Compressed Data Public Key Cryptosystems with DLP Over Extension Fields

M. Ashraf and B. B. Kırlar

***Abstract*—In recent years, Public Key Cryptosystems (PKCs) are converging to gain high security with reduced bandwidth for data transmission. The goal of these PKCs is to face the challenges imposed by availability of faster processors for cryptanalysis and higher data transmission rates. For this purpose new PKCs are proposed which include LUC-PKC, GH-PKC, XTR-PKC and Torus based cryptography. In these systems, the cryptographic operations are carried out in subfield whereas security of extension field is ensured. The discrete logarithm problem in extension field is relatively hard when compared with subfield. In this paper we survey these PKCs by giving the underlying mathematical concepts with key group operations, relevant details of PKC, and then achieved goals in these systems. We also indicate the vulnerability of such systems to SPA attacks, wherever, applicable.**

***Index Terms*—Public Key Cryptosystems, Discrete Logarithm Problem, extension fields, LFSR, characteristic sequence, trace function, Torus Based Cryptography.**

I. Introduction

CRYPTOSYSTEMS based on intractability of discrete logarithm was first time realized by Diffie and Hellman in 1976 [1]. In their work, they showed that two parties $\mathcal{A}$ and $\mathcal{B}$ can communicate securely over an unsecured channel. For example, let $G =< g >$ be a multiplicative of large prime order and $2 < a, b < \#G$, $\mathcal{A}$ computes g^a and $\mathcal{B}$ computes g^b. They exchange these messages over unsecured channel and compute $(g^b)^a$ and $(g^a)^b$ respectively to acquire a common key g^{ab}. In this case the intractability of Discrete Logarithm Problem (DLP) that is the computation of a given g^a depends upon the large group order. On the other hand, if group order is large then number of bits to represent group element is also large. Therefore, larger transmission bandwidth is required which reduces communication efficiency.

Over the last few years, efforts were made to improve efficiency of Public Key Cryptosystems (PKCs) in terms of compact representation and increased security. These improvements resulted in form of LUC-PKC [3], GH-PKC [4], XTR-PKC [7] and Torus based cryptography [12]. In these systems, group operations are carried out in intermediate or prime subfields (i.e; $\mathbb{F}_{p^k}$, $k \mid r$ or $\mathbb{F}_p$) whereas, security of extension field (i.e; $\mathbb{F}_{p^r}$, where $r = 2, 3$ and 6 for LUC-PKC, GH-PKC and XTR-PKC, respectively) is ensured. Hence, high security is achieved with operands of lesser number of bits. In contrast, for Diffie-Hellman PKC both group operations and DLP are in prime field $\mathbb{F}_p$.

Manuscript received March 11, 2012.

Muhammad Ashraf is with the Institute of Applied Mathematics, METU, Ankara, Turkey, e-mail: ashraf6061@gmail.com

Barış Bülent Kırlar is with the Department of Mathematics, Süleyman Demirel University, Isparta, Turkey, e-mail: bariskirlar@sdu.edu.tr

Smith and Lennon introduced PKC based on Lucas functions in [2], which was further refined by Smith and Skinner in [3]. They used a subgroup of order $p + 1 \in \mathbb{F}_{p^2}$ and employed Lucas functions to perform group operation over prime subfield $\mathbb{F}_p$ thus achieving security of $\mathbb{F}_{p^2}$ for cryptographic protocols. Thereby, they compressed the operands by a factor of 2. The GH-PKC was proposed by Gong and Harn in 1999 [4]. They used 3rd order recurrence relation for Linear Feedback Shift Register (LFSR) using characteristic polynomial of degree three. This characteristic polynomial being irreducible cubic over $\mathbb{F}_p$ splits in $\mathbb{F}_{p^3}$ to ensure that roots belong to $\mathbb{F}_{p^3}$ and hence DLP in $\mathbb{F}_{p^3}$. The output sequence of LFSR is computed over $\mathbb{F}_p$ and elements are represented by $\log p$ bits. Hence, a compressed representation with DLP over $\mathbb{F}_{p^3}$. Moreover, GH-PKC employs a subgroup of order p^2+p+1 of $\mathbb{F}^*_{p^3}$ to construct cryptographic protocols. After GH-PKC, Lenstra and Verheul proposed XTR system [7] based on trace computation for cryptographic protocols. They observed that a cubic polynomial of the form;

$$f(x) = x^3 - \mathrm{Tr}(\alpha)x^2 + \mathrm{Tr}(\alpha)^p x - 1 \in \mathbb{F}_{p^2}[x],$$

splits in $\mathbb{F}_{p^6}$, where $\alpha \in \mathbb{F}_{p^6}$ and $\mathrm{Tr}(\alpha) = \alpha+\alpha^{p^2}+\alpha^{p^4} \in \mathbb{F}_{p^2}$. They proved that the elements α of $\mathbb{F}_{p^6}$ with trace in $\mathbb{F}_{p^2}$ forms a subgroup of order p^2-p+1. They also showed that powers of these elements α^n for $n \in \mathbb{Z}$ also belong to this subgroup. Thus, trace computation is carried out in $\mathbb{F}_{p^2}$ resulting into compression by a factor of 3. Some improvements in XTR were also proposed in [10] and [11] but the underlying concept does not change. We will survey only concepts and main areas for highlighting concepts.

Rubin and Silverberg [12] proposed Torus based Public Key Cryptography in 2003. They observed that cryptographic operation in extension field $\mathbb{F}_{p^n}$ are basically carried out in subgroup of $\mathbb{F}^*_{p^n}$ which is equivalent to scalar restriction ($\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}$) of the group. This restriction decomposes as a product of algebraic tori $\mathbb{T}_r$ for $r|n$. To enjoy full security of $\mathbb{F}^*_{p^n}$ the torus must be of the form $\mathbb{T}_n(\mathbb{F}_p) \cong G_{p,n} \subseteq \mathbb{F}^*_{p^n}$. $\varphi(n)$ is the dimension of torus over $\mathbb{F}_p$, where φ is Eulers totient function. This implies compression of $n/\varphi(n)$ is achieved. The cryptographic protocols can be carried out by computing compression map $\rho : G_{p,n} \to \mathbb{F}_p^{\varphi(n)}$ and decompression map $\psi : \mathbb{F}_p^{\varphi(n)} \to G_{p,n}$ such that $\rho \circ \psi = 1$.

This paper is organized as follows, in section 2, LUC-PKC and its relevant details are discussed. In section 3, GH-PKC or cubic field systems are presented. In section 4 XTR-PKC and related details are given. In section 5, we discuss the torus based cryptosystem and finally in section 6, we conclude the paper. Being a survey paper, relevant papers and authors are frequently referred.

II. LUC-Public Key Cryptosystem

LUC-PKC is a Public Key Cryptosystem based on the properties of Lucas functions. This system was introduced by Smith and Lennon in 1993 [2] as an alternate PKC to Diffie-Hellman and RSA cryptographic protocols. In this PKC, a second order linear recurrence relation is used to construct Diffie-Hellman key exchange protocol and RSA type cryptosystem. Later on it was further refined by Smith and Skinner [3] in 1994, by presenting cryptosystem and digital signature schemes. We will discuss salient underlying arithmetic operations and their adaptation to Diffie-Hellman's key exchange protocol.

Linear Recurrence of Higher Order [2]. Let $\ell, a_i \in \mathbb{Z}$, for $0 < i < m$, then the sequence of integers $\hat{S}_n = \{s_\ell\}$ defined by:

$$s_n = \sum_{i=1}^{m} a_i f_{n-i} = a_1 f_{n-1} + a_2 f_{n-2} + \cdots + a_m f_{n-m},$$

which is called an mth order linear recurrence relation. In this relation next term is computed through linear relation of previous m terms. For example, the second order linear recurrence can be given by,

$$f_n = A f_{n-1} - B f_{n-2}, \text{ with } \gcd(A, B) = 1, \qquad (1)$$

with given f_0 and f_1. The generating function $G(x)$ corresponding to equation (1), is as follows:

$$G(x) = x^2 - Ax + B. \qquad (2)$$

The procedure to derive generating function can be found in [13]. Let α_1 and α_2 be two roots of equation (2), then the sum $(\alpha_1 + \alpha_2)$ and product $(\alpha_1 \cdot \alpha_2)$ of these roots is of special attention. If $g_1, g_2 \in \mathbb{Z}$ then following relation was proved in [2]:

$$A(g_1\alpha_1^{n-1} + g_2\alpha_2^{n-1}) - B(g_1\alpha_1^{n-2} + g_2\alpha_2^{n-2}) = g_1\alpha_1^n + g_2\alpha_2^n.$$

This implies any sequence $\hat{S}_n$ generated by equation (1), is of the form $g_1\alpha_1^n + g_2\alpha_2^n$ with $s_0 = 2$ and $s_1 = g_1\alpha_1 + g_2\alpha_2$. For LUC-PKC, following solutions to $G(x)$ are of special attention as interesting relations can be defined for applications in this PKC. These solutions are given below:

$$\gamma_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2},$$
$$\lambda_n = \alpha_1^n + \alpha_2^n,$$

with $\gamma_0 = 0, \gamma_1 = 1$ and $\lambda_0 = 2, \lambda_1 = g_1$. Note that γ_n and λ_n depends only on the integers g_1 and g_2 and the terms $\gamma_n(g_1, g_2)$ and $\lambda_n(g_1, g_2)$ are called *Lucas Functions* of g_1 and g_2.

Some Interesting Relations [2]. Let $A = \alpha_1 + \alpha_2$, $B = \alpha_1\alpha_2$ and discriminant of $G(x)$,

$$\Delta = A^2 - 4B = (\alpha_1 - \alpha_2)^2$$

be given, then following relations hold:

- $\lambda_{2n} = \lambda_n^2 - 2B^n$.
- $\lambda_{2n-1} = \lambda_n\lambda_{n-1} - AB^{n-1}$.
- $\lambda_{2n+1} = A\lambda_n^2 - B\lambda_n\lambda_{n-1} - AB^n$.
- $\lambda_n^2 = \Delta\gamma_n^2 + 4B^n$.
- $2\lambda_{n+m} = \lambda_n\lambda_m + \Delta\gamma_n\gamma_m$.
- $2B\lambda_{n-m} = \lambda_n\lambda_m - \Delta\gamma_n\gamma_m$.

Now, if second order generating function is $\bar{G}(x) = x^2 - \lambda_k(A, B)x + B^k$, then $\lambda_k(A, B) = \alpha_1^k + \alpha_2^k$. Similarly, we have

$$\lambda_n(\lambda_k(A, B), b^k) = (\alpha_1^k)^n + (\alpha_2^k)^n = \lambda_{nk}(A, B).$$

It shows a clear generalization of the rule for composition of powers, with subscript of a Lucas function playing the role of a power.

Diffie-Hellman Key Exchange and Lucas Functions. The Diffie-Hellman type key exchange protocol can be established by using Lucas functions. Let $\mathcal{A}$ and $\mathcal{B}$ want to agree on a common key $\mathcal{K}$. Also let $m, n \in \mathbb{Z}$ and $g \in \mathbb{F}_p$ a primitive element, where p is a large prime. Then $\mathcal{A}$ and $\mathcal{B}$ can do the following independently to agree on a common key $\mathcal{K}$.

- $\mathcal{A}$ computes g^m and sends to $\mathcal{B}$.
- $\mathcal{B}$ computes g^n and sends to $\mathcal{A}$
- $\mathcal{A}$ and $\mathcal{B}$ computes $\mathcal{K} = (g^n)^m = (g^m)^n = g^{nm}$.

Similarly, for Lucas functions Diffie-Hellman key exchange is carried out as follows:

- $\mathcal{A}$ computes $\lambda_m(A, B)$ and sends to $\mathcal{B}$.
- $\mathcal{B}$ computes $\lambda_n(A, B)$ and sends to $\mathcal{A}$
- $\mathcal{A}$ and $\mathcal{B}$ computes $\mathcal{K} = \lambda_m(\lambda_n(A, B)) = \lambda_n(\lambda_m(A, B)) = \lambda_{mn}(A, B)$.

Achieved Goals. Following main goals are achieved in LUC cryptosystem:

- Data transmission in prime field $\mathbb{F}_p$ and DLP lie in extension field $\mathbb{F}_{p^2}$.
- A compression factor of 2 is achieved.
- Adaptation to cryptographic protocols using Lucas functions.

III. GH-Public Key Cryptosystem

Gong and Harn proposed new public key cryptosystem in [4]. They used characteristic sequence of an LFSR to construct DLP over $\mathbb{F}_{p^3}$ while computations are carried out in prime field $\mathbb{F}_p$, with p, prime. In this section we will give the basic details of this cryptosystem and Diffie-Hellman key exchange, based on this concept as an example.

Definition : LFSR Sequence. Let $f(x)$ be a polynomial given by,

$$f(x) = \sum_{i=0}^{n} c_i x^i, \; c_i \in \mathbb{F}_p \text{ and } c_n = 1.$$

and $\hat{s}$ be a sequence over $\mathbb{F}_p$ such that;

$$\hat{s} = \{s_i\} = s_0, s_1, s_2, \ldots; \text{ with } s_i \in \mathbb{F}_p.$$

The $\hat{s}$ is called an LFSR sequence of order n generated by $f(x)$ if it satisfies the following linear recursive relation:

$$s_{k+n} = \sum_{i=0}^{n-1} c_i s_{k+i}, \; k = 0, 1, \ldots$$

The states $s_0, s_1, \ldots, s_{n-1}$ are called an *initial states* of the sequence $\hat{s}$ generated by $f(x)$.

Characteristic Sequence and Trace Representation. If $f(x)$ is an irreducible polynomial over $\mathbb{F}_p$, and let α be a root of

$f(x)$ in extension field $\mathbb{F}_{p^r}$, then the trace function is defined as

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{r-1}}.$$

In the extension field $\mathbb{F}_{p^3}$ the i-th term of $\hat{s}$ for some $\beta \in \mathbb{F}_p$ can be given as:

$$s_i = \mathrm{Tr}(\beta\alpha^i),\ i = 0, 1, 2 \ldots$$

If $\beta = 1$ then sequence $\hat{s}$ is called characteristic sequence of $f(x)$.

Lemma 1 [13]. If $f(x) \in \mathbb{F}_p[x]$ is irreducible over $\mathbb{F}_p$ and $\hat{s}$ as defined above is generated by $f(x)$, then

$$per(\hat{s}) = per(f) = ord(\alpha),$$

where $\alpha \in \mathbb{F}_{p^r}$ such that $f(\alpha) = 0$. Here, period of f and order of α are denoted by $per(f)$ and $ord(\alpha)$, respectively.

Third Order Characteristic Equation of GH-PKC. Let $\hat{s}$ be characteristic sequence generated by irreducible polynomial $f(x) = x^3 - ax^2 + bx - 1$ with $a, b \in \mathbb{F}_p$ and $f(x) \in \mathbb{F}_p[x]$. Let the initial states of $\hat{s}$ be $s_0 = 3, s_1 = a$, and $s_2 = a^2 - 2b$ then following holds:

Lemma 2 [4]. If $per(f)$ dividing by $p^2 + p + 1$ is equal to $per(\hat{s})$, then for some $k \in \mathbb{Z}$, s_k can be determined as follows:

$$s_k = \mathrm{Tr}(\alpha^k),\ k = 0, 1, \ldots,$$

where $\alpha \in \mathbb{F}_{p^3}$ is a root of $f(x)$.

Reciprocal Sequence. Let $f(x) = x^3 - ax^2 + bx - 1$ be the characteristic equation with associated characteristic sequence $s_k = s_k(a, b)$ or $s_k(f)$, then the reciprocal polynomial $f^{-1}(x)$ of $f(x)$ is defined as:

$$f^{-1}(x) = x^3 - bx^2 + ax - 1,$$

and the associated reciprocal sequence is $s_{-k}(a, b) = s_k(b, a)$.

Lemma 3 [4]. Let $f(x) = x^3 - ax^2 + bx - 1$ be an irreducible polynomial over $\mathbb{F}_p$, $\hat{s}$ be its characteristic sequence and $\alpha \in \mathbb{F}_{p^3}$ be the root of $f(x)$. Then following holds:

- For all integers e and r,

$$s_e(s_r(a, b), s_{-r}(a, b)) = s_{er}(a, b)$$

- For all integers n and m
  - i) $s_{2n} = s_n^2 - 2s_{-n}$,
  - ii) $s_n s_m - s_{n-m} s_{-m} = s_{n+m} - s_{n-2m}$.
- If $\gcd(k, per(\hat{s})) = 1$, then α^{kp^i}, $i = 0, 1, 2$ are three roots of $g(x) = x^3 - s_k x^2 + s_{-k} x - 1 \in \mathbb{F}_{p^3}$. The proofs can be found in [4].

Formulae to Compute (s_k) [4]. Let $k = \sum_{i=0}^{\ell} k_\ell 2^{\ell - i}$, $k_i \in \{-1, 0, 1\}$ be the binary representation of k, $T_0 = k_0 \neq 0$, and $T_j = k_j + 2T_{j-1}$, $1 \geq j \geq \ell$. If three terms of the $\hat{s}$ $(s_{T_{j-1}-1}, s_{T_{j-1}}, s_{T_{j-1}+1})$ are known then the next three terms $(s_{T_j-1}, s_{T_j}, s_{T_j+1})$ can be computed as follows:

If $k_j = 0$

$$\begin{aligned} s_{T_j-1} &= s_{T_{j-1}} s_{T_{j-1}-1} - b s_{-T_{j-1}} + s_{-(T_{j-1}+1)}; \\ s_{T_j} &= s_{T_{j-1}}^2 - 2 s_{-T_{j-1}}; \\ s_{T_j+1} &= s_{T_{j-1}} s_{T_{j-1}+1} - a s_{-T_{j-1}} + s_{-(T_{j-1}-1)}. \end{aligned}$$

If $k_j = 1$

$$\begin{aligned} s_{T_j-1} &= s_{T_{j-1}}^2 - 2 s_{-T_{j-1}}; \\ s_{T_j} &= s_{T_{j-1}} s_{T_{j-1}+1} - a s_{-T_{j-1}} + s_{-(T_{j-1}-1)}; \\ s_{T_j+1} &= s_{T_{j-1}+1}^2 - 2 s_{-(T_{j-1}-1)}. \end{aligned}$$

If $k_j = -1$

$$\begin{aligned} s_{T_j-1} &= s_{T_{j-1}-1}^2 - 2 s_{-(T_{j-1}-1)}; \\ s_{T_j} &= s_{T_{j-1}} s_{T_{j-1}+1} - a s_{-T_{j-1}} + s_{-(T_{j-1}-1)}; \\ s_{T_j+1} &= s_{T_{j-1}+1}^2 - 2 s_{-(T_{j-1}+1)}. \end{aligned}$$

The initial conditions are $s_0 = 3$, $s_1 = a$, $s_2 = a^2 - 2b$, $s_{-1} = b$, and $s_{-2} = b^2 - 2a$. The algorithm for above formulae can be found in [5]. Moreover, an algorithmic improvement in computational complexity for GH-PKC was also proposed in [6], but the basic concept does not change.

GH-PKC based Diffie-Hellman Key Exchange Scheme. Following key distribution scheme is just as an example for adaptation to cryptographic protocols:

- ***System Public parameters.*** A prime p, $f(x) = x^3 - ax^2 + bx - 1$ an irreducible polynomial over $\mathbb{F}_p$ with order $q = p^2 + p + 1$.
- $\mathcal{A}$ selects $a, 0 < a < q$ such that $\gcd(a, q) = 1$ as private key and computes public key (s_a, s_{-a}) and sends this key to $\mathcal{B}$.
- $\mathcal{B}$ selects $b, 0 < b < q$ such that $\gcd(b, q) = 1$ as private key and computes public key (s_b, s_{-b}) and sends this key to $\mathcal{A}$.
- $\mathcal{A}$ computes:

$$\mathcal{K} = (s_{ab}, s_{-ab}) = (s_a(s_b, s_{-b}), s_{-a}(s_b, s_{-b})).$$

- $\mathcal{B}$ computes:

$$\mathcal{K} = (s_{ab}, s_{-ab}) = (s_b(s_a, s_{-a}), s_{-b}(s_a, s_{-a})).$$

In this way both $\mathcal{A}$ and $\mathcal{B}$ compute common key $\mathcal{K} = (s_{ab}, s_{-ab})$.

Remark: ***Resistance to SPA attacks.*** Additionally, we observe that the operations while computing $k_j = 0$ and $k_j = 1$ are almost identical. This makes the algorithm resistant against Simple Power Analysis (SPA) attacks. In SPA attacks some environmental parameters (electrical power spectrum, timing analysis etc.) are analyzed to extract secret information of the cryptosystem.

Achieved Goals. In GH-PKC following gaols are achieved:

- Compact representation of operands over $\mathbb{F}_p$. A compression ratio by a factor of 3/2 is achieved [9].
- LFSR based computation of cryptographic protocols.
- Resistant to SPA based side channel attacks by employing identical computation as indicated above.
- Adaptation of the concept for public key cryptosystems such as Diffie-Hellman key distribution scheme, RSA type PKC, and digital signature scheme etc.

IV. XTR-Public Key Cryptosystem

XTR is an acronym for 'ECSTR' which means Efficient and Compact Subgroup Trace Representation. XTR-PKC was

proposed by Lenstra and Verheul in [7]. In this system, the computations are performed in an intermediate subfield of the form $\mathbb{F}_{p^2}$ rather than a prime field of the form $\mathbb{F}_p$. The security level benefits from the harder DLP defined over the extension field F_{p^6}. The subgroup of $\mathbb{F}^*_{p^6}$ is selected so that the irreducible cubic polynomial $f \in \mathbb{F}_{p^2}[x]$ can be fixed in the form $f(x) = x^3 - \mathrm{Tr}(\alpha)x^2 + \mathrm{Tr}(\alpha)^p x - 1$, where $f(\alpha) = 0$.

XTR Subgroup and Underlying Arithmetic. Let $\alpha \in \mathbb{F}_{p^6}$, then the conjugates of α over $\mathbb{F}_{p^2}$ are α, α^{p^2}, and α^{p^4}. The trace of α over $\mathbb{F}_{p^2}$ and the norm of α over $\mathbb{F}_{p^2}$ are as follows:

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^{p^2} + \alpha^{p^4},$$

and

$$\mathrm{Norm}(\alpha) = \alpha \cdot \alpha^{p^2} \cdot \alpha^{p^4} = \alpha^{1+p^2+p^4}. \quad (3)$$

Note that,

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \text{ so } |\mathbb{F}_{p^n}| = \prod_{d|n} \Phi_d(p).$$

where $\Phi_d(x)$ is d-th cyclotomic polynomial. So we have,

$$\begin{aligned} |\mathbb{F}_{p^6}| &= p^6 - 1 \\ &= (p^2 - p + 1)(p^2 + p + 1)(p + 1)(p - 1) \\ &= \Phi_6(p)\Phi_3(p)\Phi_2(p)\Phi_1(p). \end{aligned}$$

Therefore, an element of $\mathbb{F}_{p^6}$ of order dividing $p^2 - p + 1$ does not lie in any proper subfield of $\mathbb{F}^*_{p^6}$. Now we select $\alpha \in \mathbb{F}_{p^6}$ such that $ord(\alpha) > 3$ dividing $p^2 - p + 1$. This implies $p^2 \equiv p - 1 \pmod{p^2 - p + 1}$ and $p^4 \equiv -p \pmod{p^2 - p + 1}$. After selecting such subgroup the conjugates of $\alpha \in \mathbb{F}_{p^6}$ over $\mathbb{F}_{p^2}$ becomes α, $\alpha^{p-1} = \alpha^{p^2}$, and $\alpha^{-p} = \alpha^{p^4}$. In the light of above properties, equation (3) becomes

$$\mathrm{Norm}(\alpha) = \alpha^{1+p^2+p^4} = \alpha^{1+p-1-p} = 1.$$

After this development $f(x) \in \mathbb{F}_{p^2}[x]$ has the following representation with the roots α, α^{p-1}, $\alpha^{-p} \in \mathbb{F}_{p^6}$:

$$\begin{aligned} f(x) &= (x - \alpha)(x - \alpha^{p-1})(x - \alpha^{-p}) \\ &= x^3 - \mathrm{Tr}(\alpha)x^2 + \mathrm{Tr}(\alpha)^p x + (-1)^3 \mathrm{Norm}(\alpha) \\ &= x^3 - \mathrm{Tr}(\alpha)x^2 + \mathrm{Tr}(\alpha)^p x - 1. \end{aligned}$$

In this case, $f(x)$ is actually minimal polynomial of $\alpha \in \mathbb{F}_{p^6}$ over $\mathbb{F}_{p^2}$. Therefore, any power of α^k for $k \in \mathbb{Z}$, and its conjugates are the roots of $f(x)$ [13]. So, we can replace $\mathrm{Tr}(\alpha)$ with $\mathrm{Tr}(\alpha^k)$ and $f(x)$ still remains minimal polynomial as defined above. Therefore, we compute $\mathrm{Tr}(\alpha^k) \in \mathbb{F}_{p^2}$ instead of computing $\alpha^k \in \mathbb{F}_{p^6}$. As a result, the number of bits of group operands for exponentiation is reduced by a factor of 3.

Definitions and Notations. Some definitions and notations are given below for subsequent use.

- Let $c \in \mathbb{F}_{p^2}$ and $f(c, x) \in \mathbb{F}_{p^2}[x]$, then

$$f(c, x) = x^3 - cx^2 + c^p x - 1.$$

- Let $\tau(c, n) = \mathrm{Tr}(\alpha^n)$ in shorthand we use $\tau(c, n) = c_n$.
- Let $S_n(c) = (c_{n-1}, c_n, c_{n+1}) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$.

Fundamentals for XTR Computational Algorithm [7]. We annotate the fundamental results being applied in XTR-PKC. The detailed information is provided in [7].

i). $c_{-n} = c_{np} = c_n^p$, for $n \in \mathbb{Z}$ and $c_n \in \mathbb{F}_{p^2}$.
ii). $c_{u+v} = c_u.c_v - c_v^p.c_{u-v} + c_{u-2v}$, for $u, v \in \mathbb{Z}$.
iii). $c_{2u} = c_u^2 - 2c_u^p$.
iv). $c_{u+2} = c.c_{u+1} - c^p.c_u + c_{u-1}$.
v). $c_{2u-1} = c_{u-1}.c_u - c^p.c_u^p + c_{u+1}^p$.
vi). $c_{2u+1} = c_{u+1}.c_u - c.c_u^p + c_{u-1}^p$.

XTR Algorithm for Computation of $S_u(c)$ given u and c.

- If $u = 0$, then $S_0(c) = (c^p, 3, c)$.
- If $u = 1$, then $S_1(c) = (3, c, c^2 - 2c^p)$.
- If $u = 2$, then use $c_{u+2} = c.c_{u+1} - c^p.c_u + c_{u-1}$, and $S_1(c)$ to compute c_3 and thereby $S_2(c)$.
- For $u > 2$ to compute $S_u(c)$ define $\hat{S}_i(c) = S_{2i+1}(c)$ and let $\hat{m} = u$. If m if even, then $\hat{m} = \hat{m} - 1$. Let $\hat{m} = 2m + 1$, also $k = 1$ and compute $\hat{S}_k(c) = S_3(c)$. Let $m = \sum_{j=0}^{r} m_j 2^j$ with $m_j \in \{0, 1\}$ and $m_r = 1$. For $j = r - 1, r - 2, \ldots, 0$ do the following:
  - If $m_j = 0$, then use $\hat{S}_k(c) = (c_{2k}, c_{2k+1}, c_{2k+2})$ to compute $\hat{S}_{2k}(c) = (c_{4k}, c_{4k+1}, c_{4k+2})$ and replace k by $2k$.
  - If $m_j = 1$, then use $\hat{S}_k(c) = (c_{2k}, c_{2k+1}, c_{2k+2})$ to compute $\hat{S}_{2k+1}(c) = (c_{4k+2}, c_{4k+3}, c_{4k+4})$ and replace k by $2k + 1$.

Now $2k + 1 = m$ and $S_{\hat{m}}(c) = \hat{S}_m(c)$. If u is even, then use $S_{\hat{m}}(c) = (c_{\hat{m}-1}, c_{\hat{m}}, c_{\hat{m}+1})$ to compute $S_{\hat{m}+1}(c) = (c_{\hat{m}}, c_{\hat{m}+1}, c_{\hat{m}+2})$ and replace $\hat{m}$ by $\hat{m} + 1$. As a result $S_u(c) = S_{\hat{m}}(c)$.

Algorithm to Compute $\mathrm{Tr}(\alpha)$

1. Apply XTR algorithm for $u = p + 1$ and random $c \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ to compute c_{p+1}.
2. If $c_{p+1} \in \mathbb{F}_p$ then return to Step 1.
3. Apply XTR algorithm for $u = (p^2 - p + 1)/q$ and c to compute $d = c_{(p^2-p+1)/q}$, where q is order of α.
4. If $d = 3$, then return to step 1.
5. Let $\mathrm{Tr}(\alpha) = d$.

XTR based Diffie-Hellman (DH) Key Exchange Scheme [7]. The XTR-DH key exchange protocol is given to serve as an example for cryptographic adaptation of the XTR concept. Let $\mathcal{A}$ wants to exchange a key $\mathcal{K}$ with $\mathcal{B}$. The public parameters are $p, q, \mathrm{Tr}(\alpha)$, where q is the order subgroup of $\mathbb{F}_{p^6}$. Following is the protocol:

- $\mathcal{A}$ selects at random $a \in \mathbb{Z}, 1 < a < q - 2$, and compute $S_a(\mathrm{Tr}(\alpha)) = (\mathrm{Tr}(\alpha^{a-1}), \mathrm{Tr}(\alpha^a), \mathrm{Tr}(\alpha^{a+1}))$ and sends $\mathrm{Tr}(\alpha^a) \in \mathbb{F}_{p^2}$ to $\mathcal{B}$.
- $\mathcal{B}$ selects at random $b \in \mathbb{Z}, 1 < b < q - 2$, and compute $S_b(\mathrm{Tr}(\alpha)) = (\mathrm{Tr}(\alpha^{b-1}), \mathrm{Tr}(\alpha^b), \mathrm{Tr}(\alpha^{b+1}))$ and sends $\mathrm{Tr}(\alpha^b) \in \mathbb{F}_{p^2}$ to $\mathcal{A}$.
- $\mathcal{A}$ receives $\mathrm{Tr}(\alpha^b)$ from $\mathcal{B}$ and computes $S_a(\mathrm{Tr}(\alpha^b)) = (\mathrm{Tr}(\alpha^{(a-1)b}), \mathrm{Tr}(\alpha^{ab}), \mathrm{Tr}(\alpha^{(a+1)b}))$ and subsequently determines $\mathcal{K} = \mathrm{Tr}(\alpha^{ab})$.
- $\mathcal{B}$ receives $\mathrm{Tr}(\alpha^a)$ from $\mathcal{A}$ and computes $S_b(\mathrm{Tr}(\alpha^a)) = (\mathrm{Tr}(\alpha^{(b-1)a}), \mathrm{Tr}(\alpha^{ab}), \mathrm{Tr}(\alpha^{(b+1)a}))$ and subsequently determines $\mathcal{K} = \mathrm{Tr}(\alpha^{ab})$.

Achieved Goals. The XTR cryptosystem achieves following main goals:

- Compact representation of operands over $\mathbb{F}_{p^2}$ and compression is achieved by a factor of 3.

- The advantage of DLP in extension field $\mathbb{F}_{p^6}$ is ensured.
- It is also resistant to SPA attacks in a similar fashion as mentioned in GH-PKC section.
- Trace based computation of group operations by means of symmetric polynomials. Therefore, only $\varphi(n)$ elements are required to represent an element of $\mathbb{F}_{p^n}$ in $\mathbb{F}_{p^r}$ such that $r < n,\ r|n$.
- Adaptation tor cryptographic protocols such as Diffie-Hellman key exchange, encryption/decryption and digital signature scheme etc.

V. Torus Based Cryptosystems

Torus based public key cryptosystem is yet another system that enjoys the extension field security and carry out group operations in prime or intermediate subfields. This system was proposed by Rubin and Silverberg in [12]. This system is an improvement over LUC-PKC [2], and GH-PKC [4], where as, its performance is comparable with XTR-PKC [7].

Algebraic Tori. An algebraic torus T over $\mathbb{F}_p$ is an algebraic group defined over $\mathbb{F}_p$ which of that defined on some extension field is isomorphic to $(\mathbb{G}_m)^d$, where $\mathbb{G}_m$ is the multiplicative group and d is dimension of T. For every n, an algebraic torus T_n can be defined with the property that $T_n(\mathbb{F}_p)$ consists of the elements α in $\mathbb{F}_{p^n}^*$ such that $\mathrm{Norm}(\alpha) = 1$ over $\mathbb{F}_{p^r}^*$ with $r|n$.

Definitions.

- ***Algebraic Variety.*** An algebraic variety is an object which can be defined in a purely algebraic way, starting from polynomials or more generally from finitely generated algebras over fields. The variety structure allows to express all elements and operations in terms of polynomials.
- ***Weil Restriction.*** The Weil restriction (also known as Restriction of scalars) is a functor which, for any finite extension of fields $\mathbb{F}_{p^n}/\mathbb{F}_p$ and any algebraic variety X over $\mathbb{F}_{p^n}$, produces another variety $\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}X$, defined over $\mathbb{F}_p$. This means Weil restriction decomposes a multiplicative group $\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}G_m$ as a product of algebraic tori, one for each divisor of n.

Fundamental Arithmetic for Torus Based Cryptography. As defined above the $\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}\mathbb{G}_m$ is a torus. As per the property of Weil restriction of scalars gives an isomorphism:

$$(\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}\mathbb{G}_m)(\mathbb{F}_p) \cong \mathbb{G}_m(\mathbb{F}_{p^n}) = \mathbb{F}_{p^n}^*,$$

and Norm map for $\mathbb{F}_p \subset \mathbb{F}_{p^r} \subset \mathbb{F}_{p^n}$:

$$\mathrm{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}\mathbb{G}_m \xrightarrow{N_{\mathbb{F}_{p^n}/\mathbb{F}_{p^r}}} \mathrm{Res}_{\mathbb{F}_{p^r}/\mathbb{F}_p}\mathbb{G}_m.$$

For $\mathbb{F}_p$ points we have:

$$T_n(\mathbb{F}_p) \cong \{\alpha \in \mathbb{F}_{p^n}^* : N_{\mathbb{F}_{p^n}/\mathbb{F}_{p^r}}(\alpha) = 1\},$$

whenever $\mathbb{F}_p \subset \mathbb{F}_{p^r} \subset \mathbb{F}_{p^n}$. The dimension of T_n is $\varphi(n)$. $T_n(\mathbb{F}_p)$ is a cyclic subgroup $\mathbb{G}_{p,n} \subseteq \mathbb{F}_{p^n}^*$ of order $\Phi_n(p)$, where Φ_n is the n-th cyclotomic polynomial. This implies that the security of cryptosystems based on the group T_n is that of $\mathbb{F}_{p^n}^*$.

Lemma 4, [12].

i). $T_n(\mathbb{F}_p) \cong \mathbb{G}_{p,n}$.

ii). $\#T_n(\mathbb{F}_p) = \Phi_n(p)$.

iii). If $\alpha \in T_n(\mathbb{F}_p)$ is an element of prime order not dividing n, then α does not lie in any proper subfield of $\mathbb{F}_{p^n}/F_p$.

Definitions

- *Rationality of Tori [12]:* Let T be an algebraic torus over $\mathbb{F}_p$ of dimension d. Then T is rational if and only if there is a birational map $\rho : T \to \mathbb{A}^d$ defined over $\mathbb{F}_p$.
- *Rational Parametrization of T [12]:* There are *Zariski* open subsets $W \subset T$ and $U \subset \mathbb{A}^d$, and rational functions $\rho_1, \ldots, \rho_d \in \mathbb{F}_p[x_1, \ldots, x_t]$ and $\psi_1, \ldots, \psi_t \in \mathbb{F}_p[y_1, \ldots, y_d]$ such that $\rho : W \to U$ and $\psi : U \to W$ are inverse isomorphisms. Such a map is a rational parametrization of T.

In this way a compact representation of the group $T(\mathbb{F}_p)$ by means of rational parametrization of torus T is obtained. Thus every element of $W(\mathbb{F}_p) \subset T(\mathbb{F}_p)$ is represented by d coordinates in $\mathbb{F}_q$.

Rational parametrization of T_2. To build a better understanding of rational parametrization for T_2 we proceed as follows. Let $\mathrm{char}(\mathbb{F}_p) \neq 2$ and $\mathbb{F}_{p^2} = \mathbb{F}_p(\gamma) : \gamma \in \mathbb{F}_{p^2}^*$ with $\omega = \gamma^2 \in \mathbb{F}_p^*$. Since $\gamma^p = -\gamma$, this implies

$$\begin{aligned} G_{p,2} &= \{a + b\gamma : a, b \in \mathbb{F}_p \text{ and } (a + b\gamma)^{p+1} = 1\}, \\ &= \{a + b\gamma : a, b \in \mathbb{F}_p \text{ and } (a^2 - \omega b^2) = 1\}. \end{aligned}$$

Define maps,

$$\rho : G_{p,2} - \{\pm 1\} \to \mathbb{F}_p^* \quad : \rho(c + d\gamma) = \frac{1+c}{d}$$

and

$$\psi : \mathbb{F}_p^* \to G_{p,2} \quad : \psi(a) = \frac{a+\gamma}{a-\gamma}.$$

Now $\psi(a) \cdot \psi(b) = \psi\left(\frac{ab+d}{a+b}\right)$. Therefore, all operations are carried out in $\mathbb{F}_p$ directly and multiplication in T_2 has been translated into the map $(a, b) \mapsto \frac{ab+d}{a+b}$ from $(\mathbb{F}_p^*)^2$ to $\mathbb{F}_p^*$.

Adaptation to Cryptographic Protocols [12]. As a demonstration, we provide analogous Diffie-Hellman key exchange protocol based on the concept of torus based cryptography.

- ***Pre-computations.*** The following are the pre-computations for Torus Based Cryptography:
  - Choose a prime power q and an integer n such that the torus T_n over $\mathbb{F}_q$ has an explicit parametrization, and a prime $\ell|\Phi_n(q)$.
  - Let $m = \varphi(n)$.
  - Fix birational map, $\rho : T_n(\mathbb{F}_q) \to \mathbb{F}_{q^m}$ and its inverse ψ such that $\rho \circ \psi = 1$.
  - Choose $\alpha \in T_n$ of order ℓ and let $g = \rho(\alpha) \in \mathbb{F}_{q^m}$.
  - The public is n, q, ρ, ψ, ℓ and either g or $\alpha = \psi(g)$.
- ***Key agreement scheme.***
  1. $\mathcal{A}$ chooses a random integer a in the range $1 \leq a \leq \ell - 1$ and computes $P_{\mathcal{A}} := \rho(\alpha^a) \in \mathbb{F}_{q^m}$ and send it to $\mathcal{B}$.
  2. $\mathcal{B}$ chooses a random integer b in the range $1 \leq b \leq \ell - 1$ and computes $P_{\mathcal{B}} := \rho(\alpha^b) \in \mathbb{F}_{q^m}$ and send it to $\mathcal{A}$.
  3. $\mathcal{A}$ computes $\rho(\psi(P_{\mathcal{B}})^a) \in \mathbb{F}_{q^m}$.
  4. $\mathcal{B}$ computes $\rho(\psi(P_{\mathcal{A}})^b) \in \mathbb{F}_{q^m}$.

Why it works? Since $\rho \circ \psi$ is the identity, we have $\rho(\psi(P_{\mathcal{B}})^a) = \rho(\alpha^{ab}) = \rho(\psi(P_{\mathcal{A}})^b)$.

Achieved Goals. Following are the main goals achieved by Torus based Cryptography:

- Data compression by rational parametrization of a torus.
- Representation of group elements of extension field $\mathbb{F}_{p^n}$ by only $\varphi(n)$ elements of $\mathbb{F}_p$.
- Torus based compression works where trace based representation has limitations [12].
- Multiplication is used as group operation instead of exponentiation. Therefore novel methods to speed up group operations are not required. This allows full functionality of group structure for variety of applications.
- The countermeasures against SPA is an open problem in this case.

VI. Conclusions

In this paper we surveyed LUC-PKC, GH-PKC, XTR-PKC and Torus based cryptosystems by going through underlying mathematical concepts and their adaptation to public key cryptosystems. These cryptosystems compress data by representing group elements in subfield of an extension field in such a way that DLP lies in extension field. In LUC-PKC, GH-PKC, and XTR-PKC novel methods for faster group operations are required, where as, in torus based cryptography conventional methods for multiplication can be employed. The group operations are carried out in prime or intermediate subfields whereas DLP lies in extension fields. As a summary, the LUC-PKC exploits Lucas functions in such a way that group operands lie in prime subfield $\mathbb{F}_p$ and DLP has to be solved in extension field $\mathbb{F}_{p^2}$. The GH-PKC carry out group operations in prime subfield and DLP in $\mathbb{F}_{p^3}$. The characteristic sequence of an LFSR is exploited for cryptographic protocol. The XTR-PKC carry out group operations in intermediate subfield $\mathbb{F}_{p^2}$ and DLP in $\mathbb{F}_{p^6}$. The trace function is used for data compression and cryptographic protocols are based on properties of trace function and symmetric polynomials over finite fields. The torus based cryptography employs rational parameterization of algebraic torus for cryptographic protocols. We also pointed out for the first time that the algorithm for computing k-th term of LFSR sequence in GH-PKC has additional characteristic to lure away simple power analysis attacks.

Acknowledgment

We would like to express my sincere gratitude to the anonymous referees for their valuable comments, to Professor Ersan Akyıldız for his diligent guidance and encouragement.

References

[1] W. Diffie, M.E. Hellman. New directions in cryptography, IEEE Trans. on Information Theory 22, 1976, 644-654.
[2] P. Smith, and M. Lennon. LUC: A new public key system, Proceedings of the 9th IFIP Symp. - IFIP/Sec 1993, 103-117.
[3] P. Smith, C. Skinner. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, Advances in Cryptology - Asiacrypt 1994, Lect. Notes in Comp. Sci. 917, Springer, Berlin, 1995, 357-364.
[4] G. Gong, L. Harn. Public-key cryptosystems based on cubic finite field extensions, IEEE trans on Information Theory 45, 1999, 2601-2605.
[5] G. Gong, L. Harn, and Huapeng Wu. The GH Public-key cryptosystem, SAC 2001, Lect. Notes in Comp. Sci. 2259, Springer, 2001, 284-300.
[6] G. Gong, A. Hassan, H. Wu, and A. Youssef. An Efficient Algorithm for Exponentiation in DH Key Exchange and DSA in Cubic Extension Fields, Research report at Faculty of Math., University of Waterloo, 2002.
[7] A. K. Lenstra, E. R. Verheul. The XTR public key system, Advances in Cryptology - CRYPTO 2000, Lect. Notes in Comp. Sci. 1880, Springer, Berlin, 2000, 1-19.
[8] A. K. Lenstra, E. R. Verheul. An overview of the XTR public key system, Publickey cryptography and computational number theory (Warsaw, 2000), de Gruyter, Berlin, 2001, 151-180.
[9] W. Bosma, J. Hutton, E. R. Verheul. Looking beyond XTR, Advances in Cryptology - Asiacrypt 2002, Lect. Notes in Comp. Sci. 2501, Springer, Berlin, 2002, 46-63.
[10] M. Stam and A. Lenstra. Speeding up XTR, Advances in Cryptology - ASIACRYPT 2001, Lect. Notes in Comp. Sci. 2248, Springer, 2001, 125-143.
[11] M. Shirase, D. Han, Y. Hibin, H. Kim, and T. Takagi. A more compact representation of XTR cryptosystem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E91-A:2843-2850, 2008.
[12] K. Rubin and A. Silverberg. Torus-based cryptography, Advances in Cryptology - CRYPTO 2003, Lecture Notes in Computer Science, 2729:349-365, 2003.
[13] R. Lidl and H. Niederreiter. Finite Fields, Addison-Wesley Publishing Company, 1983.