通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

马海英,曾国荪,王占君,王 伟.高效可证明安全的基于属性的在线/离线加密机制[J].通信学报,2014,(7):104~112

高效可证明安全的基于属性的在线/离线加密机制

Efficient and provably secure attribute-based online/offline encryption schemes

投稿时间： 2013-03-18

DOI：10.3969/j.issn.1000-436x.2014.7.013

中文关键词：基于属性加密 在线/离线 密钥封装 轻量级设备 可证明安全

英文关键词:attribute-based encryption online/offline key encapsulation lightweight devices provable security

基金项目:国家高技术研究发展计划(“863”计划)基金资助项目(2009AA012201)；国家自然科学基金资助项目(61272107, 61202173, 61103068, 61272424, 11371207, 61202006, 61300167)；NSFC-微软亚洲研究院联合基金资助项目(60970155)；上海市优秀学科带头人计划基金资助项目(10XD1404400)；国家教育部博士点基金资助项目(20090072110035)；教育部网络时代科技论文快速共享专项研究课题基金资助项目(20110740001)；上海自然科学基金资助项目(13ZR1443100)；南通市科技计划基金资助项目(BK2013050, BK2012026, BK2011070)；江苏省高校自然科学研究基金资助项目(12KJB520015, 12KJB520013)

作者	单位
马海英，曾国荪，王占君，王 伟	1. 同济大学 计算机科学与技术系，上海 201804；2. 南通大学 计算机科学与技术学院，江苏 南通 226019；3. 南通大学 理学院，江苏 南通 226007

中文摘要：

为了提高加密的效率，将在线/离线密码技术引入到ABE中，提出了基于属性的在线/离线加密(ABOOE)机制。ABOOE将加密过程非平凡地分解成离线和在线2个阶段，离线阶段在不知明文和所需属性集合的前提下，对复杂计算进行预处理；在线阶段获知消息和属性集合后，仅需少量简单计算即可生成密文。首先构建出一个CPA安全的ABOOE方案。为了提高ABOOE的安全性，提出基于属性的在线/离线密钥封装机制(ABOOKEM)和一个相应方案，并构造出一种将单向性ABOOKEM转化成CCA安全ABOOE的通用性方法。该方法在不增加计算量的前提下有效提高了ABOOE的安全性。与知名ABE方案相比，所提出的ABOOE极大地提高了ABE中加密的效率，特别适用于计算能力高度受限的终端设备。

英文摘要：

To improve the encryption efficiency, the online/offline cryptography was extended to ABE and the primitive of attribute-based online/offline encryption (ABOOE) was proposed. The ABOOE non-trivially splited the encryption process into two phases: the offline phase first executed most of heavy computations prior to knowing the message and the attributes’ set; and then the online phase only performed light computations to produce the ciphertext once the attributes’ set and the message get available. An ABOOE scheme was first constructed with the CPA security. To enhance its security, the primitive of attribute-based online/offline KEM (ABOOKEM) was also introduced and a concrete ABOOKEM scheme was given, and then a generic transformation was proposed to get security against chosen-ciphertext attack (CCA) for ABOOE from any ABOOKEM with one-wayness. This transformation greatly improved the security for ABOOE without increasing the amount of computation. Compared with the famous ABE schemes, the proposed schemes improved the encryption efficiency and get suitable for power-constrained devices.

查看全文 查看/发表评论 下载PDF阅读器

关闭