Electronic Colloquium on Computational Complexity - Reports Series 1997 - available via:
ECCC
TR97-018
FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem*

Oded Goldreich† Shafi Goldwasser‡ Shai Halevi§

May 8, 1997

Abstract

Following Ajtai's lead, Ajtai and Dwork have recently introduced a public-key encryption scheme which is secure under the assumption that a certain computational problem on lattices is hard on the worst-case. Their encryption method may cause decryption errors, though with small probability (i.e., inversely proportional to the security parameter).

In this note we modify the encryption method of Ajtai and Dwork so that the legitimate receiver always recovers the message sent. That is, we make the Ajtai-Dwork Cryptosystem error-free.

Keywords: Public-key Encryption Schemes, Computational Problems in Lattices.

*This research was supported by DARPA grant DABT63-96-C-0018.

†Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel. E-mail: oded@wisdom.weizmann.ac.il. Currently visiting LCS, MIT.

‡MIT – Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139. E-mail shafi@theory.lcs.mit.edu.

§MIT – Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139. E-mail shaih@theory.lcs.mit.edu.

1 Introduction

A major project of our field is to find concrete hard problems which can be used for "doing Cryptography" (e.g., constructing encryption schemes, message-authentication codes and digital signatures). As current state of the art in Complexity Theory does not allow to prove that such (cryptographically-useful) problems are hard, one has to rely on unproven and yet plausible assumptions. It is thus important to have as many alternative/unrelated assumption as possible, so that Cryptography can be based on any one of them. So far there are very few alternatives; and so Ajtai's work [1], which suggests a new domain out of which adequately-hard problems can be found, marks an important day for Cryptography.

In particular, Ajtai constructed a one-way function based on the assumption that Lattice Reduction is hard in the worst-case. Following his lead, Ajtai and Dwork have recently introduced a public-key encryption scheme which is secure, provided that the following (worst-case complexity) assumption holds [2]:

Assumption ISVP (Infeasibility of Shortest Vector Problem): There exists no polynomial-time algorithm, which given an arbitrary basis for an n-dimensional lattice, having a "unique poly(n)-shortest vector", finds the shortest (non-zero) vector in the lattice. By having a *unique* poly(n)-*shortest vector* we mean that any vector of length at most poly(n) times bigger than the shortest vector is an integer multiple of the shortest vector.

The encryption method of Ajtai and Dwork [2], has a non-zero decryption-error probability. Specifically, when working with security parameter n, the ciphertext of the message bit '1' is decrypted to be a '0' with probability $\frac{1}{n}$. (The ciphertext corresponding to the message bit '0' is always decrypted as '0'.)

In this note we modify the encryption method of Ajtai and Dwork so that every message is always decrypted correctly. Thus, we obtain a error-free encryption scheme which is secure under the same assumption used by Ajtai and Dwork.

2 The Encryption Scheme

In this section we recall the construction of Ajtai and Dwork [2] and describe our modification of it. In our scheme we set the common parameters as they do, and use almost the same key-generation algorithm. The modification is merely in the encryption of the bit '1' and respectively in the decryption algorithm.

2.1 The Ajtai-Dwork Construction

We start by recalling the Ajtai-Dwork construction. To simplify the exposition we present the scheme in terms of real numbers with infinite precision. In realty, following [2], one uses approximations (i.e., to n-bit binary expansions).

Common Parameters. Given security parameter n, we let $m = n^3$, $R \stackrel{\text{def}}{=} 2^{O(n \log n)}$, and $r \stackrel{\text{def}}{=} n^{-3}$. We denote by B (for big) the n-dimensional sphere of radius R, and by S (for small) the n-dimensional sphere of radius r.

Private-key. Given security parameter n, the private-key is a uniformly chosen vector in the n-dimensional unit sphere. We denote this vector by u.

Public-key.

1. select $a_1, \ldots, a_m$ uniformly from the set of vectors $\{x \in B : \langle x, u \rangle \in \mathcal{Z}\}$, where $\langle x, y \rangle$ denotes the inner-product of the vectors x and y, and $\mathcal{Z}$ denotes the set of integers.
2. For $i = 1, \ldots, m$, select $\delta_{i,1}, \ldots, \delta_{i,n}$ uniformly in S, and set $\delta_i = \sum_{j=1}^{n} \delta_{i,j}$. (Thus, each of the δ_i's is a random variable which is almost "concentrated uniformly" among the vectors of length $\sqrt{n} \cdot r$.)
3. Set $v_i = a_i + \delta_i$, for $i = 1, \ldots, m$.
4. Let i_0 be the smallest i for which the width of the parallelepiped spanned by $v_{i+1}, \ldots, v_{i+n}$ is at least $n^{-2} \cdot R$. (By [2], with overwhelmingly high probability i_0 exists and is smaller than $m/2$.) For $j = 1, \ldots, n$, let $w_j \stackrel{\text{def}}{=} v_{i_0+j}$, and denote by $P(w_1, \ldots, w_n)$ the parallelepiped spanned by $w_1, \ldots, w_n$.

The public-key consists of the sequence of vectors $(v_1, \ldots, v_m)$ and the integer $i_0 \in \{1, \ldots, m\}$.

Encryption. To encrypt a '0', we uniformly select $b_1, \ldots, b_m \in \{0, 1\}^m$, and reduce the vector $v' = \sum_{i=1}^{m} b_i \cdot v_i$ modulo the parallelepiped $P(w_1, \ldots, w_n)$. By *reducing a vector v' modulo P*, we mean obtaining a vector v in P so that $v' = v + \sum_{i=1}^{n} c_i \cdot w_i$, where the c_i are all integers. The vector v is the ciphertext which correspond to the bit '0'.

To encrypt a '1' we uniformly select a vector v in the parallelepiped P. This vector is the ciphertext which correspond to the bit '1'.

Decryption. Given a ciphertext, c, and the private-key u, we compute $\tau = \langle c, u \rangle$. We decrypt the ciphertext as a '0' if τ is within $1/n$ of some integer and decrypt it as a '1' otherwise.

Decryption errors. In [2], Ajtai and Dwork have shown that if c is an encryption of '0', then the fractional part of τ is always less than $1/n$ in absolute value, and that if c is an encryption '1' then the fractional part of τ is distributed almost uniformly in $(-\frac{1}{2}, +\frac{1}{2}]$. Thus, an encryption of '0' will always be decrypted as '0', and an encryption of '1' has a probability of $1/n$ to be decrypted as '0'.

2.2 An Error-free Construction

We proceed now to describe our modification which eliminates the decryption errors from the construction above. In this modified scheme, just like in the original Ajtai-Dwork scheme, encrypting a '0' results in a ciphertext c such that $\langle c, u \rangle$ is close to an integer. However, in our scheme we also make sure that encrypting a '1' results in a ciphertext c such that $\langle c, u \rangle$ is far from any integer. The modified scheme is as follows:

Common Parameters and private-key. The common parameters n, m, R, r, B and S, and the private key u, are set in exactly the same manner as in the original scheme.

Public-key *(modified).*

1. The vectors $v_1, \cdots, v_m$ are chosen in exactly the same manner as in the original scheme. Namely, we first select at random the vector $a_1, \cdots, a_m \in B$ s.t. $\langle a_i, u \rangle \in \mathcal{Z}$, then choose the "small vectors" $\delta_1, \cdots, \delta_m$ and set $v_i = a_i + \delta_i$.

2. The integer i_0 us set just like in the original scheme, as the first index for which the width of the parallelepiped $P(v_{i_0+1}, \cdots, v_{i_0+n})$ is $\geq n^{-2} \cdot R$.

3. In addition, we pick i_1 uniformly at random from all the indices i for which $\langle a_i, u \rangle \in 2\mathcal{Z} + 1$. That is, i_1 is selected so that $\langle a_{i_1}, u \rangle$ is an odd integer. We note that such an index exists with probability $\approx 1 - 2^{-m}$.

The public-key consists of the sequence of vectors $(v_1, \ldots, v_m)$ and the integers $i_0, i_1 \in \{1, \ldots, m\}$.

Encryption *(modified).* We encrypt a '0' just like in the original scheme, by uniformly selecting $b_1, \ldots, b_m \in \{0,1\}^m$, and reducing the vector $\sum_{i=1}^m b_i \cdot v_i$ modulo the parallelepiped $P(w_1, \ldots, w_n)$. The difference is in the encryption of a '1'. We do that by uniformly selecting $b_1, \ldots, b_m \in \{0,1\}^m$, and reducing the vector $\frac{1}{2}v_{i_1} + \sum_{i=1}^m b_i \cdot v_i$ modulo the parallelepiped $P(w_1, \ldots, w_n)$.

Decryption *(modified)*: Given a ciphertext, c, and the private-key u, we compute $\tau = \langle c, u \rangle$. We decrypt the ciphertext as a '0' if τ is within $1/4$ of some integer and decrypt it as a '1' otherwise.

In contrast to the encryption scheme in [2], we can show that in our scheme there is no decryption error. Furthermore, by the setting of parameters in [2] we have:

Proposition 1 (error-free decryption): *For every $\sigma \in \{0,1\}$, every choice of the private and public keys, and every choice of b_i's by the encryption algorithm, the ciphertext, c, satisfies $\langle c, u \rangle \in \mathcal{Z} + \frac{\sigma}{2} \pm \frac{2}{n}$.*

Proof: The case of $\sigma = 0$ was proven in [2]. Actually, the non-integer part was bounded there by $1/n$. The case $\sigma = 1$ follows by letting $c' = c - \frac{\sigma}{2} \cdot v_{i_1}$ and observing that

$$\begin{aligned} \langle c, u \rangle &\equiv \langle 0.5 \cdot v_{i_1}, u \rangle + \langle c', u \rangle \pmod 1 \\ &\equiv (0.5 \pm \frac{1}{n^2}) \pm \frac{1}{n} \pmod 1 \end{aligned}$$

(Using the fact that $\langle a_{i_1}, u \rangle$ is an odd integer.) The claim follows. ■

3 Security of the Modified Scheme

To prove the security of the modified scheme, we start by invoking the main result of Ajtai and Dwork [2]:

Theorem 2 *[2, Thm 7.1]: Under Assumption ISVP, it is infeasible to distinguish the encryption of $\sigma = 0$ from a uniformly distributed point in $P = P(w_1, \ldots, w_n)$, when given $(v_1, \ldots, v_m)$ and i_0 as auxiliary inputs. (We stress that $(v_1, \ldots, v_m), i_0$ and the encryption of '0' are distributed as described above.)*

Note that this theorem establishes the security (cf., [3]) of the encryption scheme of Ajtai and Dwork [2], since in that scheme $\sigma = 1$ is encrypted as a uniformly chosen point in P. However, to establish the security of our (modified) encryption scheme (under the same assumption), we need to prove

Theorem 3 (security): *Under Assumption ISVP, it is infeasible to distinguish the encryption of $\sigma = 0$ from the encryption of $\sigma = 1$, when given $(v_1, \ldots, v_m)$ and i_0, i_1 as auxiliary inputs. (We stress that $(v_1, \ldots, v_m), i_0, i_1$ and the encryptions are distributed as described above.)*

Let us denote by $E_e(\sigma)$ the probabilistic encryption of σ using the encryption key $e \stackrel{\text{def}}{=} ((v_1, \ldots, v_m), i_0, i_1)$. Assuming ISVP, we will show that for both $\sigma \in \{0, 1\}$, it is infeasible to distinguish $(e, E_e(\sigma))$ from (e, Π), where Π is uniformly distributed in $P = P(v_{i_0+1}, \ldots, v_{i_0+n})$.

First we show that this holds for $\sigma = 0$. Note that this claim is not identical to Theorem 2, as here the distinguisher is given i_1 as extra information. Still, Theorem 2 does imply the following

Lemma 3.1 *Under Assumption ISVP, it is infeasible to distinguish $(e, E_e(0))$ from (e, Π), where $e \stackrel{\text{def}}{=} ((v_1, \ldots, v_m), i_0, i_1)$ is selected as above and Π is uniformly distributed in $P = P(v_{i_0+1}, \ldots, v_{i_0+n})$.*

Proof: Suppose towards the contradiction that there exists a distinguisher, D, of running-time $t(n)$ and distinguishing gap $\epsilon(n)$ (between $(e, E_e(0))$ and (e, Π) as in the claim). We construct a new distinguisher, D', as follows

input: $((v_1, \ldots, v_m), i_0)$ and p.

preprocessing: Using D, we find an index j which approximately maximizes the distinguishing gap of D on inputs of the form $(e_j, \cdot)$, where $e_j = ((v_1, \ldots, v_m), i_0, j)$. This is done by estimating, for every $j = 1, \ldots, m$, the value of

$$\text{Prob}(D(e_j, E_{e_j}(0)) = 1) - \text{Prob}(D(e_j, \Pi) = 1)$$

where the probability is taken over the internal coin tosses of both the encryption algorithm (i.e., choice of b_i's) and D. Invoking D for $\text{poly}(n)/\epsilon(n)^2$ times we may obtain, with overwhelmingly high probability, an approximation of the above upto $\epsilon(n)/4$. Let $\tau \in \{\pm 1\}$ denote the sign of the approximated difference for the best j.

decision: Using j and τ, found in the preprocessing, we invoke D on input (e, p). Let $\sigma \in \{\pm 1\}$ denote the output of D. Then D' outputs $\tau \cdot \sigma$.

Clearly, D' has running time $\text{poly}(n, t(n), \epsilon(n)^{-1})$, which is polynomial in n whenever $t(n)/\epsilon(n)$ is. It is easy to see that

$$|\text{Prob}(D'(e', E_e(0)) = 1) - \text{Prob}(D'(e', \Pi) = 1)| > \epsilon(n)/2$$

where $e \stackrel{\text{def}}{=} ((v_1, \ldots, v_m), i_0, i_1)$ is selected as above and $e' \stackrel{\text{def}}{=} ((v_1, \ldots, v_m), i_0)$. Thus, we have a distinguisher violating the conclusion of Theorem 2, and so contradiction follows. ■

Using Lemma 3.1, we easily derive

Lemma 3.2 *Under Assumption ISVP, it is infeasible to distinguish $(e, E_e(1))$ from (e, Π), where e and Π are as in Lemma 3.1.*

Proof: Suppose towards the contradiction that there exists a distinguisher, D, of running-time $t(n)$ and distinguishing gap $\epsilon(n)$ (between $(e, E_e(1))$ and (e, Π) as in the claim). We construct a new distinguisher, D', as follows

input: $e = ((v_1, \ldots, v_m), i_0, i_1)$ and p.

processing: Let p' denote the result of reducing $p - \frac{1}{2}v_{i_1}$ modulo $P = P(v_{i_0+1}, \ldots, v_{i_0+n})$. Algorithm D' computes p', and outputs $D(p')$.

Observe that $E_e(0)$ and $E_e(1) - \frac{1}{2}v_{i_1}$ (reduced mod P) are identically distributed. Similarly, Π and $\Pi - \frac{1}{2}v_{i_1}$ (reduced mod P) are identically distributed. Thus, D' distinguishes $(e, E_e(0))$ from (e, Π), in contradiction to the claim of Lemma 3.1. The current lemma follows. ■

Combining Lemmas 3.1 and 3.2, we have established Theorem 3. ■

Comment 1 – An alternative proof of Theorem 3. The security of the [2]-encryption scheme is established via a sequence of reductions, the first of which transforms a distinguisher of (ciphertext,public-key) pairs into a distinguisher of public-keys from sequences of m uniformly distributed points in the big sphere B. One can easily verify that this argument holds also for distinguishers of encryptions under our modified scheme. ■

Comment 2 – Added security. Recall from Proposition 1 that if the ciphertext c is an encryption of the bit σ, then it satisfies $\langle c, u \rangle \in \mathcal{Z} + \frac{\sigma}{2} \pm \frac{2}{n}$, so there is a "gap" between encryptions of '0'a and '1's. We can take advantage of this gap, by picking larger "errors" δ_i during the key-generation process. Indeed, it can be shown that the scheme remains error-free even if we pick each δ_i as a sum of n vectors which are uniformly selected in a sphere of radius n^{-2} (rather than n^{-3} as above).

This "larger errors" can add to the security of the system. Indeed, going through the proof in [2] one can verify that this factor of n in the error size is translated into a corresponding factor in the $poly(n)$-uniqueness of Assumption ISVP. Specifically, the security proof in [2] assumes the difficulty of finding the shortest non-zero vector in a lattice with a "unique n^8-shortest vector". Instead, when using these larger errors, *and without any change in the other parameters in the proof,* one can show that it is sufficient to assume difficulty of finding the shortest non-zero vector in lattices with a "unique n^7-shortest vector".

References

[1] Miklos Ajtai. Generating Hard Instances of Lattice Problems. In *28th ACM Symposium on Theory of Computing*, pages 99–108, Philadelphia, 1996.

[2] Miklos Ajtai and Cynthia Dwork. A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence, *ECCC*, TR96-065, Dec. 1996. To appear in *28th ACM Symposium on Theory of Computing*, 1997.

[3] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption, *JCSS*, Vol. 28, No. 2, pages 270–299, 1984.