MATHEMATICS OF COMPUTATION
Volume 70, Number 234, Pages 801–808
S 0025-5718(00)01274-6
Article electronically published on June 12, 2000

ON THE UNIFORMITY OF DISTRIBUTION OF THE RSA PAIRS

IGOR E. SHPARLINSKI

Abstract. Let $m = pl$ be a product of two distinct primes p and l. We show that for almost all exponents e with $\gcd(e, \varphi(m)) = 1$ the RSA pairs (x, x^e) are uniformly distributed modulo m when x runs through

- the group of units $\mathbb{Z}_m^*$ modulo m (that is, as in the classical RSA scheme);
- the set of k-products $x = a_{i_1} \cdots a_{i_k}$, $1 \le i_1 < \cdots < i_k \le n$, where $a_1, \cdots, a_n \in \mathbb{Z}_m^*$ are selected at random (that is, as in the recently introduced RSA scheme with precomputation).

These results are based on some new bounds of exponential sums.

1. Introduction

Let $m = pl$ be a product of two distinct primes p and l, and let $\mathcal{E}_m$ be the set of integers e, $1 \le e \le \varphi(m)$, with $\gcd(e, \varphi(m)) = 1$, where $\varphi(N)$ is the Euler function. In this paper we consider the distribution modulo m of the *RSA pairs* (x, x^e). First of all we show that for almost all exponents $e \in \mathcal{E}_m$ this distribution is exponentially close to the uniform distribution, when $x \in \mathcal{U}_m$ runs through the group of units $\mathcal{U}_m = \mathbb{Z}_m^*$ modulo m. This result is an analogue of the results of [5, 6] about the uniformity of distribution of the *Diffie–Hellman triples*. Then we also consider the case when x runs through all possible k-products of the form

$$x = \prod_{j=1}^{k} a_{i_j}, \qquad 1 \le i_1 < \cdots < i_k \le n,$$

for some fixed $a_1, \dots, a_n \in \mathcal{U}_m$. We show that for almost all n-element sequences $a_1, \dots, a_n \in \mathcal{U}_m$, the corresponding pairs (x, x^e) are uniformly distributed modulo m. Such pairs have been considered in [4] and provide a promising way to speed up the RSA encryption with precomputation.

Such uniformity of distribution results, although they do not have immediate security implications, still provide some useful information about pseudorandomness of the mapping $x \to x^e$, see [16]. In particular, it would be disastrous to discover that these pairs are not uniformly distributed; in this case one could guess their left-most bits with higher than average probability. Several other results about the uniformity of distribution and other properties of some pseudorandom generators of cryptographic interest are given in [9, 10, 11, 13, 24] for the *power generator*, which includes the *RSA generator* and the *Blum–Blum–Shub generator*

Received by the editor June 22, 1999.
2000 *Mathematics Subject Classification.* Primary 11T71, 94A60; Secondary 11K38, 11T23.
Key words and phrases. RSA cryptosystem, uniform distribution, precomputation, exponential sums.

(see [3, 7, 15, 17, 26]), and in [2, 12, 22, 23, 25] for the *Naor–Reingold generator* (see [18]).

As in [5, 6] our main tool is exponential sums. In fact our results directly depend on some estimates of these papers.

Throughout the paper all implicit constants in symbols "O" are absolute.

2. Notation and auxiliary results

Given a set $\mathcal{M}$ of N points $(u_\nu, v_\nu) \in [0,1]^2$, $\nu = 1, \ldots, N$, of the unit square, we define the *discrepancy* $D(\mathcal{M})$ of this set as

$$D(\mathcal{M}) = \sup_B \left| \frac{A_N(B)}{N} - \mu(B) \right|,$$

where the supremum is taken over all boxes $B = [\alpha, \beta] \times [\gamma, \delta] \in [0,1]^2$, $\mu(B) = (\beta - \alpha)(\delta - \gamma)$ and $A_N(B)$ is the number of points of this set which hit B.

According to a standard principle, we can bound the discrepancy $D(\mathcal{M})$ by bounding the corresponding exponential sums. For arbitrary sets such a relation is given by the *Erdös–Turán–Koksma inequality* (see Theorem 1.21 of [8]) which we present in the following implicit form.

For an integer a we define $\overline{a} = \max\{|a|, 1\}$.

Lemma 1. *There exists an absolute constant $C > 0$ such that for any integer $L \geq 1$ the bound*

$$D(\mathcal{M}) \leq C \left(\frac{1}{L} + \frac{1}{N} \sum_{0<|r|+|s|<L} \frac{1}{\overline{r}\,\overline{s}} \left| \sum_{\nu=1}^{N} \exp\left(2\pi i (r u_\nu + s v_\nu)\right) \right| \right)$$

holds.

Let us define

$$\mathbf{e}_d(z) = \exp(2\pi i z/d).$$

The following lemma shows how to reduce general exponential sums to exponential sums with prime power denominators (for example, see Problem 12.d to Chapter 3 of [27]).

Lemma 2. *Let $m = m_1 m_2$, where $m_1 \geq m_2 \geq 2$ and $\gcd(m_1, m_2) = 1$, and let k_1, k_2 be such that*

$$k_1 m_2 \equiv 1 \pmod{m_1} \qquad \textit{and} \qquad k_2 m_1 \equiv 1 \pmod{m_2}.$$

Then for any polynomial $f(x)$ with integer coefficients

$$\sum_{x \in \mathcal{U}_m} \mathbf{e}_m(f(x)) = \sum_{x_1 \in \mathcal{U}_{m_1}} \mathbf{e}_{m_1}\left(k_1 f(x_1)\right) \sum_{x_2 \in \mathcal{U}_{m_2}} \mathbf{e}_{m_2}\left(k_2 f(x_2)\right),$$

where $\mathcal{U}_m$, $\mathcal{U}_{m_1}$ and $\mathcal{U}_{m_2}$ are the groups of units modulo m, m_1 and m_2, respectively.

Indeed, this statement follows from Problem 12.d to Chapter 3 of [27] if one remarks that

$$k_1 m_2 + k_2 m_1 \equiv 1 \pmod{m}.$$

We also need an upper bound of certain double sums which is essentially the main result of [5].

Lemma 3. *For any prime number p the bound*

$$\max_{\gcd(r,s,p)=1} \sum_{e=1}^{p-1} \left| \sum_{x=1}^{p-1} \mathbf{e}_p\left(rx + sx^e\right) \right|^4 = O(p^{14/3})$$

holds.

Proof. Let g be a primitive root modulo p. Then

$$\sum_{y=1}^{p-1} \left| \sum_{x=1}^{p-1} \mathbf{e}_p\left(rx + sx^y\right) \right|^4 = \sum_{y=1}^{p-1} \left| \sum_{x=1}^{p-1} \mathbf{e}_p\left(rg^x + sg^{xy}\right) \right|^4 .$$

The last sum is estimated as $O(p^{14/3})$ (uniformly over all r and s with $\gcd(r,s,p) = 1$) in the proof of Theorem 8 of [5]. □

We define exponential sums

$$W(r,s) = \sum_{e \in \mathcal{E}_m} \left| \sum_{x \in \mathcal{U}_m} \mathbf{e}_m\left(rx + sx^e\right) \right| .$$

Lemma 4. *Let $m = pl$, where p and l are two distinct primes. Then the bound*

$$\max_{\gcd(r,s,m)=1} W(r,s) = O\left(m^{23/12}\right)$$

holds.

Proof. Lemma 2 implies that there exist some integer numbers k_p and k_l with $\gcd(p, k_p) = \gcd(l, k_l) = 1$ and such that

$$\sum_{x \in \mathcal{U}_m} \mathbf{e}_m\left(rx + sx^e\right) = \sum_{x_1=1}^{p-1} \mathbf{e}_p\left(k_p\left(rx_1 + sx_1^e\right)\right) \sum_{x_2=1}^{l-1} \mathbf{e}_l\left(k_l\left(rx_2 + sx_2^e\right)\right).$$

From the previous equation and the Cauchy inequality we derive

$$\begin{aligned} W(r,s) &\leq \sum_{e \in \mathcal{E}_m} \left| \sum_{x_1=1}^{p-1} \mathbf{e}_p\left(k_p\left(rx_1 + sx_1^e\right)\right) \right| \left| \sum_{x_2=1}^{l-1} \mathbf{e}_l\left(k_l\left(rx_2 + sx_2^e\right)\right) \right| \\ &\leq \varphi(m)^{1/2} \left(\sum_{e \in \mathcal{E}_m} \left| \sum_{x_1=1}^{p-1} \mathbf{e}_p\left(k_p\left(rx_1 + sx_1^e\right)\right) \right|^4 \right)^{1/4} \\ &\qquad \times \left(\sum_{e \in \mathcal{E}_m} \left| \sum_{x_2=1}^{l-1} \mathbf{e}_l\left(k_l\left(rx_2 + sx_2^e\right)\right) \right|^4 \right)^{1/4} \\ &\leq \varphi(m)^{1/2} \left(\frac{\varphi(m)}{p-1} \sum_{e=1}^{p-1} \left| \sum_{x_1=1}^{p-1} \mathbf{e}_p\left(k_p\left(rx_1 + sx_1^e\right)\right) \right|^4 \right)^{1/4} \\ &\qquad \times \left(\frac{\varphi(m)}{l-1} \sum_{e=1}^{l-1} \left| \sum_{x_2=1}^{l-1} \mathbf{e}_l\left(k_l\left(rx_2 + sx_2^e\right)\right) \right|^4 \right)^{1/4} . \end{aligned}$$

Using the bound of Lemma 3, we obtain the desired result. □

We also remark that the same (and even somewhat simpler) considerations imply the bounds

$$\max_{\gcd(r,s,m)=p} W(r,s) = O\left(m^2 l^{-1/12}\right) \tag{1}$$

and

$$\max_{\gcd(r,s,m)=l} W(r,s) = O\left(m^2 p^{-1/12}\right). \tag{2}$$

Let $1 \le k \le n$ be integers. Denote by $\mathcal{F}_{n,k}$ the set of binary vectors $\mathbf{u} = (u_1, \dots, u_n) \in \{0,1\}^n$ of *Hamming weight* k, that is

$$\mathcal{F}_{n,k} = \{\mathbf{u} = (u_1, \dots, u_n) \in \{0,1\}^n \mid u_1 + \ldots + u_n = k\}.$$

Thus

$$|\mathcal{F}_{n,k}| = \binom{n}{k}.$$

For a given n-dimensional vector $\mathbf{a} = (a_1, \dots, a_n) \in \mathcal{U}_m^n$ and a binary vector $\mathbf{u} = (u_1, \dots, u_n) \in \{0,1\}^n$ we put

$$x_{\mathbf{a}}(\mathbf{u}) = \prod_{j=1}^{n} a_j^{u_j}$$

and define

$$S_{k,n}(r,s) = \sum_{\mathbf{a}\in\mathcal{U}_m^n} \sum_{e\in\mathcal{E}_m} \left| \sum_{\mathbf{u}\in\mathcal{F}_{n,k}} \mathbf{e}_m\left(r x_{\mathbf{a}}(\mathbf{u}) + s x_{\mathbf{a}}^e(\mathbf{u})\right)\right|.$$

Lemma 5. *Let $m = pl$, where p and l are two distinct primes. Then the bound*

$$\max_{\gcd(r,s,m)=1} S_{k,n}(r,s) = O\left(m|\mathcal{U}_m|^n \left(|\mathcal{F}_{n,k}|^{1/2} + |\mathcal{F}_{n,k}| m^{-1/12}\right)\right)$$

holds.

Proof. Using the Cauchy inequality and changing the order of summation, we derive

$$\begin{aligned} S_{k,n}(r,s)^2 & \\ &\le |\mathcal{U}_m|^n |\mathcal{E}_m| \sum_{\mathbf{a}\in\mathcal{U}_m^n} \sum_{e\in\mathcal{E}_m} \left| \sum_{\mathbf{u}\in\mathcal{F}_{n,k}} \mathbf{e}_m\left(r x_{\mathbf{a}}(\mathbf{u}) + s x_{\mathbf{a}}^e(\mathbf{u})\right)\right|^2 \\ &= |\mathcal{U}_m|^n |\mathcal{E}_m| \sum_{\mathbf{u},\mathbf{v}\in\mathcal{F}_{n,k}} \sum_{\mathbf{a}\in\mathcal{U}_m^n} \sum_{e\in\mathcal{E}_m} \mathbf{e}_m\left(r x_{\mathbf{a}}(\mathbf{u}) + s x_{\mathbf{a}}^e(\mathbf{u}) - r x_{\mathbf{a}}(\mathbf{v}) - s x_{\mathbf{a}}^e(\mathbf{v})\right). \end{aligned}$$

The contribution to this sum of each pair with $\mathbf{u} = \mathbf{v}$ is $|\mathcal{U}_m|^n |\mathcal{E}_m|$. For each pair $\mathbf{u}, \mathbf{v} \in \mathcal{F}_{n,k}$ with $\mathbf{u} \ne \mathbf{v}$ we can find i and j, $1 \le i < j \le n$, with $u_i = v_j = 1$ and $u_j = v_i = 0$. Without loss of generality we may assume that $i = 1$, $j = 2$. In this case $x_{\mathbf{a}}(\mathbf{u}) = A a_1$ and $x_{\mathbf{a}}(\mathbf{v}) = B a_2$, where A and B do not depend on a_1 and a_2. Therefore

$$\begin{aligned} &\sum_{\mathbf{a}\in\mathcal{U}_m^{n-2}} \sum_{e\in\mathcal{E}_m} \mathbf{e}_m\left(r x_{\mathbf{a}}(\mathbf{u}) + s x_{\mathbf{a}}^e(\mathbf{u}) - r x_{\mathbf{a}}(\mathbf{v}) - s x_{\mathbf{a}}^e(\mathbf{v})\right) \\ &\quad = \sum_{a_3,\dots,a_n\in\mathcal{U}_m^n} \sum_{e\in\mathcal{E}_m} \sum_{a_1\in\mathcal{U}_m} \mathbf{e}_m\left(r A a_1^e + s A^e a_1^e\right) \sum_{a_2\in\mathcal{U}_m} \mathbf{e}_m\left(-r B a_2 - s B^e a_2^e\right), \end{aligned}$$

where A and B depend only on $\mathbf{u}$, $\mathbf{v}$ and $a_3, \dots, a_n$. Furthermore, by the Cauchy inequality we obtain

$$\left| \sum_{e \in \mathcal{E}_m} \sum_{a_1 \in \mathcal{U}_m} \mathbf{e}_m \left(rAa_1^e + sA^e a_1^e \right) \sum_{a_2 \in \mathcal{U}_m} \mathbf{e}_m \left(-rBa_2 - sB^e a_2^e \right) \right|^2$$
$$\leq \sum_{e \in \mathcal{E}_m} \left| \sum_{a_1 \in \mathcal{U}_m} \mathbf{e}_m \left(rAa_1^e + sA^e a_1^e \right) \right|^2 \times \sum_{e \in \mathcal{E}_m} \left| \sum_{a_2 \in \mathcal{U}_m} \mathbf{e}_m \left(rBa_2 + sB^e a_2^e \right) \right|^2 .$$

Taking into account that $A, B \in \mathcal{U}_m$, as in the proof of Lemma 4 we obtain that each factor in the above expression is $O(m^{17/6})$. We have $|\mathcal{U}_m| = \varphi(m) = (p-1)(l-1) \geq 0.25m$. Therefore $m^{17/6} = O(|\mathcal{U}_m|^2 m^{5/6})$ and the desired result follows. □

As after Lemma 4, we also remark that

(3) $$\max_{\gcd(r,s,m)=p} S_{k,n}(r,s) = O\left(m |\mathcal{U}_m|^n \left(|\mathcal{F}_{n,k}|^{1/2} + |\mathcal{F}_{n,k}| l^{-1/12} \right) \right)$$

and

(4) $$\max_{\gcd(r,s,m)=l} S_{k,n}(r,s) = O\left(m |\mathcal{U}_m|^n \left(|\mathcal{F}_{n,k}|^{1/2} + |\mathcal{F}_{n,k}| p^{-1/12} \right) \right).$$

Finally we recall that there exists an absolute constant $c > 0$ such that the Euler function $\varphi(N)$ satisfies the inequality

(5) $$\varphi(N) \geq c \frac{N}{\log \log N}$$

for any integer $N \geq 2$, (for example, see Problem 9.g to Chapter 2 of [27]).

3. Distribution of the RSA pairs

Now we are prepared to formulate our main results.

Denote by D_e the discrepancy of the pairs of fractional parts

$$\left(\left\{ \frac{x}{m} \right\}, \left\{ \frac{x^e}{m} \right\} \right), \qquad x \in \mathcal{U}_m.$$

Theorem 6. *Let $m = pl$, where p and l are two distinct primes. Then the bound*

$$\frac{1}{|\mathcal{E}_m|} \sum_{e \in \mathcal{E}_m} D_e = O(m^{-1/12} \log^2 m \log \log m)$$

holds.

Proof. Select $L = m$. Combining Lemma 1 with Lemma 4 and the bounds (1) and (2), we derive

$$\begin{aligned}
\sum_{e\in\mathcal{E}_m} D_e
&= O\left(1 + \sum_{\substack{0<|r|+|s|<m\\ \gcd(r,s,m)=1}} \frac{m^{11/12}}{\overline{r}\,\overline{s}} + \sum_{\substack{0<|r|+|s|<m\\ \gcd(r,s,m)=p}} \frac{ml^{-1/12}}{\overline{r}\,\overline{s}} + \sum_{\substack{0<|r|+|s|<m\\ \gcd(r,s,m)=l}} \frac{mp^{-1/12}}{\overline{r}\,\overline{s}}\right)\\
&= O\left(1 + m^{11/12}\log^2 m + mp^{-1}l^{-1/12}\log^2 l + ml^{-1}p^{-1/12}\log^2 p\right)\\
&= O\left(m^{11/12}\log^2 m\right).
\end{aligned}$$

Recalling that $|\mathcal{E}_m| = \varphi(\varphi(m))$ and taking into account the bound (5) and the inequality $\varphi(m) \ge 0.25m$, we obtain the desired result. $\square$

In particular, we see that for any $\delta > 0$ for a random exponent e chosen uniformly from $\mathcal{E}_m$ with probability at least $1 - \delta$ the bound

$$D_e = O\left(\delta^{-1} m^{-1/12} \log^2 m \log\log m\right)$$

holds.

Given integers $1 \le k \le n$ and an n-dimensional vector $\mathbf{a} = (a_1, \dots, a_n) \in \mathcal{U}_m^n$, denote by $D_{\mathbf{a},k,e}$ the discrepancy of the pairs of fractional parts

$$\left(\left\{\frac{x_{\mathbf{a}}(\mathbf{u})}{m}\right\}, \left\{\frac{x_{\mathbf{a}}^e(\mathbf{u})}{m}\right\}\right), \qquad \mathbf{u} = (u_1, \dots, u_n) \in \mathcal{F}_{n,k},$$

where

$$x_{\mathbf{a}}(\mathbf{u}) = \prod_{j=1}^{n} a_j^{u_j}.$$

Using Lemma 5 and the bounds (3) and (4), in the same way as we have used Lemma 4 and the bounds (1) and (2) in the proof of Theorem 6, we obtain the following statement.

Theorem 7. *Let $m = pl$, where p and l are two distinct primes. Then the bound*

$$\frac{1}{|\mathcal{U}_m|^n |\mathcal{E}_m|} \sum_{\mathbf{a}\in\mathcal{U}_m^n} \sum_{e\in\mathcal{E}_m} D_{\mathbf{a},k,e} = O\left(\left(|\mathcal{F}_{n,k}|^{-1/2} + m^{-1/12}\right) \log^2 m \log\log m\right)$$

holds.

In particular, we see that for any $\delta > 0$ for a random vector $\mathbf{a}$ and a random exponent e chosen uniformly and independently from $\mathcal{U}_m^n$ and $\mathcal{E}_m$ with probability at least $1 - \delta$ the bound

$$D_{\mathbf{a},k,e} = O\left(\delta^{-1}\left(|\mathcal{F}_{n,k}|^{-1/2} + m^{-1/12}\right) \log^2 m \log\log m\right)$$

holds.

4. Remarks

Let p be a prime and let g be an element of a finite field $\mathbb{F}_p$ of p elements of multiplicative order t.

As we have mentioned, an analogue of Theorem 6 for Diffie–Hellman triples (g^x, g^y, g^{xy}) has been obtained in [5, 6] (provided that t is large enough). On the other hand, obtaining an analogue of Theorem 7 is an interesting open problem which is related to the Diffie–Hellman scheme with precomputation. In particular, similar questions have been briefly addressed in [20, 21]. More specifically, we are interested in establishing the uniformity of distribution of the following pairs of fractional parts

$$\left(\left\{\frac{z_{\mathbf{b}}(\mathbf{u})}{t}\right\}, \left\{\frac{g^{z_{\mathbf{b}}(\mathbf{u})}}{p}\right\}\right), \qquad \mathbf{u} = (u_1, \ldots , u_n) \in \mathcal{F}_{n,k},$$

where

$$z_{\mathbf{b}}(\mathbf{u}) = \sum_{j=1}^{n} b_j u_j,$$

for a random n-dimensional vector $\mathbf{b} = (b_1, \ldots , b_n) \in \mathbb{Z}_t^n$ over the residue ring modulo t.

Even studying the distribution of only the first component, that is, just vectors $z_{\mathbf{b}}(\mathbf{u})$, $\mathbf{u} \in \mathcal{F}_{n,k}$, would be of interest, see [20, 21]. We remark that several uniformity of distribution results about the vectors $z_{\mathbf{b}}(\mathbf{u})$, when $\mathbf{u}$ runs through all n-dimensional binary vectors, are known [1, 2, 12, 14, 19, 21, 25] and have some cryptographic applications.

Acknowledgment

The author would like to thank Phong Nguyen for a number of fruitful discussions.

References

[1] M. Ajtai, 'Generating hard instances of lattice problems', *Electronic Colloq. on Comp. Compl.*, Univ. of Trier, **TR96-007** (1996), 1–29. CMP 97:06

[2] W. Banks, F. Griffin, D. Lieman and I. E. Shparlinski, 'Non-linear complexity of the Naor-Reingold pseudo-random function', *Proc. the 2nd Intern. Conf. on Information Security and Cryptology*, Seoul, 1999, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, (to appear).

[3] L. Blum, M. Blum and M. Shub, 'A simple unpredictable pseudo-random number generator', *SIAM J. Comp.*, **15** (1986), 364–383. MR **87k:**65007

[4] V. Boyko, M. Peinado and R. Venkatesan, 'Speeding up discrete log and factoring based schemes via precomputations', *Proc. of Eurocrypt'98*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1403** (1998), 221–234.

[5] R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, 'On the statistical properties of Diffie–Hellman distributions', *Israel J. Math.*, (to appear).

[6] R. Canetti, J. B. Friedlander and I. E. Shparlinski, 'On certain exponential sums and the distribution of Diffie–Hellman triples', *J. London Math. Soc.*, (1999), 799–812. CMP 99:17

[7] T. W. Cusick, C. Ding and A. Renvall, *Stream Ciphers and Number Theory*, Elsevier, Amsterdam, 1998. MR **99h:**94045

[8] M. Drmota and R.F. Tichy, *Sequences, Discrepancies and Applications*, Springer-Verlag, Berlin, 1997. MR **98j:**11057

[9] J. B. Friedlander, D. Lieman and I. E. Shparlinski, 'On the distribution of the RSA generator', *Proc. Intern. Conf. on Sequences and Their Applications (SETA'98), Singapore*, Springer-Verlag, London, 1999, 205–212.

[10] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, 'Period of the power generator and small values of Carmichael's function', *Math. Comp.*, (to appear).

[11] J. B. Friedlander and I. E. Shparlinski, 'On the distribution of the power generator', *Math. Comp.*, (to appear).

[12] F. Griffin and I. E. Shparlinski, 'On the linear complexity of the Naor-Reingold pseudo-random function', *Proc. 2nd Intern. Conf. on Information and Communication Security*, Sydney, 1999, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1726** (1999), 301–308.

[13] F. Griffin and I. E. Shparlinski, 'On the linear complexity profile of the power generator', Trans. IEEE Inform. Theory (to appear).

[14] R. Impagliazzo and M. Naor, 'Efficient cryptographic schemes provably as secure as subset sum', *J. Cryptology*, **9** (1996), 199–216. MR **97k:**94030

[15] J. C. Lagarias, 'Pseudorandom number generators in cryptography and number theory', *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **42** (1990), 115–143. MR **92f:**11109

[16] M. Luby, *Pseudorandomness and Cryptographic Applications*, Princeton Univ. Press, Princeton, 1996. MR **97b:**94024

[17] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Cryptography*, CRC Press, Boca Raton, FL, 1996. MR **99g:**94015

[18] M. Naor and O. Reingold, 'Number-theoretic constructions of efficient pseudo-random functions', *Proc. 38th IEEE Symp. on Foundations of Comp. Sci.*, 1997, 458–467.

[19] M. Naor and O. Reingold, 'Synthesizers and their application to the parallel construction of pseudo-random functions', *J. Comp. and Sys. Sci.*, **58** (1999), 336–375. CMP 99:15

[20] P. Nguyen, I. E. Shparlinski and J. Stern, 'Distribution of modular sums and the security of the server aided exponentiation', *Preprint*, 2000, 1–16.

[21] P. Nguyen and J. Stern, 'The hardness of the hidden subset sum problem and its cryptographic implications', *Proc. CRYPTO'99*, Santa Barbara, 1999, Springer-Verlag, Berlin, **1666** (1999), 31–46.

[22] I. E. Shparlinski, 'On the uniformity of distribution of the Naor-Reingold pseudo-random number function', *Finite Fields and Their Appl.* (to appear).

[23] I. E. Shparlinski, 'On the Naor-Reingold pseudo-random number generator from elliptic curves', *Appl. Algebra in Engin., Commun. and Computing* (to appear).

[24] I. E. Shparlinski, 'On the linear complexity of the power generator', *Designs, Codes and Cryptography*, (to appear).

[25] I. E. Shparlinski and J. H. Silverman, 'Linear complexity of the Naor–Reingold pseudo-random number function from elliptic curves', *Preprint*, 1999, 1–14.

[26] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, FL, 1995. MR **96k:**94015

[27] I. M. Vinogradov, *Elements of Number Theory*, Dover Publ., NY, 1954. MR **19:**933e

Department of Computing, Macquarie University, Sydney, New South Wales 2109, Australia

E-mail address: `igor@ics.mq.edu.au`