LFSR-Based Signatures with Message Recovery

Xiangxue Li, Dong Zheng, and Kefei Chen
(Corresponding author: Xiangxue Li)

Department of Computer Science and Engineering, Shanghai Jiaotong University
Shanghai, 200030, China. (Email: xxli@sjtu.edu.cn)

(Received Nov. 14, 2005; revised and accepted Dec. 16, 2005)

Abstract

In order to reduce key sizes and bandwidth, several LFSR-based (linear feedback shift register) public key cryptosystems and signature schemes have been proposed. Digital signatures with message recovery are useful for many applications in which small messages (*e.g.*, 100 bits or so) should be signed. This paper first presents a new sequence operation, called DSO, based on existing sequence operations, and then proposes a LFSR-based signature scheme with message recovery and a LFSR-based signature scheme with partial message recovery. We support the proposed schemes with security analysis. Our schemes take the advantage that they require less computation complexity, less representation and less bandwidth than those required in their counterparts based on finite fields of $\mathbb{Z}_q$.

Keywords: Characteristic sequence, digital signature, discrete logarithm problem, linear feedback shift register sequence, message recovery

1 Introduction

With the rapid development of information security, nowadays cryptosystems are more important than those in previous eras. To Design an efficient and secure cryptosystems has become a very challenging task for researchers in order to meet the requirements of communication bandwidth, information rate, computational speed, and various security strategies. The finite-field based public-key cryptosystems, such as ElGamal cryptosystems [3], DSS [10], and RSA [14], require that the field sizes must be chosen large enough to strengthen their security. But this affects the efficiency of the schemes because the time to do the underlying operations grows (and rather quickly) as the security parameter increases. For applications where bandwidth is limited, we prefer to avoid this. Recently, several cryptosystems have been proposed to successfully reduce the representation of the elements of the finite fields with the coefficients of their minimal polynomials [4, 8, 9, 16]. For instance, Niederreiter [9] has proposed encryption and key agreement schemes based on general n-th order LFSR sequences. Giuliani and Gong [4] proposed a general class of LFSR-based key agreement and signature schemes based on n-th order characteristic sequences. These schemes have the advantage that they do not require as much bandwidth as their counterparts based on finite fields.

Digital signatures with message recovery are useful for many applications in which small messages (*e.g.*, 100 bits or so) should be signed [11, 13]. For example, small messages including time, date and identifiers are signed in certified email services and time stamping services. In these situations, it is desirable to minimize the total length of the original messages and the appended signatures. To date, there are many research work along this line. In [2], Bellare and Rogway gave a RSA-based signing scheme PSS-R which provides message recovery, and further extended to provide schemes for Rabin signatures with analogous properties. In [1], Abe and Okamoto showed a signature scheme with message recovery in the DL-type (*i.e.*, elliptic curve based). In [18], Zhang *et.al.* proposed an identity based message recovery signature scheme.

In this paper, we first derive a new sequence operation, called DSO(*D*erived *S*equence *O*peration), and then propose a LFSR-based signature scheme with message recovery which can be viewed as LFSR-based version of existing work [1, 18]. The resulting scheme is very simple and efficient, since it only requires 1 SO1 operation in the signing algorithm. Another appealing advantage is that the resulting signature is only 2-tuple in Z_P^2. Its limitation is that the size of the message to be signed is limited to fixed length. To eliminate such flaw, we extend the scheme to a LFSR-based signature scheme with partial message recovery. In this case, the signer can sign arbitrary messages of any bit-length. We also support the schemes with security analysis.

The paper will proceed as follows. After some preliminary work, Section 3 will describe a new sequence operation DSO based on existing operations SO1 and SO2. Section 4 will present our LFSR-based signature scheme with message recovery. We will give its security analysis in Section 5. Section 6 will extend the scheme in Section 4 to the scenario where the message to be signed can be of any bit-length. The paper will end with some concluding

remarks.

2 Preliminaries

2.1 LFSR Sequences

Let q be a prime or a power of prime, $f(x) = x^d - a_1 x^{d-1} + a_2 x^{d-2} - \ldots + (-1)^d a_d, a_i \in GF(q)$ be an irreducible polynomial over $GF(q)$, and let α be a root of $f(x)$ in the extension $GF(q^d)$.

A sequence $s = \{s_k\}$ over $GF(q)$ is said to be a LFSR sequence generated by $f(x)$ if $s_{k+d} = a_1 s_{k+d-1} - a_2 s_{k+d-2} + \ldots + (-1)^{d+1} a_d s_k$ for all $k \geq 0$, where $a_1, \ldots, a_d$ are elements of $GF(q)$. If an initial state of $s = \{s_k\}$ is given by $s_k = tr(\alpha^k), k = 0, 1, \ldots, d-1$, where $tr(\cdot)$ is the trace map from $GF(q^d)$ to $GF(q)$, then $\{s_k\}$ is called a *d-th* order characteristic sequence. Let the periodic of s_k be P, we may define $s_k = s_{P+k}$ for all $k \leq 0$, thus we can consider the sequence $\{s_k\}$ with indices running over all integers. We denote $\bar{s}_i = (s_i, s_{i+1}, \ldots, s_{i+d-1})$ the *i-th* state of the LFSR sequence, and define the set $A_k = (s_k, s_{2k}, \ldots, s_{rk})$, where r is defined by

$$r = \begin{cases} d-1 & \text{for general } q \text{ and } d, \\ d/2 & \text{if } q = p^2, \text{and } d \text{ is even}, \\ (d-1)/2 & \text{if } q = p^2 \text{ and } d \text{ is odd}. \end{cases}$$

The set $A_k = (s_k, s_{2k}, \ldots, s_{rk})$ need smaller bits for representation than that in the ordinary case. For mare details, see [4, 6, 7, 9, 17].

2.2 LFSR-based Complexity Problems

There are two main operations in LFSR-based cryptosystems.

Sequence Operation 1(SO1): Given A_k and an integer l , where $0 \leq k, l < P$, compute A_{kl}.

Sequence Operation 2(SO2): Given states $\bar{s}_k$ and $\bar{s}_l$ for some $0 \leq k, l < P$, compute $\bar{s}_{k+l}$.

Both **SO1** and **SO2** can be performed efficiently by existing algorithms [4].

Definition 1. *The LFSR-Based Discrete Logarithm Problem (LFSR-DLP) is, given (q, d, P, A_1, A_l), to find l.*

Definition 2. *The State-Based Discrete Logarithm Problem (S-DLP) is, given $(q, d, P, \bar{s}_1, \bar{s}_l)$, to find l.*

Definition 3. *LFSR-DLP Assumption. We say that the LFSR-DLP problem is (t, ε)-hard if for all t-time adversary $\mathcal{A}$, we have:* $Adv^{LFSR-DLP}(\mathcal{A}) = \Pr[\mathcal{A}(q, d, P, A_1, A_l) = l | 0 \leq l < P] < \varepsilon$.

Definition 4. *S-DLP Assumption. We say that the S-DLP problem is (t, ε)-hard if for all t-time adversary $\mathcal{A}$, we have:* $Adv^{S-DLP}(\mathcal{A}) = \Pr[\mathcal{A}(q, d, P, \bar{s}_1, \bar{s}_l) = l | 0 \leq l < P] < \varepsilon$.

It was proven that the LFSR-DLP and S-DLP are computationally equivalent to the DLP [4].

2.3 Secure Signatures

The strongest notion of security for signature schemes was defined as follows [5].

Secure Signature: A signature scheme $\mathcal{S} =<$ *KeyGen, Sign, Verify* $>$ is existentially unforgeable under an adaptive chosen message attack if it is infeasible for a forger $\mathcal{F}$ who only knows the public key to produce a valid message-signature pair after obtaining polynomially many signatures on messages of its choice from the signer.

More concretely, for any probabilistic polynomial time forger $\mathcal{F}$, there does not exist a non-negligible probability ε such that

$$Adv(\mathcal{F}) = Pr\left[\begin{array}{l} (\mathtt{pk}, \mathtt{sk}) = \mathtt{KeyGen}(1^l), \\ \mathtt{M_i} = \mathcal{F}(\mathtt{pk}, \mathtt{M}_1, \sigma_1, ..., \mathtt{M_{i-1}}, \sigma_{\mathtt{i}-1}), \\ \sigma_\mathtt{i} = \mathtt{Sign}(\mathtt{sk}, \mathtt{M_i})(\mathtt{i} = 1, ..., \mathtt{k}) \\ (\mathtt{M}, \sigma) = \mathcal{F}(\mathtt{pk}, \mathtt{M}_1, \sigma_1, ..., \mathtt{M_i}, \sigma_\mathtt{i}), \\ \mathtt{M} \neq \mathtt{M_i}(\mathtt{i} = 1, ..., \mathtt{k}) \\ \mathtt{Verify}(\mathtt{pk}, \mathtt{M}, \sigma) = \mathtt{accept} \end{array}\right] \geq \varepsilon.$$

Exact Security of Signatures: A forger $\mathcal{F}$ $(t, q_H, q_S, \varepsilon)$-breaks the signature scheme $\mathcal{S} =<$ *KeyGen, Sign, Verify* $>$ under an adaptive chosen message attack if after at most q_H queries to the hash oracle, q_S signature queries to the signature oracle and t processing time, $\mathcal{F}$ outputs a valid forgery with probability at least ε.

2.4 Notations

In this paper, we will use some notations listed as follows.
$|q|$-the length of q in bits;
$[m]^{k_1}$-the most significant k_1 bits of m;
$[m]_{k_2}$-the least significant k_2 bits of m.

3 New Sequence Operation

This section describes a new sequence operation, called **DSO**, which is derived from SO1 and SO2. We believe that combining SO1 and SO2, the new sequence operation can be useful to construct other new LFSR-based cryptographic primitives.

DSO: Given $A_1, \bar{s}_k$, and an integer l, where $0 \leq k, l < P$, compute $\bar{s}_{kl}$.

Theorem 1. *There exists an efficient algorithm that performs the new sequence operation DSO.*

Proof. We show by a constructive method that Theorem 1 holds, *i.e.*, we will construct an efficient algorithm to execute **DSO**. The algorithm is depicted as follows.
Input: $A_1, \bar{s}_k, l, P$ prime.
Output: $\bar{s}_{kl}$.

1) Compute A_{kl} from A_k and l using SO1.
2) For $1 \leq i < d$, compute A_{kl+i} as follows:
   a. compute l^{-1} such that $ll^{-1} = 1 \bmod P$;
   b. compute $\overline{s}_{il^{-1}}$ from A_1 and il^{-1} using SO1;
   c. compute $\overline{s}_{k+il^{-1}}$ from $\overline{s}_k$ and $\overline{s}_{il^{-1}}$ using SO2;
   d. compute $A_{k+il^{-1}}$ from $\overline{s}_{k+il^{-1}}$ using SO2;
   e. compute A_{kl+i} from $A_{k+il^{-1}}$ and l using SO1.
3) Obtain $\overline{s}_{kl} = (s_{kl}, s_{kl+1}, \ldots, s_{kl+d-1})$ from $A_{kl}, A_{kl+1}, \ldots, A_{kl+d-1}$.

Remark: In step 2, we can obtain $\overline{s}_{il^{-1}} = (s_{il^{-1}}, s_{il^{-1}+1}, ..., s_{il^{-1}+d-1})$ due to the fact that we have A_1, il^{-1}, $il^{-1}+1$,..., $il^{-1}+d-1$ and the sequence operation SO1. We can compute $A_{k+il^{-1}} = (s_{k+il^{-1}}, s_{2(k+il^{-1})}, ..., s_{r(k+il^{-1})})$ from $\overline{s}_{k+il^{-1}}$ since we can run the sequence operation SO2 $r-1$ times. □

In the following sections, we will use SO1, SO2, and the new sequence operation DSO to construct LFSR-based signatures with message recovery.

4 LFSR-Based Signature Scheme with Message Recovery

Digital signatures with message recovery are useful for many applications in which small messages (*e.g.*, 100 bits or so) should be signed. For example, small messages including time, date and identifiers are signed in certified email services and time stamping services. In these situations, it is desirable to minimize the total length of the original messages and the appended signatures. To date, there are many research work along this line [1, 2, 11, 13]. Current section presents a LFSR-based signature scheme with message recovery. The proposed scheme is somewhat related to conventional Schnorr signatures [15] and consists of four algorithms Init, KeyGen, Sign, and Verify as depicted below.

Init: Given the security parameter 1^k, the algorithm Init generates the Domain parameters: q, d, P, A_1. Moreover, to produce a signature with message recovery on some k_1-bit message, three hash functions $H : \{0,1\}^* \longrightarrow \{0,1\}^k$, $F_0 : \{0,1\}^{k_1} \longrightarrow \{0,1\}^{k_0}$, $F_1 : \{0,1\}^{k_0} \longrightarrow \{0,1\}^{k_1}$, $k = k_0 + k_1$, are also required.

KeyGen: To obtain his secret key and corresponding public key, a user randomly chooses $\omega (0 \leq \omega < P)$, and computes $\overline{s}_\omega$. The user's key pair is $(\omega, \overline{s}_\omega)$. He keeps ω secret, while $\overline{s}_\omega$ may be made public by the trusted entity CA.

Sign: To sign some message m with his secret key ω, the signer acts as follows. If all these steps are performed successfully, the receiver will obtain a valid signature (h, σ) with message recovery on the message m.

1) Pick randomly a number k $(0 \leq k < P)$;
2) Compute A_k from A_1 and k using SO1;
3) Set $m' = F_0(m) || (F_1(F_0(m)) \bigoplus m)$;
4) Compute $h = H(A_k) + m'$;
5) Set $\sigma = k - h\omega$;
6) Output (h, σ) as the signature with message recovery on the message m.

Note that unlike the standard signatures [4], the resulting signature (h, σ) in our scheme is only a 2-tuple, which is with message recovery, *i.e.*, the message m does not have to be transferred along with the signature (h, σ) as explained in the following algorithm.

As for the computational costs, besides some evaluations of hash functions and simple modular addition, to produce a valid signature only requires 1 sequence operation SO1 [4]. Thus, our signature generation algorithm is really very simple and efficient.

Verify: Upon receiving a signature (h, σ) on some message from the signer with public key $\overline{s}_\omega$, any verifier can perform the following tasks to recover the corresponding message hidden in the signature and check its validity.

1) Compute $\overline{s}_\sigma$ from A_1 and σ using SO1;
2) Compute $\overline{s}_{\omega h}$ from $\overline{s}_\omega$ and h using DSO;
3) Determine $\overline{s}_{\sigma+h\omega}$ from $\overline{s}_\sigma$ and $\overline{s}_{h\omega}$ using SO2;
4) Compute A_k from $\overline{s}_{\sigma+h\omega}$ using SO2;
5) Set $m' = h - H(A_k)$;
6) Parse m' as $m' = [m']^{k_0} || [m']_{k_1}$;
7) Recover the message m as $m = [m']_{k_1} \bigoplus F_1([m']^{k_0})$;
8) Accept the signature (h, σ) and the recovered message m if the following equation holds:$[m']^{k_0} = F_0(m)$; reject otherwise.

This ends the description of our LFSR-based signature scheme with message recovery. The following section will give a simple security analysis.

5 Security Analysis

5.1 Correctness

From SO1, SO2, and DSO, it is straightforward to check that the property of correctness holds.

5.2 Unforgeability

As for the property of unforgeability of the proposed signature scheme with message recovery, we show by the following theorem that it is secure if the *S-DLP* assumption holds. In fact, using the generic technique ID reduction lemma [12], it is possible to construct a formal security reduction for the LFSR-based signature scheme. For brevity, however, we adopt an informal proof that is much easier to understand.

Theorem 2. *If a valid signature of our proposed scheme can be generated without the knowledge of the secret key of the signer, then the S-DLP problem can be solved in polynomial time.*

Proof. Suppose that without the knowledge of the secret key of the signer, any third party $\mathcal{A}$ can successfully construct on the message m^* a valid signature (h^*, σ^*) with message recovery which can pass the verification algorithm. Since m^* is hidden in the value m' and F_0, F_1, H are hash functions whose outputs can be viewed as random numbers, $\mathcal{A}$ must have the capability of computing the value A_k with non-negligible probability in polynomial time. To achieve his goal, $\mathcal{A}$ may have the following two ways.

On the one hand, $\mathcal{A}$ may try to obtain A_k by computing k directly from the equation $k = \sigma + h\omega$ which contains one secret parameter ω only known to the signer, thus the adversary $\mathcal{A}$ cannot produce a valid A_k by this way.

On the other hand, $\mathcal{A}$ may first pick a random k, therefore he can compute A_k, and $\overline{s}_k$. Then the adversary can compute h^* from A_k and m^*. But he cannot determine the value of σ^* from $\overline{s}_{\sigma^*}$ which can be produced from $\overline{s}_k$ and $\overline{s}_{h^*\omega}$, since he faces the difficulty of solving *S-DLP* problem.

Combining all these above, the soundness of the conclusion follows. This completes the proof of Theorem 2. □

6 LFSR-based Signatures with Partial Message Recovery

Section 4 manages to propose a LFSR-based signature scheme with complete message recovery. In that scheme, however, there exists a serious limitation, *i.e.*, the size of the message to be signed is fixed to k_2 bit-length. This means that the scheme cannot deal with the message whose size is larger than k_2, in other words, the scheme cannot sign the messages of arbitrary lengths. To eliminate such limitation, this section will propose a LFSR-based signature scheme with partial message recovery.

The scheme also consists of four algorithms, Init, KeyGen, Sign, and Verify. Thereinto, Init, KeyGen are the same as those in Section 4.

Sign: To sign some message m with his secret key ω, the signer acts as follows.

1) Parse the message m as $m = m_0||m_1$, where m_1 is of k_1 bit-length;
2) Pick randomly a number k ($0 \leq k < P$);
3) Compute A_k from A_1 and k using SO1;
4) Set $m' = F_0(m_1)||(F_1(F_0(m_1)) \bigoplus m_1)$;
5) Compute $h = H(m_0, A_k) + m'$;
6) Set $\sigma = k - h\omega$;
7) Output (m_0, h, σ) as the signature on the message m.

Verify: Upon receiving a signature (m_0, h, σ) on some message, any verifier can perform the following tasks to recover the corresponding message hidden in the signature and check its validity.

1) Compute $\overline{s}_\sigma$ from A_1 and σ using SO1;
2) Compute $\overline{s}_{\omega h}$ from $\overline{s}_\omega$ and h using DSO;
3) Determine $\overline{s}_{\sigma+h\omega}$ from $\overline{s}_\sigma$ and $\overline{s}_{h\omega}$ using SO2;
4) Compute A_k from $\overline{s}_{\sigma+h\omega}$ using SO2;
5) Set $m' = h - H(m_0, A_k)$;
6) Parse m' as $m' = [m']^{k_0}||[m']_{k_1}$;
7) Recover the partial message m_1 as $m_1 = [m']_{k_1} \bigoplus F_1([m']^{k_0})$;
8) Accept the signature (m_0, h, σ) and the recovered message $m = m_0||m_1$ if the following equation holds:$[m']^{k_0} = F_0(m_1)$; reject otherwise.

This ends the descriptions of our LFSR-based signatures with partial message recovery. The proofs of soundness, security analysis are similar to those of LFSR-based signatures with complete message recovery as stated in Section 5. We omit those details here.

7 Conclusions

We have presented a new sequence operation DSO. Combining DSO and existing sequence operations, other new LFSR-based cryptographic primitives can be easily constructed. We then proposed a LFSR-based signature scheme with message recovery and a LFSR-based signature scheme with partial message recovery. We supported the schemes with simple security analysis. The proposed schemes take advantage of the efficiency of computation, representation and bandwidth.

8 Acknowledgement

The authors would like to thank anonymous referees for their valuable suggestions. This work is partially supported by NSFC under the grants 60573030, 60473020 and 60273049.

References

[1] M. Abe, and T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm," *ASIACRYPT 1999*, LNCS 1716, pp. 378-389, Springer-Verlag, 1999.

[2] M. Bellare, and P. Rogaway, "The exact security of digital signatures- How to sign with RSA and Rabin," *Advances in Cryptology - EUROCRYPT 96*, LNCS 1070, pp. 399-416, Springer-Verlag, 1996.

[3] T. ElGamal, "A public key cryptosystems and a signature based on discrete logarithm," *IEEE Transaction on Information Theory*, vol.31, pp. 469-472, 1985.

[4] K. Giulian, and G. Gong, "New LFSR-based cryptosystems and the trace discrete log problem (Trace-DLP)," *Sequences and Their Applications 2004*, LNCS 3486, pp. 298-312, Springer-Verlag, 2005.

[5] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal of computing*, vol. 17, no. 2, pp. 281-308, 1988.

[6] S. Golomb, *Shift Register Sequences*, Laguna Hills, CA: Aegean Park, 1982.

[7] G. Gong, amd L. Harn, "Public-key cryptosystems based on cubic finite field extensions," *IEEE Transaction on Information Theory*, vol. 24, pp. 2601-2605, 1999.

[8] A. Lenstra, and E. Verheul, "The XTR public key system," *CRYPTO 2000*, LNCS 1880, pp. 1-19, Springer-Verlag, 2000.

[9] H. Niederreiter, "Finite fields and cryptology," *Finite Fields, Coding Theory, and Advances in Communications and Computing*, M. Dekker, New York, pp. 359-373, 1993.

[10] NIST, "A proposed federal information processing standard for digital signature standard (DSS)," *Federal Register*, vol. 56, no. 169, pp. 42980-42982, 1991.

[11] K. Nyberg, and A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," *Designs, Codes and Cryptography*, vol. 7, no. 1, pp. 61-81, 1996.

[12] K. Ohta, and T. Okamoto, "On concrete security treatment of signatures derived from identification," *Advances in Cryptology - CRYPTO'98*, LNCS 1462, pp. 354-369, Springer-Verlag, 1998.

[13] J. Piveteau, "New signature scheme with message recovery," *Electronics Letters*, vol. 29, no. 25, pp. 2185, 1993.

[14] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol.21, no.2, pp. 120-126, 1978.

[15] C. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161-174, 1991.

[16] P. Smith, and C. Skinner, "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms," *ASIACRYPT'94*, LNCS 917, pp. 357-364, Springer-Verlag, 1994.

[17] C. Tan, X. Yi, and C. Siew, "On the n-th order shift register based discrete logarithm," *IEICE Transaction on Fundamentals*, vol. E86-A, no. 5, pp. 1213-1216, 2003.

[18] F. Zhang, W. Susilo, and Y. Mu, "Identity-based partial message recovery signatures," *Financial Cryptography 2005*, LNCS 3570, pp. 47-59, Springer-Verlag, 2005.

XiangXue Li is with the Cryptography and Information Security Lab and a PH.D. candidate in the Department of Computer Science and Engineering, Shanghai JiaoTong University. His main research interests include cryptography, provable security, and network security.

Dong Zheng received the Ph.D. degree from Xidian University in 1999. Now, he is an associate professor in Shanghai JiaoTong University. His research interests include provable security and new cryptographic technology.

KeFei Chen was awarded a PH.D degree in Justus-Liebig-University Giessen, German, in 1994. Now, he is a professor and doctor supervisor, deputy director of the School of Information Security, director of the Lab of Cryptography and Information Security, in Shanghai JiaoTong University. He is member of the expert committee of NSFC, of the expert reviewing committee of NSFC, and chair/member of numerous interntional conferences. His main research interests include cryptographic algorithm, information hiding, digital watermarking, wireless security technology,etc.