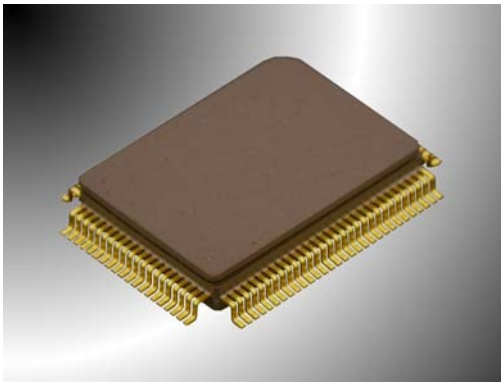
NEWS RELEASE

２００８年４月１５日
ＦＤＫ株式会社
筑　波　大　学
公立はこだて未来大学
情報セキュリティ大学院大学

世界初となるペアリング演算用のＩＣを開発



ＦＤＫ株式会社(社長：杉本俊春)、国立大学法人筑波大学(学長：岩崎洋一)、公立はこだて未来大学(学長：中島秀之)、情報セキュリティ大学院大学(学長：辻井重男)は、2005 年 11 月に独立行政法人 新エネルギー・産業技術総合開発機構(ＮＥＤＯ技術開発機構)の助成／委託を受け、このたび情報セキュリティとプライバシ対策において非常に有効な概念である双線形群を利用した、ペアリング演算用の IC(試作品)を開発致しました。

近年、情報ネットワークの進展にともなってセキュリティの対策が急務となっています。それは、小型化による情報端末の急増と社会の隅々への浸透、及びネットワークによる情報伝達収集能力の飛躍に起因しているからです。これらにより、攻撃の対象が増えたばかりでなく、攻撃に利用できるツールも増えており、セキュリティに対する要請は非常に高まっています。従来、この対策として、アクセス制御や暗号技術を用いた情報セキュリティ対策が採られてきましたが、上記の二つの進展が速すぎて追いつくのが容易ではない状況にあります。アクセス制御では情報自体は暗号化されていないので安全性の面で不安があり、また従来の暗号技術を使った対策では複雑な鍵管理が必要となるためスケーラビリティの問題があります(原理的には、鍵は端末－端末に対応しているので端末数の２乗のオーダとなります)。これは急激なユビキタスネットワーク進展と情報拡大におけるセキュリティ危機といえる状況です。

このため、ユビキタスネットワークの進展に追いつける新しい暗号システムの開発が求められています。これに答えられる仕組みが近年注目されているペアリング暗号です。ペアリング暗号を用いると公開鍵暗号基盤は極めて簡単なものとなり、鍵共有プロトコルもやり取りが不要となります。従って各端末に組み込めば非常に簡単にセキュアなシステムを組むことができるようになり、まさにユビキタスネットワーク向きといえます。

しかしながら、今までペアリング暗号の演算は処理に時間がかかる欠点がありました。従来例の代

表である RSA 公開鍵暗号の処理に比べて数倍の時間がかかり、しかもソフトウェアでの実装が主たるものでした。そこでこのたびハードウェア化に向けて、アルゴリズムの改良・実装方法の工夫等を施すことにより世界で初めてペアリング演算用 IC の開発に成功しました。本 IC は、約 20 万ゲート規模(2NAND 換算、ROM/RAM/IO 除く)で実現しており、一回のペアリング計算時間が 47μs という非常に高速な演算処理速度を達成しております (2008 年 3 月現在)。

用語解説

※1 公開鍵暗号

1976 年に Diffie 氏と Hellman 氏により考え出された暗号方式です。共通鍵暗号方式では暗号化する人と復号する人が同じ鍵を使いましたが、公開鍵暗号方式では暗号化する鍵と復号する鍵が異なっているのが大きな特徴です。この方式は一方の鍵を公開しても、もう一方の鍵が計算できないという特徴を持っています。

※2 RSA

1978 年に Ronald Rivest 氏, Adi Shamir 氏, Leonard Adleman 氏らによって開発された公開鍵暗号方式の 1 つで、開発者の頭文字をとって名付けられています。現在、インターネットをはじめとして公開鍵暗号の標準として広く普及しています。RSA 暗号を解読するには、巨大な整数を素因数分解する必要があります。現在、RSA の安全性を提供する「法」と呼ばれるパラメータとして 1024 ビットが主に使われています。

※3 ペアリング(Pairing)

ペアリングとは、楕円曲線上における双線形写像 e(,)で、任意の整数 a, b, 楕円曲線上の点 P, Q に対して $e(aP, bQ)=e(P, Q)^{ab}$ を満たすものであり、この性質を双線形性と言います。このペアリング暗号は、近年になって初めて大阪電気通信大学の境氏らによって初めて暗号鍵生成法に適用され、スタンフォード大学の Dan Boneh 氏らによって世界に広まった暗号です。

発表者

FDK ﾓｼﾞｭｰﾙｼｽﾃﾑﾃｸﾉﾛｼﾞ株式会社　事業技術本部　技術部
筑波大学　　システム情報工学研究科リスク工学専攻教授　岡本栄司
公立はこだて未来大学情報アーキテクチャ学科教授　高木剛
情報セキュリティ大学院大学情報セキュリティ研究科教授　土井洋