

Date: Sat, 26 Jan 2002 19:05:19 +0900 (JST)
Message-Id: <200201261005.TAA13210@castle.isl.ntt.co.jp>
From: kotetsu@isl.ntt.co.jp (Tetsutaro KOBAYASHI)
To: cryptrec-comment@ipa.go.jp
cc: kotetsu@sucaba.isl.ntt.co.jp, okamoto@sucaba.isl.ntt.co.jp,
fujisaki@sucaba.isl.ntt.co.jp, oguro@sucaba.isl.ntt.co.jp
Subject: [comment on EPOC-2, PSEC-KEM]

NTT の小林と申します。

本件は Cryptrec2001 の応募直後に、cryptrec-call@ipa.go.jp に
報告済みですが、念のため cryptrec-comment@ipa.go.jp にも出しておきます。

Cryptrec2001 に提出した EPOC-2 および PSEC-KEM のテストベクトルに
一部誤りが見つっております。

修正版のテストベクトルは、
<http://www.nttmcl.com/sec/>
の EPOC-2 および PSEC-KEM の項目にあります。

よろしくお願ひします。