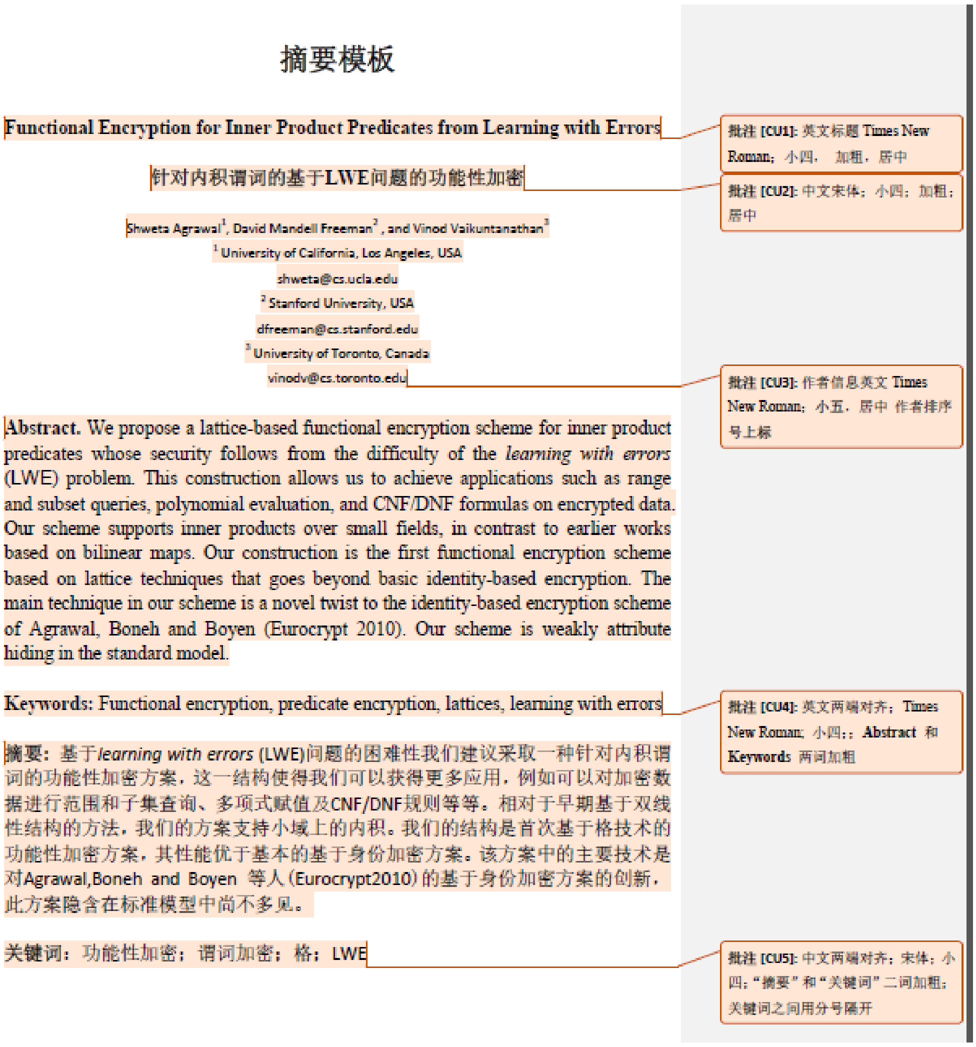
附件 4：



摘要模板

Functional Encryption for Inner Product Predicates from Learning with Errors

针对内积谓词的基于LWE问题的功能性加密

Shweta Agrawal[1], David Mandell Freeman[2] , and Vinod Vaikuntanathan[3]
[1] University of California, Los Angeles, USA
shweta@cs.ucla.edu
[2] Stanford University, USA
dfreeman@cs.stanford.edu
[3] University of Toronto, Canada
vinodv@cs.toronto.edu

Abstract. We propose a lattice-based functional encryption scheme for inner product predicates whose security follows from the difficulty of the *learning with errors* (LWE) problem. This construction allows us to achieve applications such as range and subset queries, polynomial evaluation, and CNF/DNF formulas on encrypted data. Our scheme supports inner products over small fields, in contrast to earlier works based on bilinear maps. Our construction is the first functional encryption scheme based on lattice techniques that goes beyond basic identity-based encryption. The main technique in our scheme is a novel twist to the identity-based encryption scheme of Agrawal, Boneh and Boyen (Eurocrypt 2010). Our scheme is weakly attribute hiding in the standard model.

Keywords: Functional encryption, predicate encryption, lattices, learning with errors

摘要： 基于*learning with errors* (LWE)问题的困难性我们建议采取一种针对内积谓词的功能性加密方案，这一结构使得我们可以获得更多应用，例如可以对加密数据进行范围和子集查询、多项式赋值及CNF/DNF规则等等。相对于早期基于双线性结构的方法，我们的方案支持小域上的内积。我们的结构是首次基于格技术的功能性加密方案，其性能优于基本的基于身份加密方案。该方案中的主要技术是对Agrawal,Boneh and Boyen 等人(Eurocrypt2010)的基于身份加密方案的创新，此方案隐含在标准模型中尚不多见。

关键词： 功能性加密；谓词加密；格；LWE

批注 [CU1]: 英文标题 Times New Roman；小四， 加粗，居中

批注 [CU2]: 中文宋体；小四；加粗；居中

批注 [CU3]: 作者信息英文 Times New Roman；小五，居中 作者排序号上标

批注 [CU4]: 英文两端对齐；Times New Roman; 小四;; **Abstract** 和 **Keywords** 两词加粗

批注 [CU5]: 中文两端对齐；宋体；小四;“摘要”和“关键词”二词加粗；关键词之间用分号隔开