

Message-ID: <3C878017.664BCA8C@sdl.hitachi.co.jp>
Date: Thu, 07 Mar 2002 23:58:31 +0900
From: Takaragi Kazuo <takara@sdl.hitachi.co.jp>
To: cryptrec-comment@ipa.go.jp
Subject: OK-ECDSA、OK-ECDHに関するワークショップでの議論について

CRYPTREC事務局御中

日立製作所システム開発研究所の宝木です。平素より弊社提案暗号技術に関しましてCRYPTREC活動ならびに暗号技術安全性評価では大変お世話になっております。

さて、2002年1月28日に開催された暗号技術評価ワークショップでは、弊社提案の暗号技術OK-ECDSAとOK-ECDHに関して、以下の御指摘を受けました。

- ・耐性が高いという主張は正当と考えられるが、実装による定量的評価に乏しい
- ・提案者の評価は理論的な考察のみであり、実装レベルでの留意点が記述されていないため、耐性の低い実装が行なわれる可能性がある
- ・他の手法との実装比較、プラットフォームの特徴や演算サイクルを考慮した評価が必要

- ・必要メモリ量に関しても同様
- ・スマートカード上での実装評価結果がない
- ・ハードウェア実装結果の根拠が示されていない

これらに関して、新たな実装実験結果が得られましたので、評価の参考用に概略を報告致します。

日立H8/300Hシリーズマイコン、ICカードリーダーライタ、ICカード(Cot+ホワイトカード、MiniOS搭載)、PC(RS-232Cで接続)、電流測定計を用いて電力解析システムを構築しました(電圧は5Vに設定しています)。その電力解析システムの上で、OK-ECDSA、OK-ECDHの基盤となるモンゴメリ型楕円曲線上のスカラー倍演算実行時における電力消費量に対して数万回程度の電力測定を行ない、DPA(Differential Power Analysis)攻撃を試みました。

その結果、秘密鍵の部分情報を示す兆候を得ることはできませんでした。一方で、計算データのランダム化を行わない(ランダム化射影座標を用いない)スカラー倍計算を用いた場合には、同じ環境下で秘密情報の部分情報の特定に成功しました。これらの実験結果については、いずれ学会で詳細を発表する予定でいます。また、バイナリ法にダミー演算を施した防御法との比較では、メモリ量(RAM)に関しては同等、処理速度に関して約2倍の優位性がありました。高速性を重視したウィンドウ法(サイドチャネル攻撃に対しては脆弱)との比較では、処理速度に関しては同等、メモリ量(RAM)に関して約1.5倍の優位性がありました。

また、以下のような背景があり、公募時ではハードウェア評価に関して特段の配慮を致しませんでした。

平成13年度暗号技術公募要領では、5.提出書類 (3)自己評価書 (e)ハードウェア実装評価 (5.3.e節 13ページ)において、以下のよう記述されています。

「使用したプロセス・・・
・・・シミュレーション結果でもかまいません。
公開鍵暗号技術は対象外です。」

OK-ECDSA、OK-ECDHは公開鍵暗号技術ですので、そのため弊社としましては自己評価書においてハードウェア実装評価に関して特段の詳細な記述を行ないませんでした。しかしながら、CRYPTREC事務局より提出の御要望があれば、提出させて頂く所存です。

弊社が独自で行なったハードウェア実装実験におけるサイドチャネル攻撃への耐性評価ですが、OK-ECDSA、OK-ECDHの設計時に要求していたサイドチャネル攻撃への耐性水準を十分に達成していると確信しています。しかしながら、この結果が全てのプラットフォーム上で一様に高い耐性を有することを示すものとはいえません。しかしながら少なくとも、ハードウェアに関してある程度の知識と技術を有する者が慎重に設計を行えば、サイドチャネル攻撃に対する耐性に関して同等以上の性能を有する装置を製作できると確信しております。

また、楕円曲線暗号に対するサイドチャネル攻撃についての最近の動向についても若干のコメントをさせていただきます。

2001年10月以降に、楕円曲線暗号におけるサイドチャネル攻撃の防御法に関して多くの論文[1-6]が発表(内1件はOK-ECDSA、OK-ECDH関連技術)されています。これらの論文におけるサイドチャネル攻撃の防御法の構成には一定の方向性が見受けられます。すなわち、秘密鍵に依存せず一定の処理手順をとり、その上で計算データをランダム化するという手法を用いて防御法を構成しています。(実際、OK-ECDSA、OK-ECDHもこの手法を用いて防御法を構成しています。)

しかしながら、アルゴリズム的な手法でサイドチャネル攻撃を防ぐ方法はこれらの手法を用いるものだけとは限りませんし、洗練された手法のサイドチャネル攻

撃により脆弱となる可能性についても否定できません。また、2001年12月に発表された論文[7]においては、OK-ECDSA、OK-ECDHの基盤となる技術(論文[8]に記載の技術)に対して攻撃法を構成できたとの報告があります。しかしながらその詳細は公開されておらず、その真偽性について確信を得ていません。弊社としてはサイドチャネル攻撃の最新動向に敏感に反応し、OK-ECDSA、OK-ECDHの耐性解析についてさらなる検討を続ける所存でいます。

ECDSAとOK-ECDSA、ECDHとOK-ECDHとの関連についても補足しておきます。ワイエルシュトラス型楕円曲線とモンゴメリ型楕円曲線は、(必要であれば体を拡大することにより)必ず相互に変換可能であり、その変換は多項式時間で達成できます。もしもECDSAに何らかの脆弱性が発見されれば、モンゴメリ型楕円曲線へ変換を施すことにより、直ちにOK-ECDSAにも適応されますし、その逆もそうです。例えば、OK-ECDSAにおいて(モンゴメリ型)楕円離散対数問題を解かずに署名を偽造できるとすると、ECDSAの署名をOK-ECDSAの署名に変換し、その署名を偽造し、ECDSAの署名に変換することにより、ECDSAの署名を偽造できることとなります。それゆえ、OK-ECDSAとOK-ECDHは、スキームとしては、既に多くの評価実績があり電子政府での利用に耐えらると思われるECDSAとECDHのそれぞれの安全性に根拠を置いています。

ワイエルシュトラス型楕円曲線とモンゴメリ型楕円曲線の関係については自己評価書に記載していますし、学会発表[9]も行なわれています。

事務局の皆様、ならびに委員の皆様におかれましては、上記弊社意見を御理解のうえ、今後の評価活動の参考にして頂ければ幸いに存じます。

参考文献

- [1] Brier, E., Joye, M., "Weierstrass Elliptic Curves and Side-Channel Attacks", Public Key Cryptography (PKC2002), LNCS2274, (2002), 335-345.
- [2] Fischer, W., Giraud, C., Knudsen, E.W., Seifert, J.P., "Parallel scalar multiplication on general elliptic curves over \mathbb{F}_p hedged against Non-Differential Side-Channel Attacks", International Association for Cryptologic Research (IACR), Cryptology ePrint Archive 2002/007, (2002). Available at <http://eprint.iacr.org/>
- [3] Izu, T., Takagi, T., "A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks", Public Key Cryptography (PKC2002), LNCS2274, (2002), 280-296.
- [4] Izu, T., Takagi, T., "On the Security of Brier-Joye's Addition Formula for Weierstrass-form Elliptic Curves", Technical Report No. TI-3/02, (2002). Available at <http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html>
- [5] Okeya, K., Miyazaki, K., Sakurai, K., "A Fast Scalar Multiplication Method with Randomized Projective Coordinates on a Montgomery-form Elliptic Curve Secure against Side Channel Attacks", The 4th International Conference on Information Security and Cryptology (ICISC 2001), Pre-Proceedings, (2001), 475-486.
- [6] 秋下 徹, 飯塚 健, 佐藤 英雄, "非接触型ICカード用の楕円曲線ハードウェア実装", 2002年暗号と情報セキュリティシンポジウム, SCIS02-15B-1, (2002), 1107-1112.
- [7] Yen, S.M., Kim, S., Lim, S., Moon, S., "A Countermeasure Against One Physical Cryptanalysis May Benefit Another Attack", The 4th International Conference on Information Security and Cryptology (ICISC 2001), Pre-Proceedings, (2001), 459-473.
- [8] Okeya, K., Sakurai, K., "Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack", Progress in Cryptology - INDOCRYPT 2000, LNCS1977, (2000), 178-190.
- [9] 宮崎 邦彦, 桶屋 勝幸, 櫻井 幸一, "暗号に利用可能なモンゴメリ型楕円曲線の存在数に関する一考察", 2002年暗号と情報セキュリティシンポジウム, SCIS02-4B-4, (2002), 167-172.

宝木 和夫

(株)日立製作所システム開発研究所
第7部(セキュリティシステム研究部)
〒244-0817 横浜市戸塚区吉田町292
TEL (045)860-3072 FAX (045)860-1662
E-mail: takara@sdl.hitachi.co.jp
URL: <http://www.sdl.hitachi.co.jp>
