平成 26 年度 共同利用研究報告書

平成 26 年 12 月 24 日

九州大学 マス・フォア・インダストリ研究所長 殿

所属・職名

提案者 氏名（ふりがな） 穴田（あなだ） 啓晃（ひろあき）

下記の通り共同研究の報告をいたします。 記

	※整理番号		20140008	
1.研究計画題目	社会基盤としての高機能暗号とその楕円曲線及び格子による実現			
2.種別（○で囲む）	a. 研究集会Ⅰ　(b. 研究集会Ⅱ)　c.短期共同研究　d.短期研究員			
3.研究代表者	氏名（ふりがな）	穴田（あなだ） 啓晃（ひろあき）		
	所属部局名	公益財団法人九州先端科学技術研究所 情報セキュリティ研究室	職名	研究員
	連絡先			
	e-mail		TEL	
4.研究実施期間	平成 26 年 9 月 9 日（火曜日）～平成 26 年 9 月 11 日（木曜日）			

5.参加者数・参加者リスト（＊別紙「共同利用研究報告書作成上の注意」参照）

（a および b の場合、参加者数のみ記入し、集会参加者リストを添付。 c および d の場合は下記欄に記入。）

参加者数： 30 人

氏名（ふりがな）	所属	職名	氏名（ふりがな）	所属	職名

6.本研究で得られた成果の概要

研究集会(II)として採択された本研究集会では，予定どおり 12 件の講演が実施された（プログラム：http://www.imi.kyushu-u.ac.jp/events/view/1388 ）．これら 12 件の講演は，《数学的構造》の観点から次のように分類されるものであった（CHENG 氏には両方に関する講演を頂いた）．

a)楕円曲線に基づく暗号：辻井氏，HENG 氏，CHENG 氏，安田貴徳氏，高島氏，穴田氏，寺西氏，WENG 氏

b)格子に基づく暗号：MOROZOV 氏，CHENG 氏，DAHAN 氏，有田氏，安田雅哉氏

いずれの講演も，組織委員が計画していた趣旨に沿い，《数学的構造》及び《社会基盤としての暗号機能の適用》の両面から説明がなされた．その内容は，成果物として会議録の形で IMI から出版される予定である．

一方，参加者数は 30 人と，ほぼ当初の予定どおりの規模を達成することが出来た（関連資料：参加者リスト）．これらの参加者の中には 17 名の，九州大学もしくは公益財団法人九州先端科学技術研究所（組織委員の所属機関）以外の方々を含む．これは《社会基盤としての暗号機能の適用》に対する関心の高さを表しているものと考える．これらの方々により，各講演に対する質疑応答，また講演の合間や終了後の会話の形で，活発に意見交換がなされたことは，成果の一つと捉えられる．なお閉会時には，同趣旨の研究集会の開催希望の御意見を多数頂いた．

成果物

1) IMI 研究集会会議録（出版予定），2) 参加者リスト，3) 本成果報告書

（以上）