On the Uniformity of Distribution of the Elliptic Curve ElGamal Signature

Edwin El Mahassni and Igor Shparlinski

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail: eelmaha@ics.mq.edu.au, igor@ics.mq.edu.au

Communicated by Neal Koblitz

Received July 15, 2001; revised April 11, 2002; published online June 25, 2002

We show that, under some natural conditions, the pairs \((r, s)\) produced by the elliptic curve ElGamal signature scheme are uniformly distributed. In particular, this implies that values of \(r\) and \(s\) are not correlated. The result is based on some new estimates of exponential sums. For the ElGamal signature over a finite field, a similar result has been obtained by the second author.

Key Words: ElGamal signature scheme; elliptic curves; exponential sums; uniform distribution.

1. INTRODUCTION

Let \(p \geq 3\) be a prime and let \(g\) be a primitive root modulo \(p\). For an integer \(m \geq 2\), we also denote by \(\mathbb{Z}_m\) residue ring modulo \(m\) (which we identify with the set of integers \(\{0, \ldots, m-1\}\)) and by \(\mathbb{Z}_m^*\) the group of units of \(\mathbb{Z}_m\).

The ElGamal signature scheme can be described in the following way. Let \(\mathcal{M}\) be a finite set of messages to be signed and let \(h: \mathcal{M} \rightarrow \mathbb{Z}_{p-1}\) be an arbitrary function, usually called a hash-function. We assume that the primitive root \(g\) is publicly known. The signer fixes a certain element \(x \in \mathbb{Z}_{p-1}\) which is the secret key known only to the signer and makes the value \(A \equiv g^x \pmod{p}\) publicly known. Finally, for an integer \(k \in \mathbb{Z}_{p-1}^*\) called a nonce and a message \(\mu \in \mathcal{M}\) we define the functions \(r(k)\) and \(s(k, \mu)\) by

---

1To whom correspondence should be addressed.
the conditions
\[ r(k) \equiv g^k \pmod{p}, \quad 0 \leq r(k) \leq p - 1, \]
\[ s(k, \mu) \equiv k^{-1}(h(\mu) + xr(k)) \pmod{p - 1}, \quad 0 \leq s(k, \mu) \leq p - 2, \]
and call the pair \((r(k), s(k, \mu))\) the \textit{ElGamal signature} of the message \(\mu\) with nonce \(k\), see [6, 12]. It has been shown in [10] that the distribution of pairs \((r(k), s(k, \mu))\) is asymptotically uniform in the rectangle \([0, p - 1] \times [0, p - 2]\).

The elliptic curve \text{ElGamal} signature is the elliptic curve analogue of the above algorithm (see [4]). ECDSA uses an elliptic curve \(E\) over \(\mathbb{F}_p\). If \(M = |E(\mathbb{F}_p)|\) denotes the number of rational points over \(\mathbb{F}_p\), it is well known that
\[ |M - p - 1| \leq 2p^{1/2} \]
and that \(E(\mathbb{F}_p)\) together with the point at infinity \(\mathcal{O}\) form an Abelian group, see [11].

Let \(N\) be a divisor of \(M\) and let \(G \in E(\mathbb{F}_p)\) be a fixed point of prime order \(N\), that is, \(NG = \mathcal{O}\), where \(\mathcal{O}\) is the point at infinity. Both \(G\) and \(N\) are \textit{publicly} known. For a point \(Q \in E(\mathbb{F}_p)\), we denote by \(x(Q)\), \(0 \leq x(Q) \leq p - 1\), the first component of \(Q = (x, y)\) in the affine model of \(E\). The signer’s secret key is again an element \(a \in \mathbb{Z}_N^*\).

To sign a message \(\mu \in \mathcal{M}\), one chooses a random integer \(k \in \mathbb{Z}_N^*\) usually called the \textit{nonce}, and which must be kept secret. One then defines the following two integers:
\[ \rho(k) = x(kG), \]
\[ \sigma(k, \mu) \equiv k^{-1}(h(\mu) + x\rho(k)) \pmod{N}, \quad 0 \leq \sigma(k, \mu) \leq N - 1, \]
where now \(h : \mathcal{M} \to \mathbb{Z}_N\). The pair \((\rho(k), \sigma(k, \mu))\) is the \textit{elliptic curve ElGamal signature} of the message \(\mu\) with a nonce \(k\).

In this paper, we obtain the elliptic curve analogue of the result of [10] and show that the pairs \((\rho(k), \sigma(k, \mu))\) are uniformly distributed in the rectangle \([0, p - 1] \times [0, N - 1]\). We remark that even studying only the first component \(\rho(k)\) is not trivial and require several algebraic geometry tools [5].

Although the uniformity of distribution results of [10] and this paper do not have any immediate implications for the security of the corresponding cryptographic constructions, they still provide some intuitive motivation for such conclusions. In particular, in each of the above cases the inverse statement (about non-uniformity of distribution) would be disastrous for the corresponding construction.

On the other hand, surprisingly enough, certain uniformity of distribution properties could be a tool for an attack as well. For example, a statement about the uniform distribution of the elements \((k)(k, \mu)^{-1}\), corresponding to
the pairs \(((k), (k, \mu))\) produced by the Digital Signature Algorithm and by its modifications (including the elliptic curve version) has been used in [3, 7, 8] to give a rigorous proof of a certain weakness in these schemes. We recall that the Digital Signature Algorithm is a variant of the ElGamal signature with \(p - 1\) replaced by a prime divisor \(q\) of \(p - 1\), see [6, 12]. Also, \((k)\) is now the result of the double reduction of \(g^k\), firstly modulo \(p\) and then modulo \(q\). This double reduction erases the arithmetic structure of exponential function and makes the studying of the pairs \(((k)(k, \mu))\) much more complicated. In particular, despite that, as we have mentioned, the uniformity of distribution results have been proved for the ratios \((k)(k, \mu)\), it is still an open problem to establish such a result for the pairs \(((k)(k, \mu))\) themselves.

Our result is based on a new upper bound of exponential sums with linear combinations of \(r(k)\) and \(s(k, \mu)\) which can be of independent interest.

Throughout the paper the implied constants in symbols ‘\(O\)’ and \(\ll\) may occasionally, where obvious, depend on the small positive parameter \(\epsilon\) and are absolute otherwise (we recall that \(U = O(V)\) and \(U \ll V\) are equivalent). They all are effective and can be explicitly evaluated.

2. EXPONENTIAL SUMS

For an integer \(m \geq 2\), we define \(e_m(z) = \exp(2\pi iz/m)\) and consider exponential sums

\[
S(a, b) = \sum_{k \in \mathbb{Z}^*_N} \sum_{\mu \equiv \#} e_p(a \rho(k))e_N(b \sigma(k, \mu)).
\]

Here we obtain some results about exponential sums with \(\rho(k)\) and \(\sigma(k, \mu)\) which can be of independent interest.

We need the following estimate which is Corollary 1 of [5] (where we take into account that \(\deg x = 2\) in the notation of that paper).

**LEMMA 1.** Let \(Q \in \mathbb{E}\) be a point of order \(t\). Then, the bound

\[
\max_{\gcd(a, p) = 1} \left| \sum_{k=1}^t e_p(ax(kQ)) \right| \leq 4p^{1/2}
\]

holds.

We also need the following well-known basic identity (see [3, Chap. 3, Problem 11.a]). For any integers \(u\) and \(m \geq 2\),

\[
\sum_{c=0}^{m-1} e_m(cu) = \begin{cases} 
0 & \text{if } u \not\equiv 0 \pmod{m}, \\
1 & \text{if } u \equiv 0 \pmod{m}.
\end{cases}
\]

(1)

First of all, we consider the sums \(S(a, b)\) with \(b = 0\).
Let \( \nu(m) \) denote the number of distinct prime divisors of the integer \( m \geq 2 \).

**Lemma 2.** For any \( a \in \mathbb{Z} p^* \) the bound

\[
|S(a, 0)| \leq |\mathcal{N}| 2^{\nu(p-1)+2} p^{1/2}
\]

holds.

**Proof.** Let \( \mu(m) \) denote the Mobius function. We recall that \( \mu(1) = 1, \mu(m) = 0 \) if \( m \geq 2 \) is not square-free and \( \mu(m) = (-1)^{\nu(m)} \) otherwise. Using the Mobius function \( \mu(d) \) over divisors of \( N \) to detect the co-primality condition, we obtain (see [13, Chap. 2, Sect. 3.d])

\[
S(a, 0) = |\mathcal{N}| \sum_{d|N} \mu(d) \sum_{k=1}^{N/d} e_p(ax(kG))
= \sum_{d|N} \mu(d) \sum_{k=1}^{N/d} e_p(ax(kdG)).
\]

Because \( dG \) is of multiplicative order \( N/d \), we can apply Lemma 1 to get

\[
|S(a, 0)| \leq 4|\mathcal{N}| p^{1/2} \sum_{d|N} |\mu(d)|.
\]

Noting that

\[
\sum_{d|N} \mu(d) = 2^{\nu(N)},
\]

we obtain the desired statement. ■

For a hash function \( h: \mathcal{N} \rightarrow \mathbb{Z}_N \), we also denote by \( W \) the number of pairs \( (\mu_1, \mu_2) \in \mathcal{N}^2 \) with \( h(\mu_1) = h(\mu_2) \). Thus, \( W/|\mathcal{N}|^2 \) is the probability of a collision and our results are non-trivial under a reasonable assumption that this probability is of order of magnitude close to \( 1/N \).

Now we can state the following:

**Lemma 3.** For any \( a \in \mathbb{Z}_p \) and \( b \in \mathbb{N} \) with \( b \neq 0 \), the bound

\[
|S(a, b)| \leq (d \varphi(N)NW)^{1/2}
\]

holds, where \( d = \gcd(b, N) \).

**Proof.** We have

\[
|S(a, b)| \leq \left| \sum_{k \in \mathbb{Z}_N^*} e_p(ap(k))e_N(bzk^{-1} \rho(k)) \sum_{\mu \in \mathcal{N}} e_N(bk^{-1}h(\mu)) \right|
\leq \sum_{k \in \mathbb{Z}_N^*} \left| \sum_{\mu \in \mathcal{N}} e_N(bk^{-1}h(\mu)) \right| = \sum_{k \in \mathbb{Z}_N^*} \left| \sum_{\mu \in \mathcal{N}} e_N(bkh(\mu)) \right|.
\]
Applying the Cauchy inequality and extending the summation to all \(k \in \mathbb{Z}_N\), we obtain

\[
|S(a, b)|^2 \leq \varphi(N) \sum_{k \in \mathbb{Z}_N} \left| \sum_{\mu \in \mathcal{M}} e_N(bk(h(\mu))) \right|^2
= \varphi(N) \sum_{\mu_1, \mu_2 \in \mathcal{M}} \sum_{k \in \mathbb{Z}_N} e_N(bk(h(\mu_1) - h(\mu_2))).
\]

From Lemma 1, we conclude that

\[
|S(a, b)|^2 \leq \varphi(N)NV,
\]

(2)

where \(V\) is the number of solutions of the congruence

\[
b(h(\mu_1) - h(\mu_2)) \equiv 0 \pmod{N}, \quad \mu_1, \mu_2 \in \mathcal{M},
\]

or equivalently of the congruence

\[
h(\mu_1) \equiv h(\mu_2) \pmod{N/d}, \quad \mu_1, \mu_2 \in \mathcal{M}.
\]

Therefore,

\[
V \leq \sum_{j=0}^{d-1} U_j,
\]

where \(U_j\) is the number of solutions of the congruence

\[
h(\mu_1) \equiv h(\mu_2) + jN/d \pmod{N}, \quad \mu_1, \mu_2 \in \mathcal{M}.
\]

In particular, \(U_0 = W\). Using Lemma 1, we derive

\[
U_j = \sum_{\mu_1, \mu_2 \in \mathcal{M}} \frac{1}{N} \sum_{c=0}^{N-1} e_N(c(h(\mu_1) - h(\mu_2) - jN/d))
= \frac{1}{N} \sum_{c=0}^{N-1} e_N(-cjN/d) \sum_{\mu_1, \mu_2 \in \mathcal{M}} e_N(c(h(\mu_1) - h(\mu_2)))
= \frac{1}{N} \sum_{c=0}^{N-1} e_N(-cjN/d) \left| \sum_{\mu \in \mathcal{M}} e_N(ch(\mu)) \right|^2
\leq \frac{1}{N} \sum_{c=0}^{N-1} \left| \sum_{\mu \in \mathcal{M}} e_N(ch(\mu)) \right|^2 = U_0 = W.
\]

Therefore \(V \leq dW\) and from (2) we obtain the desired result. \(\blacksquare\)
3. DISTRIBUTION OF SIGNATURES

Here we obtain our main result. Given a set \( S \) of \( T \) points \((u_j, v_j) \in [0, 1]^2, j = 1, \ldots, T, \) of the unit square, we define the discrepancy \( D(S) \) of this set as

\[
D(S) = \sup_B \frac{|A_S(B)|}{T} - |B|,
\]

where the supremum is taken over all boxes \( B = [x, y] \times [\gamma, \delta] \subseteq [0, 1]^2, |B| = (\beta - \alpha)(\delta - \gamma) \) and \( A_S(B) \) is the number of points of this set which hit \( B \).

According to a standard principle, we can bound the discrepancy \( D(S) \) by bounding the corresponding exponential sums. For arbitrary sets such a relation is given by the Erdos–Turan–Koksma inequality (see [2, Theorem 1.21]) which we present in the following form.

For an integer \( a \) we define \( \% \) as

\[
\% = \max \{ |a|, 1 \}.
\]

**Lemma 4.** For any integer \( L \geq 1 \), the bound

\[
D(S) \leq \frac{1}{L} + \frac{1}{T} \sum_{0 < |a| + |b| < L} \frac{1}{a b} \sum_{j=1}^T \exp(2\pi i(u_j + b v_j))
\]

holds.

Let \( \omega \) be the probability of collision of the hash function \( h \), that is,

\[
\omega = \frac{W}{|\mathcal{M}|^2}.
\]

**Theorem 5.** For any \( \varepsilon > 0 \), for the discrepancy \( D(S) \) of the set of \( \varphi(N)|\mathcal{M}| \) points

\[
S = \left\{ \left( \frac{\rho(k)}{p}, \frac{\sigma(k, \mu)}{N} \right) : k \in \mathbb{Z}_N^*, \ \mu \in \mathcal{M} \right\},
\]

the bound \( D(S) = O(\omega^{1/2} N^{\varepsilon}) \) holds.

**Proof.** Select \( T = \varphi(N)|\mathcal{M}| \) and \( L = p \) in Lemma 4. If \( b = 0 \), then \( a \neq 0 \) and we apply Lemma 2. For \( b \neq 0 \), we apply Lemma 3, to get

\[
D(S) \leq \frac{1}{p} + \frac{1}{\varphi(N)|\mathcal{M}|} \left( \sum_{0 < |a| \leq p} \frac{S(a, 0)}{a} \right)
\]

\[
+ \sum_{d|N} \sum_{0 \leq |a| < p} \sum_{\substack{0 < |b| < p \ \gcd(b, N) = d}} \frac{S(a, b)}{a b}
\]
\[
\leq \frac{1}{p} + \frac{2^{(p-1)} p^{1/2} \log p}{\varphi(N)} + \frac{(NW)^{1/2}}{\varphi(N)^{1/2} |\mathcal{H}|} 
\sum_{d | N} d^{1/2} \sum_{0 \leq |a| \leq p-1} \sum_{0 < |b| < p/d} \frac{1}{\bar{a} \bar{b}}.
\]

Now, the first term never dominates, and substituting \(b = cd\), we obtain
\[
D(\mathcal{S}) \leq \frac{2^{(p-1)} p^{1/2} \log p}{\varphi(N)} + \frac{(NW)^{1/2}}{\varphi(N)^{1/2} |\mathcal{H}|} 
\sum_{d | N} \frac{1}{d^{1/2}} \sum_{0 \leq |a| < p} \sum_{0 < |c| < p/d} \frac{1}{\bar{a} \bar{c}}
\]
(because \(N \leq 2p\)), where \(\tau(m)\) denotes the number of positive integer divisors of \(m \geq 2\). We recall that
\[
\frac{m}{\varphi(m)} = O(\log \log(m + 1)) \quad \text{and} \quad \log \tau(m) = O\left(\frac{\log m}{\log \log(m + 1)}\right),
\]
see [9, Theorems 5.1 and 5.2]. Also, from the inequality \(v(m)! \leq m\), we derive
\[
v(m) = O\left(\frac{\log m}{\log \log(m + 1)}\right).
\]

Therefore, for any \(\varepsilon > 0\)
\[
D(\mathcal{S}) = O(N^{-1/2+\varepsilon} + \omega^{1/2} p^{\varepsilon}).
\]  
(3)

We remark that \(\omega \geq 1/N\). Indeed, let \(H(\lambda)\) be the number of messages \(\mu \in \mathcal{H}\) with \(h(\mu) = \lambda\). Then,
\[
\sum_{\lambda \in \mathbb{Z}_N} H(\lambda) = |\mathcal{H}| \quad \text{and} \quad \sum_{\lambda \in \mathbb{Z}_N} H(\lambda)^2 = W.
\]

Thus, from the Cauchy inequality we derive
\[
|\mathcal{H}|^2 = \left(\sum_{\lambda \in \mathbb{Z}_N} H(\lambda)\right)^2 \leq N \sum_{\lambda \in \mathbb{Z}_N} H(\lambda)^2 = NW.
\]

Hence, the first term in (3) never dominates, and the result follows. ■

We remark that for any practically useful hash function \(\omega = O(N^{-1+\varepsilon})\) (in fact, one should even expect \(\omega \sim 1/N\)), the bound of Theorem 5 becomes of the form \(D(\mathcal{S}) = O(N^{-1/2+\varepsilon})\).

Finally, we note that unfortunately our analysis cannot be extended to the elliptic curve analogue of the digital signature scheme, see [1].
As usual $\mathbb{F}_p$ and $\mathbb{Z}/p\mathbb{Z}$ denote fields of $p$ elements and the residue ring modulo $p - 1$, respectively. We assume that $\mathbb{F}_p$ consists of elements $\{0, 1, \ldots, p - 1\}$ and $\mathbb{Z}/p\mathbb{Z}$ consists of elements $\{0, 1, \ldots, p - 2\}$. We also denote by $\mathbb{Z}/p\mathbb{Z}^*$ the group of units of $\mathbb{Z}/p\mathbb{Z}$.

For integers $s$ and $m \geq 1$ we denote by $\lfloor s_m \rfloor$ the remainder of $s$ on division by $m$. We also use $\log z$ to denote the binary logarithm of $z > 0$.

REFERENCES