specifically our method suits not only for linear sequence acquisition, but also for nonlinear sequence acquisition. Furthermore our approach needs not to extract effective cyclic graphical models as in iMPAs search method.

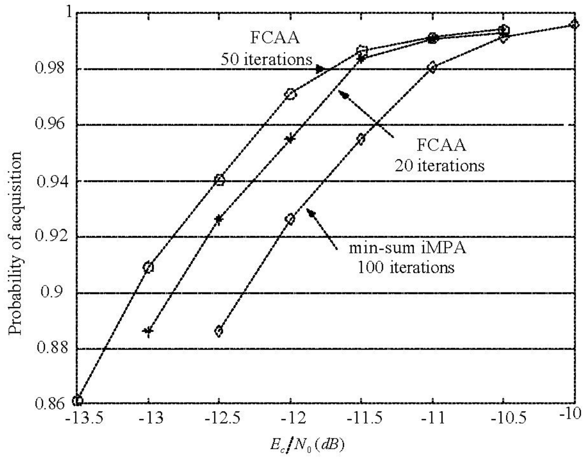

Fig.5. Comparison of acquisition performances of FCAA approaches with $M=1024$ total observations

REFERENCES

[1] A.Polydoros and C. L. Weber, "A unified approach to serial search spread-spectrum code acquisition", *IEEE Trans. Commun.*, vol.32, NO.5, pp. 542-560, May 1984.

[2] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, Spread Spectrum Communications Handbook. New York: McGraw-Hill, 1994.

[3] M. Zhu and K. M. Chugg, "A new approach to rapid PN code acquisition using iterative message passing techniques", *IEEE journal on selected areas in communications*, vol.23, NO.5, pp. 884-897, May 2005.

[4] W. Meier, and O. Staffelbach, "Fast correlation attacks on certain stream ciphers", *Journal of Cryptology*, vol.1, 1989, pp. 159-176.

[5] Yang Li-zhen, Fu Xiao-tong, Xiao Guo-zhen and Chen Ke-fei, "Research on Correlation attacks on a nonlinear generator", Journal of Xidian University, Vol.28, No.5, pp. 566-568, Oct.2001.