Efficient Blind Signatures for Accountability

Conference Paper · November 2007

DOI: 10.1109/NPSEC.2007.4371624 · Source: IEEE Xplore

4 authors, including:

Manish Singhal
Bhabha Atomic Research Centre
113 PUBLICATIONS **4,410** CITATIONS

SEE PROFILE

Efficient Blind Signatures for Accountability

Saikat Chakrabarti, Santosh Chandrasekhar, Kenneth L. Calvert and Mukesh Singhal
Laboratory for Advanced Networking, Department of Computer Science, University of Kentucky, Lexington, KY 40506
Email: {saikat,san,calvert}@netlab.uky.edu, singhal@cs.uky.edu

***Abstract*—The problem of building privacy-preserving accountability systems is long-standing and has been extensively studied by the network research community. We observe that blind signatures have potential to form critical building blocks of network security protocols, where an authority needs to vouch for the legitimacy of a message but there is also a need to keep the ownership of the message secret from the authority. Different forms of blind signature constructions exist in the literature and have found valuable use in areas such E-Cash technology and E-voting schemes. However, conventional blind signatures are quite heavyweight and thus, a direct application of these traditional signatures face scalability and performance challenges. In this paper, we present a novel third-order linear feedback shift register (LFSR) sequence-based, 2-party signature scheme, EGCLFSR, following a well-known variant of the generalized ElGamal signature scheme. Using EGCLFSR, and following fundamentals of a well known blind signature, originally used for E-Cash systems, we present an efficient blind signature BCLFSR (also the first blind signature based on LFSR sequences), which can serve as a protocol building block for privacy-preserving accountability systems. We perform a theoretical analysis including correctness and security of BCLFSR and also present a performance (computation and communication costs, storage overhead) comparison of the proposed scheme with a well-known traditional construction.**

***Index Terms*—Accountability, privacy-preserving accountability, ElGamal signature, blind signature, LFSR sequence, cubic LFSR-based cryptosystems, GH, XTR.**

I. Introduction

The current Internet architecture lacks any network-level *accountability* mechanism—that is, a means to reliably identify an entity that can be held accountable for sending a packet. Undesirable consequences of this omission include inability to attribute attacks of various kinds to higher-level users. The ability to attribute packets to a particular source is clearly desirable from the standpoint of punishing those responsible for (and thus deterring future) denial-of-service attacks, for example. This has led to recent interest in adding some form of accountability to the network service [1], [2]. The idea of one proposal [2] is that an "accountability provider" certifies each packet by signing it. The signature can be verified by ISPs along the path from sender to receiver, and ultimately by the receiver.

However, concerns about *privacy* complicate the design of any accountability service: the ability to trace communications at user level could hinder or even prevent deployment of such mechanisms. Users may not be comfortable with the notion that a record of their communications exists, even at the level of IP addresses, and even if it will not be revealed except in the case of wrongdoing. (Certainly this information is regarded as highly sensitive by Internet Service Providers [3].)

Work supported by NSF grants CNS-0626918 and IIS-0324836

The tension between accountability and privacy can be ameliorated to some extent through the use of *blind signatures*. Blind signatures are useful in protocols that require the origin of a message to be certified in some way, but anonymity of the actual originator is desirable. Although blind signature techniques have been known for some time, traditionally they are built from heavyweight cryptographic techniques. This limits their utility for the design of protocols where performance is important—for example, where signatures have to be created on-the-fly, or verified per-packet.

In this paper, we introduce a new blind signature scheme based on the properties of cubic linear-feedback shift registers (LFSRs). The performance properties of the scheme make it more suitable than traditional blind signature schemes for use in performance-sensitive network protocols. We do not claim to have solved the difficult problem of accountability completely; however, we believe our new primitive can be a useful building block for such solutions.

A. Background on Blind Signatures

Blind signatures are a specialized form of digital signatures where the signature generation involves an interactive protocol executed by an entity (the owner) possessing the message and another entity (the signer) possessing a long-term secret key, also known as the signing key. The owner transforms the message into a "blinded" message, and sends it to the signer. The signer uses its signing key, to generate a signature on the blinded message and returns the signature to the owner. The owner makes a transformation on this signature such that (1) the transformed signature is a valid signature on the original message under the long-term public key of the signer and (2) the signer cannot associate the (message, transformed signature) pair with the owner. This transformed signature is known as a blind signature. Different constructions of blind signatures have found valuable use in various areas such as E-Cash technology [4], self-certified public keys [5] and E-voting systems [6].

Blind signatures have potential as key building blocks of network security protocols, where an authority needs to vouch for the legitimacy of a message but there is also a need to keep the ownership of the message secret from the authority.

B. Contributions

In this paper, we present a protocol building block for privacy-preserving accountability systems. Network security

applications are inherently performance sensitive, so a direct application of conventional blind signature constructions would face scalability and performance challenges. To address these issues, we apply primitives from linear feedback shift register (LFSR) sequence-based public key cryptosystems (PKC)s. The proposed blind signature scheme, BCLFSR, can be useful in providing Internet Service Provider (ISP)-level accountability[1], while preserving customer anonymity.

We present a novel cubic (third-order) LFSR-based 2-party signature scheme EGCLFSR using a well-known variant of the generalized ElGamal signature scheme, EG I.3 [7]. We construct the proposed blind signature scheme using EGCLFSR and using fundamentals of a blind signature (also constructed using the EG I.3 variant), originally used in E-Cash systems [4], [8]. We provide a detailed theoretical analysis, including correctness, security and performance, of the proposed blind signature scheme.

C. Why Choose PKCs based on LFSR Sequences

A substantial portion of public key cryptography, for example, the Diffie-Hellman key agreement [9] and the Digital Signature Standard [10], is based on the discrete logarithm assumption on an underlying finite field $\mathbb{F}_q$. However, the chosen field sizes, q, must be sufficiently large to withstand the existing attacks — algorithms to solve the discrete logarithm problem. LFSR-based public key cryptosystems [11], [12], [13] use reduced representations of finite field elements. This enables us to represent finite field elements, say, in the extension field $\mathbb{F}_{q^n}$, by the corresponding minimal polynomials whose co-efficients are chosen from the base field $\mathbb{F}_q$. The security of LFSR-based public key cryptosystems is based on the difficulty of solving the discrete logarithm problem in the extension field $\mathbb{F}_{q^n}$. However, all computations, involving sequence terms, needed for the protocol are performed in the base field $\mathbb{F}_q$. This leads to substantial savings, both in communication and computational overhead, for a desired security level. For example, 170-bits of the XTR (a phonetic acronym for Efficient and Compact Subgroup Trace Representation) PKC, based on third order LFSR sequences, gives security equivalent to 1024-bits of cryptosystems using traditional representation of finite fields [12]. The performance enhancement resulting from such a transformation is shown in Section V-C. We regard 1024-bit security corresponding to traditional finite fields as the current standard and thus, use cubic-LFSR sequences in our protocol constructions.

The rest of the paper is organized as follows. We discuss related work in Section II. We also discuss the cryptographic preliminaries of cubic LFSR sequences and related public key cryptosystems in Section III. We present a useful technique to leverage accountability using efficient blind signatures in Section IV. We perform a theoretical analysis (correctness, security, and performance) of the proposed blind signature schemes in Section V. Section VI concludes the paper.

[1]An ISP is accountable for traffi c originating within any autonomous system (AS) that is supported by the ISP.

II. Related Work

We divide the related work into three sub-areas, namely blind signatures, accountability as a network service, and LFSR PKCs and applications.

A. Blind Signatures

The concept of blind signatures was introduced by Chaum [4]. Camenisch et al. [8] proposed two blind signature schemes, one based on variant of DSA and the other providing message recovery. Horster et al. [14] classified blind signature schemes into parameter hidden, message hidden, weak, interactive and strong blind signatures based on the strength of anonymity provided by the signatures and provided several example constructions based on the generalized ElGamal signature scheme [7]. Later, Horster et al. [6] presented the first blind multisignature scheme and its application in electronic voting. Pointcheval et al. [15] formalized the notion of security for blind signatures in the random oracle model and provided examples of provably secure blind signature schemes. Petersen et al. [5] proposed the use of parameter hidden signatures, to generate self-certified public keys [16].

B. Accountability as a Network Service

A number of network-layer mechanisms have been proposed for identifying sources of malicious packets [17], [18], [19], [1]. Virtually all involve additional operations as part of forwarding. In some schemes, these operations are performed on every packet, while in others they are performed probabilistically, on a small fraction of packets. In some, routers record information about packets forwarded, but in most, routers add to or modify packets in some way to "mark" them. Many of these mechanisms have the property that ability to determine the path followed by a packet is probabilistic; many packets must follow the same path in order for them to be effective. Most also focus on determining the (network-level) source *after* the fact, and at best offer deterrence rather than prevention.

The recent proposal by Bender et al. [2] takes a different approach. They posit a third-party accountability service, which vouches for the legitimacy of its customers. The idea is that transit providers require packets to be signed (using public-key cryptography) by such a service in order to forward them. Packets that are not vouched for may not be forwarded. In case of mischief, the victim can take an offending packet to the accountability server, who can identify the perpetrator.

C. LFSR-PKCs and Applications

The idea of developing a public key cryptosystem based on LFSR sequences was first proposed by Niederreiter, who also presented the encryption and decryption of messages based on nth order LFSR sequences [13]. Gong et al. [11], [20] proposed the GH (Gong-Harn) public key cryptosystem based on third-order LFSR sequences and developed an ElGamal-like digital signature scheme based on the GH-PKC. Lenstra et al. [12] proposed the XTR public key cryptosystem based on cubic LFSR sequences over specialized finite fields. Giuliani

et al. [21] presented a signature scheme using the trace discrete logarithm problem and proved the equivalence between several LFSR-based computational problems and corresponding finite field counterparts.

LFSR sequence-based PKCs have found recent applications in several efficient and scalable network authentication protocols. Chakrabarti et al. proposed first constructions of multisignature schemes, based on cubic LFSR sequences, to authenticate route discovery in the dynamic source routing protocol in mobile ad hoc networks [22] and to authenticate feedback in multicast applications [23]. Li et al. [24] presented LFSR-based signatures with message recovery and Tan et al. [25] used cubic LFSRs to develop two signature schemes equivalent to the Schnorr signature and signed ElGamal encryption schemes.

III. Cryptographic Preliminaries of Cubic LFSR Sequences and Related PKCs

A sequence of elements $\{s_k\} = s_0, s_1, \ldots$ over the finite field $\mathbb{F}_q$ is called a 3rd order homogeneous linear recurring sequence in $\mathbb{F}_q$ if for all $k \geq 0$:

$$s_{k+3} = c_0 s_{k+2} + c_1 s_{k+1} + c_2 s_k \tag{1}$$

where, $c_0, c_1, c_2 \in \mathbb{F}_q$ and s_k denotes the kth term of the sequence $\{s_k\}$. Such sequences can be efficiently generated by a special kind of electronic switching circuit, called LFSR. Consider the following monic irreducible polynomial over $\mathbb{F}_q$:

$$f(x) = x^3 - ax^2 + bx - 1; \quad a, b \in \mathbb{F}_q \tag{2}$$

The sequence $\{s_k\}$ is said to be a cubic-LFSR sequence generated by $f(x)$ if we have $c_0 = a$, $c_1 = b$ and $c_2 = 1$ in Equation 1, i.e., for all $k \geq 0$:

$$s_{k+3} = as_{k+2} - bs_{k+1} + s_k$$

The polynomial $f(x)$ is called the *characteristic polynomial* of the sequence $\{s_k\}$ if, given a root α of $f(x)$, for all $k \geq 0$, we have $s_k = \alpha^k + \alpha^{kq} + \alpha^{kq^2}$, where $\alpha \in \mathbb{F}_{q^3}$. The sequence $\{s_k\}$ is called the third-order *characteristic sequence* generated by $f(x)$ (or by α). The initial state (kth state denoted as $\bar{s}_k = \{s_k, s_{k+1}, s_{k+2}\}$) of the characteristic sequence of $f(x)$ is given by $\bar{s}_0 = \{3, a, a^2 - 2b\}$ [21].

Recently, two PKCs, namely, GH-PKC [11] and XTR-PKC [12] were proposed based on cubic LFSR sequences [26]. In cubic LFSR-based PKCs [11], [12], elements in $\mathbb{F}_{q^3}$ are represented by their corresponding minimal polynomials whose coefficients are chosen from $\mathbb{F}_q$. However, the security of cubic LFSR-based PKCs is based on the difficulty of solving the discrete logarithm problem in $\mathbb{F}_{q^3}$. This leads to substantial savings, both in communication and computational overhead, for a desired security level. In particular, 170-bits of XTR-PKC gives security equivalent to 1024-bits of cryptosystems using traditional representation of finite fields [12]. The XTR cryptosystem is constructed by choosing:

1) p, a large prime of the order of 170 bits. Set $q = p^2$.
2) Q, a large prime factor of $p^2 - p + 1$ of the order of 160 bits.
3) Characteristic polynomial $f(x) = x^3 - ax^2 + a^p x - 1$ with period Q by randomly choosing $a \in \mathbb{F}_q$ and using standard irreducibility testing algorithms.

Let $f_k(x)$ denote the minimal polynomial of α^k where $\alpha \in \mathbb{F}_{q^3}$ is a root of $f(x)$. It can be shown that the polynomial $f_k(x)$ can be represented as [11], [12], [21]: $f_k(x) = x^3 - s_k x^2 + s_k^p x - 1$ in the XTR-PKC. Thus, the polynomial f_k (we drop the indeterminate x for simplicity of notation) can be represented by $s_k \in \mathbb{F}_q$ in XTR. The sequence terms are computed using the following two sequence operations [20]:

- OP_1: Given an integer k and f_e, compute the (ke)th state of the LFSR, $\bar{s}_{ke}$;
- OP_2: Given $\bar{s}_k$ and $\bar{s}_e$ (both integers k, e can be unknown), compute the $(k+e)$th state of the LFSR, $\bar{s}_{k+e}$.

These sequence operations have been efficiently implemented in hardware [27]. We use the sequence operations to create/manipulate sequence terms in the proposed multisignature scheme.

In cubic LFSR-based PKCs, an entity randomly chooses a *long-term private key* $\mathsf{SK} = x$ in $\mathbb{Z}_Q^*$ and computes the *long-term public key* $\mathsf{PK} = \bar{s}_x = \{s_x, s_{x+1}, s_{x+2}\}$ using the sequence operation $\mathsf{OP}_1(x, f)$. Algorithms for sequence term computations use the following *commutative law* [11] for characteristic sequences: for all integers r and e, the r^{th} term of the characteristic sequence generated by the polynomial $f_e(x)$ equals the $(re)^{\text{th}}$ term of the characteristic sequence generated by the polynomial $f(x)$, i.e., $s_r(f_e) = s_{re}(f) = s_e(f_r)$.

We construct our blind signature schemes using the XTR-PKC for simplicity, although the proposed schemes can be seamlessly built using the GH-PKC and also extended to PKCs based on higher order LFSR sequences, with minor modifications.

IV. Privacy-preserving Accountability using Efficient Blind Signatures

We first develop a cubic LFSR-based 2-party signature scheme EGCLFSR using a well-known variant of the generalized ElGamal signature scheme, EG I.3 [7]. We construct the proposed blind signature scheme following EGCLFSR, and using fundamentals of the blind signature (also constructed using the EG I.3 variant), originally used in E-Cash systems [4], [8]. The use of LFSR sequences makes the blind signature scheme a good candidate for performance sensitive network protocols. The proposed blind signature scheme, BCLFSR, can be useful in providing ISP-level accountability while preserving customer anonymity.

A. Basic Idea

In our scheme, a customer within the domain of an ISP blinds a message $m \rightarrow m'$, and presents m', along with the customer's *personal* credentials, to the accountability server of the ISP. The server uses its long-term secret key to generate a signature, σ, on the blinded message, m', and returns σ to the customer. The customer transforms the signature, σ, into a blind signature σ' on the original message m. Given a valid signature σ' on a message m, under the ISP's public

key, the ISP cannot repudiate signing the message. This provides ISP-level accountability. The use of blind signatures preserves message anonymity since the ISP cannot associate the (message, blind signature) pair (m, σ') to a particular customer. The price paid for this feature is that the ISP (or third-party accountability service) must have some other means of determining the originating user when presented with a malicious packet. (One possibility is for the ISP to track closely which of its IP addresses are used by which customers at all times.)

The core of the proposed signature scheme, BCLFSR, consists of an ElGamal-like blind signature. An ElGamal-like signature σ on a message m is a tuple consisting of an ephemeral public key, and a parameter t that is the result of solving an ElGamal-like signing equation [7]. Loosely speaking, the ephemeral public key can be thought of as some randomness for the signature and the parameter t serves as the signature relative to that randomness. Informally, in an ElGamal signature-based blind signature scheme, the customer needs to transform both the ephemeral public key and the parameter t to ensure that the (blinded message, signature) pair, (m', σ) and the (original message, blind signature) pair (m, σ') are statistically independent[2]. This ensures privacy to the customer.

Next, we present a ElGamal I.3-type signature construction based on LFSR sequences.

B. A Variant of a Generalized ElGamal Signature Scheme based on LFSR Sequences

We present the cubic LFSR-based individual signature scheme, EGCLFSR [22] that is constructed using the EG I.3 [7] variant of the generalized ElGamal signature scheme.

Signature Generation	**Signature Verification**
1) Randomly choose ephemeral private key $k \in_R \mathbb{Z}_Q^*$ and compute ephemeral public key $f_k \leftarrow \mathsf{OP}_1(k, f)$. Denote $r = s_k \mod Q$ as an integer. 2) Compute hash of message $h = H(m)$; Solve for t in the following equation: $t \equiv kh - xr \mod Q$. 3) Send the signature $\sigma = \langle f_k, t \rangle$ and the message m to verifier.	1) Compute $h = H(m)$, $v = tr^{-1}$ and $u = hr^{-1}$. 2) Compute $A = f_{(v+x)} \leftarrow \mathsf{OP}_2(v, \bar{s}_x)$. 3) Compute $B = f_{(uk)} \leftarrow \mathsf{OP}_1(u, f_k)$. 4) Accept signature if $A = B$, else reject signature.

Fig. 1. The EGCLFSR two-party signature scheme

The EGCLFSR scheme consists of four phases: initialization, key generation, signature generation and signature verification. During the initialization phase, both entities, i.e., the signer and the verifier, choose and agree on the system public parameters: $\mathsf{params} = \langle p, Q, f(x), H \rangle$, where p, Q and $f(x)$ are as described in Section III and $H : \{0,1\}^* \mapsto \mathbb{Z}_Q$ is a cryptographic hash function. The signer generates its long-term private and public key pair, $(SK, PK) = (x, \bar{s}_x)$. Fig. 1 describes the signature generation and signature verification phases of CLFSR-S scheme.

Next, we present an efficient, blind signature scheme using EGCLFSR.

C. The Proposed Blind Signature Scheme Using LFSR Sequences

The proposed blind signature scheme, BCLS is a cubic LFSR-based instantiation of the EG I.3 [7] variant-based blind signature scheme, proposed by Camenisch et al. [8]. Similar to the EGCLFSR scheme, during the initialization phase, all entities choose and agree on the system public parameters, $\mathsf{params} = \langle p, Q, f(x), H \rangle$. During the key generation phase, the ISP generates its long-term (private, public) key pair, $(SK, PK) = (x, \bar{s}_x)$.

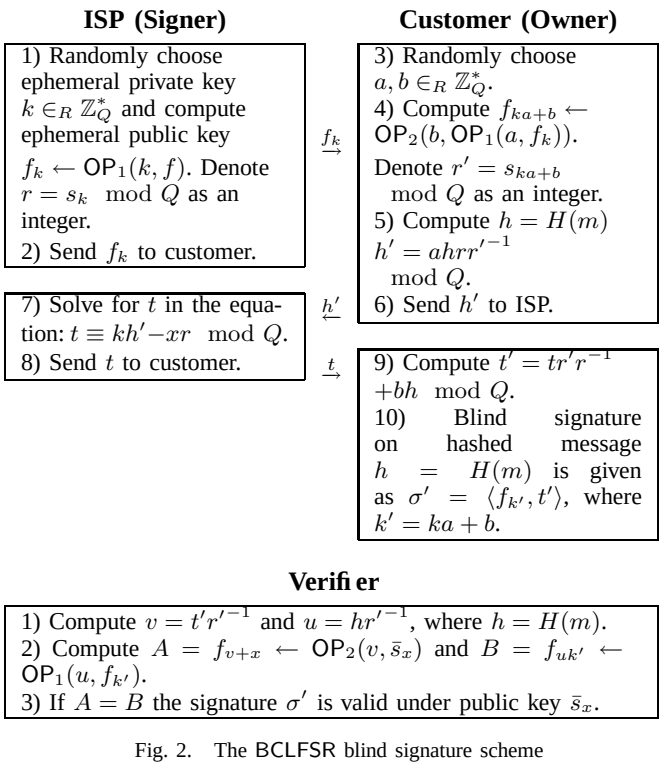

Fig. 2. The BCLFSR blind signature scheme

Fig. 2 shows the signature generation and verification phases of the proposed cubic LFSR-based blind signature scheme BCLS. The customer and the ISP interactively generate a blind signature σ' on a hashed message $h = H(m)$ as follows. (1) The ISP generates an ephemeral key pair (k, f_k) and sends the public part, f_k, to the customer. (2) The customer transforms f_k into the blind signature parameter $f_{k'}$, uses $f_{k'}$ to transform h into the blind hashed message h' and sends h' to the ISP. (3) The ISP generates a signature $\sigma = \langle f_k, t \rangle$ on the blind hashed message h' using its private key, x, and sends the parameter t to the customer. (4) The customer transforms the parameter t

[2]For a formal definition and analysis of unlinkability of blind signatures, the reader is referred to [4], [8], [15]

into t' such that the tuple $\sigma' = \langle f_{k'}, t' \rangle$ is a valid signature on hashed message $h = H(m)$ under the ISP's public key, $\bar{s}_x$.

Validity of a blind signature under the ISP's public key implies that the ISP cannot repudiate signing the message, thus, providing ISP-level accountability. Blinding of the message and signature transformations guarantee that when the customer reveals the (message, blind signature) pair (m, σ') to the verifier, the ISP cannot associate the pair to a particular customer.

V. Theoretical Analysis

We present a concise theoretical analysis of correctness, security and performance of the proposed cubic LFSR-based blind signature scheme.

A. Correctness

The cubic LFSR-based blind signature scheme, BCLFSR, is correct if the signature $\sigma' = \langle f_{k'}, t' \rangle$ generated by the customer, with cooperation of the ISP, on hashed message h passes the verification under the public key, $\bar{s}_x$, of the ISP, provided (1) all entities choose and agree upon the system public parameters $\mathsf{params} = \langle p, Q, f(x), H \rangle$; (2) the ISP honestly executes key generation algorithm of the underlying PKC, and (3) the ISP and the customer honestly execute signature generation algorithm of the BCLFSR scheme.

Proposition 1: The proposed cubic LFSR-based blind signature scheme, BCLFSR, follows the correctness property.

Proof: In the verification phase of the blind signature scheme, BCLFSR, the equality of the terms A and B can be shown as follows:

$$\begin{aligned} A &= f_{v+x} = f_{t'r'^{-1}+x} = f_{(tr'r^{-1}+bh)r'^{-1}+x} \\ &= f_{(kh'-xr)r^{-1}+bhr'^{-1}+x} = f_{(kahrr'^{-1})r^{-1}-x+bhr'^{-1}+x} \\ &= f_{kahr'^{-1}+bhr'^{-1}} = f_{(ka+b)hr'^{-1}} = f_{uk'} = B \end{aligned}$$

Thus, the signature σ' on $h = H(m)$ is valid under public key, $\bar{s}_x$ of the ISP. ■

B. Security Analysis

The security of the proposed cubic LFSR-based blind signature scheme, BCLFSR is based on the difficulty of solving the trace discrete logarithm (Tr-DL) problem in $\mathbb{F}_q$ [11], [12], [20], [21]. Informally, the trace function $Tr : \mathbb{F}_{q^3} \mapsto \mathbb{F}_q$ is given as $Tr(\alpha) = \alpha + \alpha^q + \alpha^{q^2}$. The Tr-DL problem and assumption can be defined as follows:

Definition 1: Let α be a generator of the multiplicative group $(\mathbb{F}_{q^3})^*$, where q is a large prime or a power of a large prime. The Tr-DL Problem in $\mathbb{F}_q$ can be defined as follows: Given $(q, \alpha \in (\mathbb{F}_{q^3})^*, \beta \in \mathbb{F}_q)$, find an index k such that $\beta = Tr(\alpha^k)$ or determine that there is no such index.

Let $\mathcal{A}$ be a probabilistic polynomial time (PPT) algorithm that runs in time t and solves the Tr-DL problem with probability at least ϵ. Define the advantage of the (t, ϵ) Tr-DL solver $\mathcal{A}$ as: $\mathsf{Adv}_{\mathcal{A}}^{TrDL} = Pr[\mathcal{A}(q, \alpha, \beta) = k \mid \alpha \in_R \mathbb{F}_{q^3}, k \in_R \mathbb{Z}_Q, \beta = Tr(\alpha^k)]$. The probability is over the random choices of α, k and the random bits of $\mathcal{A}$.

Tr-DL Assumption: The finite field $\mathbb{F}_q$ satisfies the Tr-DL Assumption if $\mathsf{Adv}_{\mathcal{A}}^{TrDL}(\lambda)$ is a negligible function.

Lemma 1 (Giuliani et al. [21]): The Tr-DL Problem is equivalent to the DL problem.

Lemma 2: The 2-party signature scheme EGCLFSR is equivalent to the well-known EG I.3 variant [7] of the Generalized ElGamal scheme.

Proof Sketch: $\Rightarrow$: Given a EGCLFSR signature $\sigma = \langle f_k, t \rangle$, we know $f_{(tr^{-1}+x)} = f_{(hr^{-1}k)}$. Let α be a root of the irreducible polynomial $f(x)$. Then, we have $\alpha^{tr^{-1}+x} = \alpha^{hr^{-1}k}$ with $t \equiv kh - xr$ which is the EG I.3 scheme. Thus, the EGCLFSR reduces to the EG I.3 scheme.

$\Leftarrow$: In EG I.3, $\alpha^{tr^{-1}+x} = \alpha^{hr^{-1}k}$ with $t \equiv kh - xr$. This implies $Tr(\alpha^{tr^{-1}+x}) = Tr(\alpha^{hr^{-1}k})$. Thus, the EG I.3 scheme reduces to EGCLFSR scheme. Hence, the equivalence. ■

Theorem 1: The cubic LFSR-based signature scheme, BCLFSR, is a blind signature scheme.

Proof Sketch: In the BCLFSR scheme, during generation of a blind signature $\sigma' = \langle f_{k'}, t' \rangle$ on a hashed message $h = H(m)$, the parameters known to the ISP (also referred to as the view of the ISP) are $\langle h', k, f_k, t \rangle$. The proposed cubic LFSR-based signature scheme, BCLFSR, is blind if, the (message, blind signature) pair (m, σ') is statistically independent from the view of the ISP and σ' is a valid signature on $h = H(m)$ under the ISP's public key $\bar{s}_x$ [8].

By Proposition 1, the signature σ' on the hashed message $h = H(m)$, generated following the BCLFSR scheme's signature generation algorithm, is valid under the public key, $\bar{s}_x$. What remains to be shown is that given an arbitrary view of the ISP, $\langle h', k, f_k, t \rangle$, and a valid (message, blind signature) pair (m, σ'), the elements a and b can be uniquely determined. Following the proof of Theorem 2 in [8] we can show that elements a and b can be uniquely determined as: $a = h'h^{-1}r'r^{-1} \mod Q$ and $b = (t' - tr'r^{-1})h^{-1} \mod Q$. Also, since the customer randomly chooses the elements $a, b \in \mathbb{Z}_Q^*$, the statistical independence of the (message, blind signature) pair and ISP's view is immediate [8]. ■

C. Performance Analysis

Cubic LFSR-based PKCs [11], [12], [13] use reduced representations of finite field elements. Elements in an extension field $\mathbb{F}_{q^n}$ are represented by their corresponding minimal polynomials with co-efficients in the base field $\mathbb{F}_q$. The security of LFSR-based PKCs is based on the difficulty of solving the DL problem in the extension field $\mathbb{F}_{q^n}$. However, all computations are performed in the base field $\mathbb{F}_q$.

Table I shows direct comparisons of the proposed cubic LFSR-based blind and parameter hidden signature schemes with the scheme by Camenisch et al. [8]. We consider a security benchmark of 1024-bits – the system public parameters of the scheme in [8] are given by the tuple $\mathsf{params} = \langle p, q, \alpha \rangle$, where p and q are 1024 and 160 bit primes, respectively, and α is an element of order q in $\mathbb{Z}_p^*$.

Note that given $\alpha \in \mathbb{F}_{p^6}$, where p is a 170-bit prime, computing α^k for any integer k requires approximately

TABLE I
PERFORMANCE COMPARISON. TERM e REPRESENTS MODULAR EXPONENTIATION WITH SECURITY BENCHMARK OF 1024-BITS.

	Camenisch et al. [8]	BCLFSR
Generation cost	$3e$	$3\mathsf{OP}_1 \approx 1e$
Verification cost	$2e$	$2\mathsf{OP}_1 \approx 0.66e$
PK size (bits)	1024	340
Sig. size (bits)	320	500
Underlying Pblm.	DLP	Tr-DLP

$23.4 \log_2 Q$ multiplications, where Q, the order of α, is a 160-bit prime [12]. However, computing the kth sequence term $s_k = Tr(\alpha^k)$ given f (represented by $Tr(\alpha)$) using sequence operation OP_1 takes only $8 \log(k \mod Q)$ multiplications which is approximately three times faster than computing α^k, given α [12]. The equivalent modular exponentiations for sequence operations are shown in Table I as OP_1 [0.33].

Blind signature generation and verification in our cubic-LFSR based scheme are approximately three times faster than the equivalent operations in the scheme by Camenisch et al. [8]. Furthermore, the public key size of 340-bits ($\bar{s}_x$) in the proposed blind signature, BCLFSR, is one-third the public key size of 1024-bits (α^x) used in [8]. The signature size of the scheme in [8] is 320-bits. In our proposed schemes, the size of the signature equals 500-bits.

VI. CONCLUSIONS

Blind signatures are useful in protocols that require the origin of a message to be certified in some way, but anonymity of the actual originator is desirable. Although blind signature techniques have been known for some time, traditionally they are built from heavyweight cryptographic techniques. This limits their utility for the design of protocols where performance is important. In this paper, we introduced a new blind signature scheme, BCLFSR, based on the properties of cubic LFSR sequences. The performance properties of the scheme make it more suitable than traditional blind signature schemes for use in performance-sensitive network protocols. The blind signature, BCLFSR, is constructed using a novel cubic LFSR sequence-based, 2-party signature scheme, EGCLFSR, and uses extremely fast LFSR operations to achieve superior performance and least storage overhead compared to a well known traditional construction by Camenisch et al. [8]. The security of the blind signature, BCLFSR is based on the Tr-DL(DL) Problem in $\mathbb{F}_q(\mathbb{F}_{q^3})$. BCLFSR was constructed using the XTR-PKC for simplicity, although it can be seamlessly constructed using the GH-PKC and can also be extended to PKCs based on higher order LFSR sequences, with minor modifications, depending on the desired security level.

REFERENCES

[1] X. Yang, D. Wetherall, and T. Anderson, "A dos-limiting network architecture," in *Proceedings SIGCOMM 2005 Conference, Philadelphia, USA*, August 2005, pp. 241–252.

[2] A. Bender, N. Spring, D. Levin, and B. Bhattacharjee, "Accountability as a service," in *Proceedings of 3rd Workshop on Steps to Reducing Unwanted Traffic in the Internet (part of USENIX '07)*, June 2007.

[3] J. Xu, J. Fan, M. Ammar, and S. Moon, "Prefix-preserving ip address anonymization," in *Proceedings of the IEEE International Conference on Network Protocols, Paris, France*, November 2002, pp. 280–289.

[4] D. Chaum, "Blind signatures for untraceable payments." in *Proceedings of CRYPTO: Advances in Cryptology*, 1982, pp. 199–203.

[5] H. Petersen and P. Horster, "Self-certified keys – concepts and applications." in *Proceedings of CMS*. Chapman & Hall, 1997, pp. 102–116.

[6] P. Horster, M. Michels, and H. Petersen, "Blind multisignature schemes and their relevance to electronic voting." in *Proceedings of ACSAC*. IEEE Press, 1995, pp. 149–155.

[7] P. Horster, H. Petersen, and M. Michels, "Meta-ElGamal signature schemes." in *Proceedings of ACM CCS*, 1994, pp. 96–107.

[8] J. Camenisch, J.-M. Piveteau, and M. Stadler, "Blind signatures based on the discrete logarithm problem." in *Proceedings of EUROCRYPT: Workshop on the Theory and Application of Cryptographic Techniques*, ser. LNCS, vol. 950. Springer, 1994, pp. 428–432.

[9] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, November 1976.

[10] FIPS, "Digital Signature Standard (DSS)," National Institute for Standards and Technology, pp. ii + 74, 2000.

[11] G. Gong and L. Harn, "Public-key cryptosystems based on cubic finite field extensions," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2601–2605, 1999.

[12] A. K. Lenstra and E. R. Verheul, "The XTR Public Key System," *LNCS*, vol. 1880, pp. 1–19, 2000.

[13] H. Niederreiter, "A public-key cryptosystem based on shift register sequences," in *Proceedings of EUROCRYPT*. Springer-Verlag, 1986, pp. 35–39.

[14] P. Horster, M. Michels, and H. Petersen, "Hidden signature schemes based on the discrete logarithm problem and related concepts." in *Proceedings of CMS*. Chapman & Hall, 1995, pp. 162–177.

[15] D. Pointcheval and J. Stern, "Provably secure blind signature schemes." in *Proceedings of ASIACRYPT*, ser. LNCS, vol. 1163. Springer, 1996, pp. 252–265.

[16] M. Girault, "Self-certified public keys." in *Proceedings of EUROCRYPT*, 1991, pp. 490–497.

[17] A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, S. Kent, and W. Strayer, "Hash-based IP traceback," in *ACM SIGCOMM 2001 Conference*, August 2001.

[18] X. Liu, X. Yang, D. Wetherall, and T. Anderson, "Efficient and secure source authentication with packet passports," in *USENIX Workshop on Steps to Reducing Unwanted Traffic in the Internet*, 2006.

[19] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," in *IEEE Symposium on Security and Privacy*, 2003.

[20] G. Gong, L. Harn, and H. Wu, "The GH public-key cryptosystem," in *Proceedings of SAC*. Springer-Verlag, 2001, pp. 284–300.

[21] K. J. Giuliani and G. Gong, "New LFSR-based cryptosystems and the trace discrete log problem (trace-DLP)," in *Proceedings of SETA*, 2004, pp. 298–312.

[22] S. Chakrabarti, S. Chandrasekhar, M. Singhal, and K. L. Calvert, "Authenticating DSR using a novel multisignature scheme based on cubic LFSR sequences," in *Proceedings of The Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, ser. LNCS, vol. 4572. Springer, 2007, pp. 156–171.

[23] ——, "Authenticating feedback in multicast applications using a novel multisignature scheme based on cubic LFSR sequences." in *Proceedings of The 3rd IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS)*, Canada, May 2007.

[24] X. Li, D. Zheng, and K. Chen, "LFSR-based signatures with message recovery." *International Journal of Network Security*, vol. 4, no. 3, pp. 266–270, May 2007.

[25] C. H. Tan, X. Yi, and C. K. Siew, "Signature schemes based on 3rd order shift registers." in *Proceedings of ACISP*, ser. LNCS, vol. 2119. Springer, 2001, pp. 445–459.

[26] S. W. Golomb, *Shift Register Sequences*. Holden-Day, 1967.

[27] E. Peeters, M. Neve, and M. Ciet, "XTR implementation on reconfigurable hardware." in *Proceedings of CHES*, ser. LNCS, vol. 3156. Springer, 2004, pp. 386–399.