

ブース番号	3	分野	省エネ・高効率化・新エネ
問合せ先	所属・氏名 自然科学研究科(産業創成工学専攻) 野上 保之 Tel 086-251-8127 Fax 086-251-8127 E-mail nogami@cne.okayama-u.ac.jp		
テーマ	暗号システム用の代数計算回路の高効率実装		
研究ステップ	基礎研究	1	2 3 ④ 5 応用研究
共同研究希望先企業	セキュリティ関連メーカー		
<p>【研究の概要と特徴】</p> <p>クラウドコンピューティング時代に入り、安全・安心な情報通信を支える情報セキュリティ技術に対する要求はますます高度化し、複雑になっています。それを支える暗号技術、そして暗号技術を実現する複雑な数学的計算は、スマートフォンに代表されるユビキタス端末上で快適に処理される必要があります。本研究グループでは、これを高速かつ極めてコンパクトな回路規模で実現する暗号計算チップを開発しました。従来技術と比較して、安全強度に対して数十倍のスケラビリティを一つの計算チップで実現するもので、様々なセキュリティ製品・システムで活用できます。</p> <p>【産業界へのアピールポイント】</p> <p>本研究グループでは、256ビットから5120ビットまで広範な安全強度の要求に対応できる暗号計算チップを、科学技術振興機構 A-STEP シーズ顕在化ファンドと東京エレクトロン デバイス(株)の協力により開発しました。これにより、これまでソフトウェアで処理してきた複雑な計算をより高速に処理することができ、益々大容量化する情報データに対する暗号化や認証の処理を、より高速に処理できるようになります。開発したチップは、暗号計算を高速に処理できる一方で、その回路規模は極めてコンパクトとなっており、様々なユビキタス端末への搭載が期待されます。</p> <p>【想定される用途】</p> <p>電子認証機能を搭載した携帯端末、情報通信端末など</p> <p>【特許等知的財産】</p> <p>「拡大体の乗算プログラム及び拡大体の乗算装置、 特願 2006-200946、出願日 2006/01/24」</p> <p>「拡大体の乗算プログラム及び拡大体の乗算装置、 PCT 出願 PCT/JP2007/064474、出願日 2007/01/24」</p>			

ブース番号	3	分野	省エネ・高効率化・新エネ
-------	---	----	--------------

テーマ 暗号システム用の代数計算回路の高効率実装

参考資料

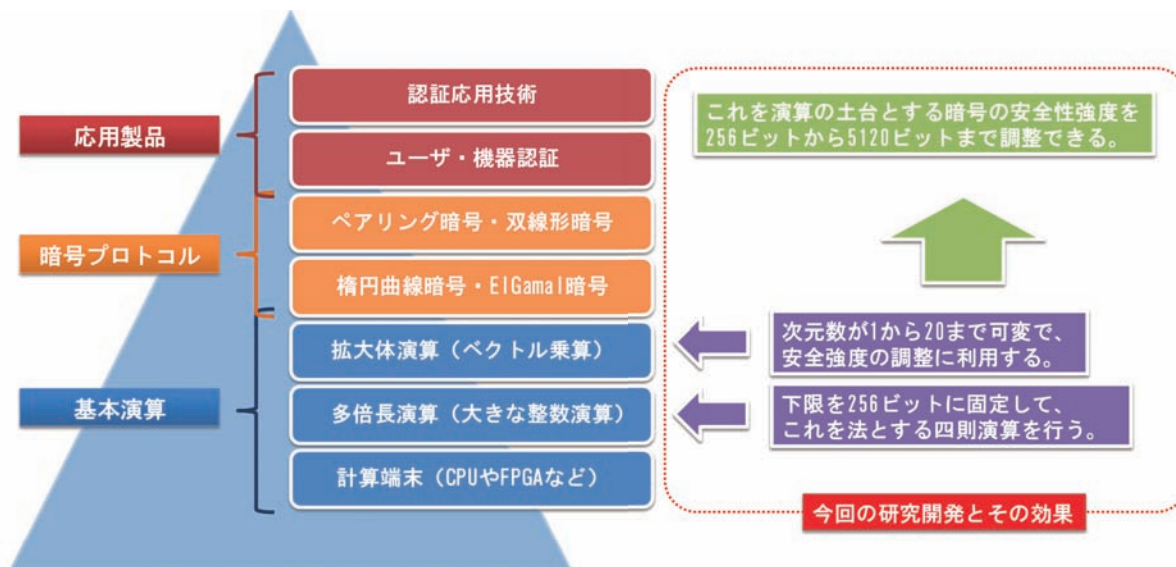


図1: 電子認証を実現する暗号技術の階層と本研究開発の効果

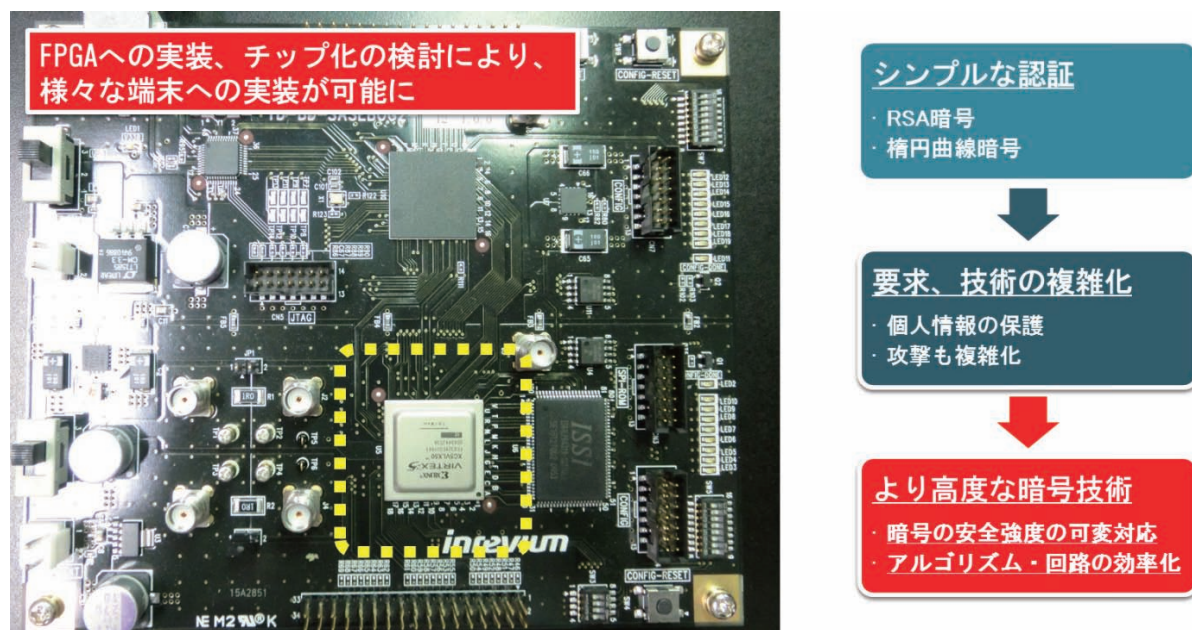


図2: 開発したアルゴリズムを搭載する試作ボード