GMI
白皮书

初步修订 Rev. 1.0
5/23/2016

上海兆芯集成电路有限公司

版权声明:

免责声明:

本产品非针对国防、军事、或航空等应用目的所设计。上海兆芯集成电路有限公司未授权或暗示授权任何相关的专利, 专利权与许可。上海兆芯集成电路有限公司不对本文件及本文档中描述的产品作出任何隐含或其它的保证。上海兆芯集成电路有限公司对本文档中的任何错误概不承担责任。此外，上海兆芯集成电路有限公司对使用或误用本文件信息，以及由于使用本文件可能产生的任何专利侵权概不承担任何责任。本文档中的信息和产品规格可能随时修改，恕不另行通知，且无义务通知任何人此类修改。

公司地址:

上海
Shanghai

上海兆芯集成电路有限公司
上海市浦东新区金科路 2860 号
（201203）
Tel: +86-021-6061-1988

北京
Beijing

北京兆芯电子科技有限公司
北京市海淀区中关村东路 1 号院 7 号楼
威盛中国芯大厦
(100084)
Tel: +86-021-6061-1988

修订纪录

文件版本	日期	修订叙述	编辑
1.0	5/20/16	Preliminary initial release	DA

目录

1. 概述

信息技术的快速发展为人类社会带来了深刻的变革。随着计算机技术的快速发展，我国在电子银行、电子商务和电子政务等方面的广泛应用，使计算机安全问题已经深入到国家的政治、经济、文化和国防建设等各个领域，遍布现代信息化社会的工作和生活每个层面。我们的世界从没有像今天这样关注知识产权、个人身份信息以及其他敏感信息的保护问题。

国密即国家密码局认定的国产密码算法，即商用密码。商用密码的应用领域十分广泛，主要用于对不涉及国家秘密内容但又具有敏感性的内部信息、行政事务信息、经济信息等进行加密保护。比如：商用密码可用于企业门禁管理、企业内部的各类敏感信息的传输加密、存储加密，防止非法第三方获取信息内容；也可用于各种安全认证、 网上银行、数字签名等。

SM3 密码杂凑算法是为满足电子认证服务系统等应用需求，国家密码管理局于 2010 年 12 月 17 日发布的。该标准适用于商用密码应用中的数字签名和验证、消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。

SM4 分组密码算法，原名 SMS4，国家密码管理局于 2012 年 3 月 21 日发布，该标准适用于密码应用中使用分组密码的需求。

GMI 是一套由兆芯自主研发的算法指令集。

其中，GMI 最大的特色是，通过调用兆芯 CPU 私有指令，实现硬件支持国密 SM3 算法和国密 SM4 算法。通过使用 GMI 算法加速引擎，我们将获得比软件实现更快的性能。

2. 带给客户的价值

OpenSSL 是一个开放源代码的 SSL 协议、密码算法库以及应用程序的产品实现，可以免费用于任何商业或非商业的目的。由于采用 C 语言开发，OpenSSL 的源代码库具有良好的跨平台性能，支持 Linux、Unix、Windows、Mac 和 VMS 等多种平台。目前，OpenSSL 在市场上已经获得广泛的应用，许多类型的软件中的安全部分都使用了 OpenSSL 的库，如 VOIP 的 OpenH323 协议、Apache 服务器、Linux 安全模块等等。

使用 GMI SM3/SM4 指令实现的 Library 已经被集成到 OpenSSL，任何运行于 ZX-CPU 平台的 API 将能够通过 OpenSSL 的 EVP 方法调用到 GMI SM3/SM4 指令。

2.1 GMI SM3 的价值

SM3 摘要算法在加密过程中不需要使用密钥进行加密，因此不存在密钥管理与分发的问题。但是由于摘要算法运算机密计算量比较客观，应用中往往需要考虑加密数据量对性能的影响，因此对加密数据量有一定的限制。从上面的评测结果可以看到，随着摘要数据量的增大，GMI 的性能优势相对于 intel I7 CPU 愈发明显，在大数据量下性能可以是 intel I7 的 2 倍以上，因此**使用 GMI 来实现 SM3 加密产品可以实现在更短的时间内实现更大数据量的摘要加密。**

2.2 GMI SM4 的价值

SM4 分组密码算法往往用在大数据加密的场景下，因此在实际应用中其数据量往往非常大。通过上面的性能分析对比可以看到使用 GMI 后的加密性能均优于 Intel I7 性能。**在业界最常用的 ECB 和 CBC 模式下在最常应用的大数据加密情况下，性能提升更加明显。当数据量大于 1K Byte 后，其性能可以是 Intel I7 性能的 3 倍以上。**

3. 应用模型

3.1 SM3 的应用模型

SM3 可以应用于需要计算杂凑值（摘要）的场合。特别是以下三种场合：

- 文件校验

比较熟悉的文件校验算法有奇偶校验和 CRC 校验，但是这两种校验并没有抗数据篡改的能力。而 SM3 应用于文件校验，不仅能够保证数据在传输过程中未出现错误，更能保证文件在传输过程中未被恶意篡改。一个很典型的应用是 ftp 服务，用户可以用此算法来保证多次断点续传，特别是从镜像站点下载的文件的正确性。其应用方法是，将得到的文件用 SM3 算法计算出杂凑值（摘要），与站点上提供的文件的 SM3 摘要做比对，当二者一致，则认为获得了正确的文件。

- 数字签名和认证

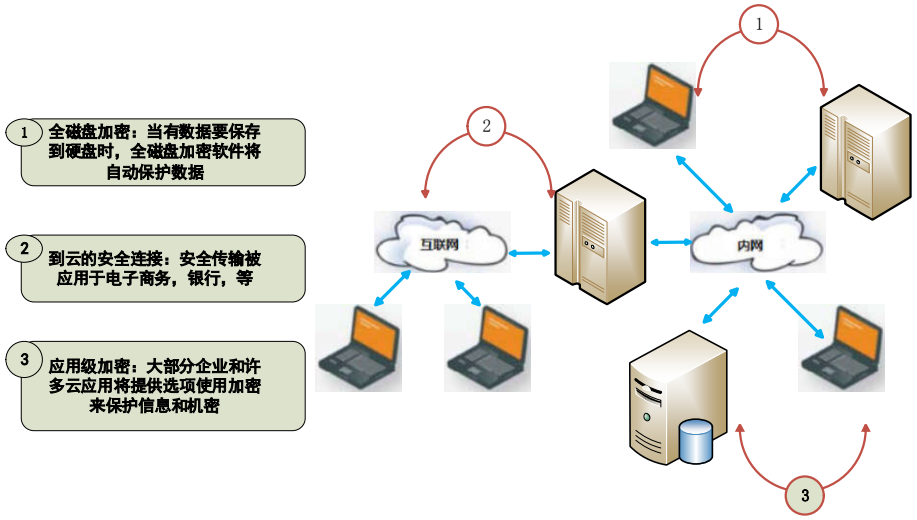
国密 SM2 数字签名算法中，指定使用 SM3 作为摘要算法。

- 身份认证

常常利用“挑战-认证”模式来保证传输信道是可信的。首先 A 方向 B 方发送随机串（“挑战”），B 方将该随机串和自己的口令字一起进行 SM3 运算后，返还结果给 A，A 也会将该随机串和已知的口令字进行 SM3 运算，并将结果与从 B 处得到的结果相比较（“认证”），如相同，则可在认为 B 方拥有该口令字，即认为挑战通过，可被认证（这种认证的方式中，双方需拥有相同的口令字）。

3.2 SM4 的应用模型

典型的 SM4 应用模型如图示：



- **全磁盘加密**

随着信息的电子化，保存在计算机设备上的个人信息，商业信息等敏感数据的安全性越来越受到人们的重视。对于个人客户来说，个人的密码，照片，视频等一般都属于敏感信息。一旦这些信息面临泄露，个人隐私受到巨大威胁时，比如存储有这些信息的计算机设备丢失或不得不请他人维修时，常使用全磁盘加密技术来解决这些问题。对于企业客户或组织来说，很多重要的商业机密文件或政策文件一旦泄露就会给企业和组织带来巨大损失。从一些调查来看，企业或组织的计算机设备一般不会被盗窃，而其数据泄露的时机主要存在于处理旧设备或对计算机设备进行维修时。全磁盘加密技术可以让企业或组织在处理旧设备时或对设备进行维修时，即使面对敏感信息泄露的威胁也无后顾之忧。

目前常见的全磁盘加密产品采用的加密算法多为 AES 算法，在中国国内的一些实际应用中存在政策风险。为了满足这类实际应用的需求，中国的操作系统厂商或应用软件厂商会推出使用国密 SM4 的全磁盘加密功能的操作系统或应用软件。而在在这些实现中，全磁盘加密功能一般都是实时的加解密数据，这对加解密过程的性能要求是很高的，此时可以使用 GMI 实现国密 SM4 以替代传统的纯软件实现，从而不仅能防止算法被篡改，还能提高运算速度。

- **云应用**

构建可信云平台时，当云中有对数据做加密和解密需求的时候，可以使用 GMI 实现国密 SM4 替代传统的纯软件实现，从而不仅能防止算法被篡改，还能提高运算速度。

- **应用级加密**

大部分企业和云应用将提供多种选项来对安全信息使用加密技术。比如数据库，应用服务器，中间件，邮件服务器以及虚拟机管理程序等都会用到 SM4 加密技术。此时都可以通过 GMI SM4 硬件实现来替代传统的软件实现。