ペアリング暗号の安全性評価

受賞業績　**ペアリング暗号解読の世界記録達成および安全な次世代暗号の選定**

高木 剛 [*1]　林 卓也 [*1]　篠原 直行 [*2]　下山 武司 [*3]

[*1] 九州大学マス・フォア・インダストリ研究所　[*2] (独) 情報通信研究機構ネットワークセキュリティ研究所
[*3] (株) 富士通研究所ソフトウェア技術研究所

このたび，栄えある喜安記念業績賞を受賞し，大変光栄に思います．本研究プロジェクトを遂行するにあたり，(独) 情報通信研究機構　盛合志帆様，NTT セキュアプラットフォーム研究所　青木和麻呂様，富士通研究所　小暮淳様，安田雅哉様に多大なるご協力をいただきました．この場をお借りしまして，改めて感謝の意を表したいと思います．

受賞テーマの対象となった暗号技術は，情報セキュリティの基盤となる技術で，インターネットにおける安全な通信や著作権保護などを支える技術として，さまざまな場面で利用されています．我々の研究で扱った「ペアリング暗号」と呼ばれる暗号は，2000 年に提案された新しい公開鍵暗号で，暗号化したデータを復号せずに検索できる機能など，さまざまな応用が実現できる暗号方式です．その応用の広さを背景に，活発に研究開発が行われており，ISO, IEEE, IETF 等において，標準化が進められています．一方，新しい暗号であるがゆえに，実用的かつ安全な鍵の長さの見積もりが重要な研究課題となっていました．この安全な鍵の長さを正確に見積もるためには，世界最高水準の解読プログラムと最新の解読アルゴリズムを使って計算実験を行い，攻撃者の解読能力の計算限界を知る必要があります．我々の持つ数学的知識やプログラミング技術を背景に，高速な解読プログラムを開発することにより，それまで解読に数十万年かかると考えられていた 278 桁(923 ビット)の鍵の長さのペアリング暗号を 148 日で解読することに成功しました．この記録はペアリング暗号解読の世界記録であり（**図 -1**），我々の解読プログラムが世界最高水準であることの 1 つの証であると言えます．

これらの成果は，安全な鍵の長さを評価するための技術的根拠として活用されており，我が国の電子政府システムの安全性向上等に貢献しています．本受賞を励みにこれからも研究を重ね，本分野のさらなる発展に貢献できるよう精進する所存です．

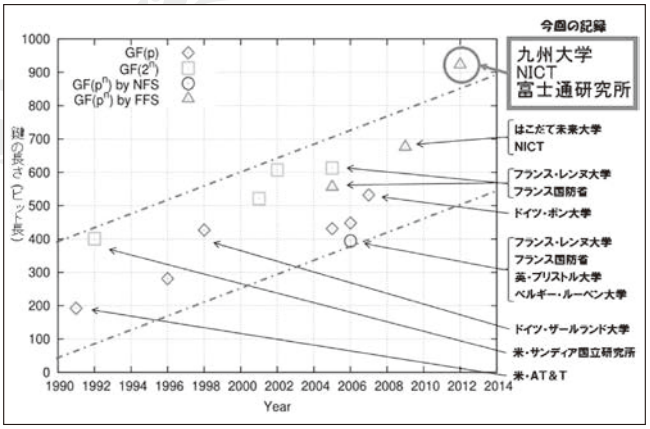

図 -1　離散対数問題の解読世界記録の推移

(2013 年 5 月 15 日受付)

高木 剛（正会員）　takagi@imi.kyushu-u.ac.jp
1995 年名古屋大学大学院理学研究科修士課程修了．PhD（TU Darmstadt）．現在，九州大学マス・フォア・インダストリ研究所教授．暗号および情報セキュリティに関する研究に従事．第 8 回船井情報科学振興賞．

林 卓也（正会員）　t-hayashi@imi.kyushu-u.ac.jp
2013 年九州大学大学院数理学府博士後期課程修了，博士（機能数理学）．同年より九州大学マス・フォア・インダストリ研究所学術研究員，公開鍵暗号の安全性解析の研究に従事．IACR, IEICE 各会員．

篠原 直行　shnhr@nict.go.jp
2009 年より情報通信研究機構研究員，博士（数理学）．計算機代数学および公開鍵暗号の安全性解析に関する研究に従事．日本数式処理学会 2008 年度奨励賞．IEICE，JSIAM，JSSAC 各会員．

下山 武司　shimo-shimo@jp.fujitsu.com
1991 年富士通研究所入社，現在主任研究員，博士（工学）．暗号解読・暗号設計に関する研究に従事，2006 年素因数分解世界記録樹立．2007 年電気科学技術奨励賞，2007 年本会喜安記念業績賞．