

示例目的

演示使用SM3加密算法demo。

支持型号列表：

支持型号	AT32L021 系列
------	-------------

1 快速使用方法

1.1 硬件资源

1) AT-START开发板 (AT32L021)

1.2 软件资源

1) SourceCode

- sm3_demo源程序

- AT32驱动库

2) Doc

- SC0126_AT32L021_SM3_DEMO

注意：所有project都是基于keil 5而建立，若用户需要在其他编译环境上使用，请参考BSP中templates工程中各种编译环境（例如IAR6/7, keil 4/5）进行简单修改即可。

1.3 示例使用

软件使用：

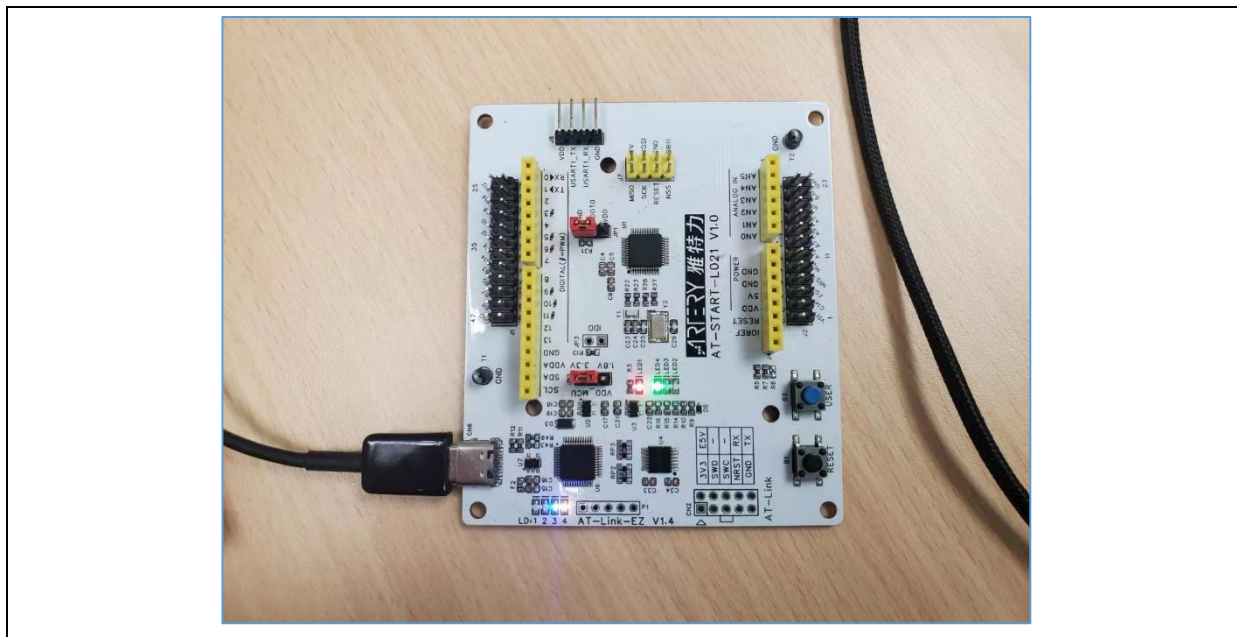
打开对应的sm3_demo工程, utilities\at32l021_sm3_demo

或打开对应的sm3_demo工程, utilities\at32l021_gmssl_sm3_demo

- 编译通过之后下载到开发板

- 通过开发板上的AT-Link-EZ USB串口连接电脑端打印运行信息。

图 1 接到开发板的 USB 串口



1.4 示例说明

1.4.1 at32l021_sm3_demo

示例中使用的SM3源码来自于：[SMx/SM3 at master · NEWPLAN/SMx · GitHub](#)。

示例中展示了9个不同的pattern的SM3运算，并且由speed_sm3()函式来评估运算效能。

1.4.2 at32l021_gmssl_sm3_demo

示例中使用的SM3源码来自于：<https://github.com/guanzhi/GmSSL>。

示例中展示了9个不同的pattern的SM3运算，并且由speed_sm3()函式来评估运算效能。

2 版本历史

表 1. 文档版本历史

日期	版本	变更
2024.9.26	2.0.0	最初版本

重要通知 - 请仔细阅读

买方自行负责对本文所述雅特力产品和服务的选择和使用，雅特力概不承担与选择或使用本文所述雅特力产品和服务相关的任何责任。

无论之前是否有过任何形式的表示，本文档不以任何方式对任何知识产权进行任何明示或默示的授权或许可。如果本文档任何部分涉及任何第三方产品或服务，不应被视为雅特力授权使用此类第三方产品或服务，或许可其中的任何知识产权，或者被视为涉及以任何方式使用任何此类第三方产品或服务或其中任何知识产权的保证。

除非在雅特力的销售条款中另有说明，否则，雅特力对雅特力产品的使用和/或销售不做任何明示或默示的保证，包括但不限于有关适销性、适合特定用途（及其依据任何司法管辖区的法律的对应情况），或侵犯任何专利、版权或其他知识产权的默示保证。

雅特力产品并非设计或专门用于下列用途的产品：（A）对安全性有特别要求的应用，例如：生命支持、主动植入设备或对产品功能安全有要求的系统；（B）航空应用；（C）航天应用或航天环境；（D）武器，且/或（E）其他可能导致人身伤害、死亡及财产损害的应用。如果采购商擅自将其用于前述应用，即使采购商向雅特力发出了书面通知，风险及法律责任仍将由采购商单独承担，且采购商应独立负责在前述应用中满足所有法律和法规要求。

经销的雅特力产品如有不同于本文档中提出的声明和/或技术特点的规定，将立即导致雅特力针对本文所述雅特力产品或服务授予的任何保证失效，并且不应以任何形式造成或扩大雅特力的任何责任。

© 2024 雅特力科技 保留所有权利