D12-015

作品名稱
適用於低功耗行動通訊並具有抵抗能量分析攻擊之雙域橢圓曲線密碼處理器
A Power-Analysis Resistant DF-ECC Processor for Low-Power Mobile Applications

隊伍名稱
矽星隊 / SI2 STAR

隊長
李人偉　交通大學電子工程研究所

隊員
鍾思齊　交通大學電子工程研究所

作品摘要

在電子通訊網路應用裡，如何有效地保有個人資料的正確性、安全性及隱私性已是系統設計裡不可避免之考量。橢圓曲線密碼（Elliptic Curve Cryptography, ECC）是目前公認最具安全性的公開金鑰加密機制，相較於傳統的RSA，ECC可以用小於數倍以上的金鑰位元長達到一樣的安全度，這表示在硬體實現上，不管是效能、複雜度，甚至是能量消耗，ECC均有其優勢。在2000年，國際電機電子工程師學會（IEEE）也針對 ECC制定了應用的規範IEEE P1363，包含加密/解密、簽章/認證與金鑰交換，其可廣泛被應用在各種電子商務，包含無線射頻辨識、金融交易、數位版權管理等。但是對於近年來熱門的行動通訊還有能量分析攻擊法（Power-Analysis Attacks），高效能、低複雜度與高硬體安全度的需求越來越受到重視，因此，本作品提出了全新的積體電路架構與實現方式，達到目標設計一個支援雙域（Dual Fields, GF（p）and GF（2^m））運算且具有能量分析攻擊防護的ECC處理器。

因為過去大部分的文獻都是各自訴求速度與硬體複雜度的改進，針對 ECC 提出不同的映射座標與排程方式，但是這些都忽略了能量分析攻擊法，以現今的量測技術，不需要昂貴的設備就已經可以在數條能量消耗軌跡分析出金鑰值，所以沒有保護的ECC硬體加速器很容易遭受駭客的攻擊。據此，本作品提出一個新的Montgomery division演算法和利用隨機化橢圓點（Randomized Elliptic Curve Point）技巧，加速硬體運算以及避免運算中間值與金鑰存在相依性造成以洩漏私密訊息。硬體實現上，設計一個新的異質運算單元（Heterogeneous Processing Element）架構有效提升硬體運算速度；再者，利用完全管線化與平行資料處理技巧在運算單元與基本電路元件中優化時脈與複雜度以更進一步提高效能。另外，為了支援即時應用也提出了一個免預算機制。在功能性與彈性度上，我們使用一個能支援任意金鑰長度的硬體架構。此ECC硬體加速器不僅可達非常高的吞吐量，且記憶體資料流經過最佳化，相當適合未來低功耗可攜式電子產品的需求。透過UMC 90-nm CMOS 1P9M製程，晶片的量測結果顯示，我們設計的一個 0.41mm^2 160位元長的雙域橢圓曲線密碼處理器（Dual-Field Elliptic Curve Cryptographic Processor, DF-ECC Processor）可以在0.34/0.29ms 11.7/9.3μJ完成一筆完整的GF（p）/GF（2^m）的橢圓曲線點純量乘法運算（Elliptic Curve Scalar Multiplication, ECSM）。和過去文獻相比，此設計具有下列特點：

（1）單位面積高運算處理速度 （2）低消耗功率

（3）優異的能量分析攻擊防護 （4）高彈性度

（5）高安全度 （6）支援即時應用。

Abstract

Nowadays, ensuring accuracy, security, and privacy for data management is essential in communication applications. Compared to traditional RSA algorithm, elliptic curve cryptography (ECC) can provide the same security level with shorter key size. This means that the ECC hardware device has benefits in hardware performance, hardware cost, and even power consumption in related applications. In 2000, IEEE proposed a standard, IEEE P1363, to develop ECC scheme for encryption/decryption, signature/authentication, and key management in public-key cryptosystem. It is wieldy applied in commercial products such as radio-frequency identification, marketing, and digital right expression.

For the past several years, many previous works have been published for ECC hardware implementation aiming at the performance improvement. However, even if the ECC is secure at cryptanalysis, the private data of an unprotected hardware device can be extracted by physical attacks due to side-channel leakage. The power-analysis attacks, initially presented by Kocher, can reveal the key value by analyzing the power information of a cryptographic implementation such as on an application-specified integrated circuit, field-programmable gate array, or microprocessor.

In this work, we propose a new design method for providing an efficient solution of dual-field ECC processor with power-analysis resistance. By randomized elliptic curve point technique, the correlation between the target power traces and power model can be broken. To reduce computation latency, a new Montgomery division is proposed also. For hardware implementation, the fully-pipelined heterogeneous processing element architecture is exploited to improve hardware performance by parallel processing. Besides, a free pre-computation scheme is presented to avoid system retard and provide real-time application. For functionality and user ability, we use a flexible architecture to support arbitrary key size. After optimizing data bandwidth, this proposed ECC processor not only achieves high data rate but also consumes low energy per operation. Thus our proposed solution is well suitable for mobile device. By using UMC 90-nm CMOS 1P9M technology, a 0.41 mm^2 160-bit DF-ECC processor can perform one elliptic curve scalar multiplication in 0.34/0.29ms with 11.7/9.3μJ. Compared with previous works, our design is advantage in

(1) hardware efficiency (2) energy dissipation (3) power-analysis resistance (4) user convenience (5) security level (6) real-time application.

指導教授

李鎮宜

交通大學電子工程研究所

李鎮宜教授，1986和1990年各別取得比利時魯汶大學電機工程碩士與博士學位。1991年返回交通大學電子工程系所任教。2003~2006年之間擔任交通大學電子工程系系主任、2006~2007年之間擔任交通大學晶片系統研究中心主任、2007~2010年之間擔任交通大學研發長。目前為IEEE TCAS-II期刊副編輯與IEEE Symposium on VLSI Circuits大會委員。

研究領域

包含低功耗人體近身網路、高效能多媒體、能量分析攻擊抵抗加解密系統整合晶片。研究成果累計著有16篇IEEE JSSC期刊論文、十多項以上技術轉移與共近四十項的國內外專利。

張錫嘉

交通大學電子工程研究所

張錫嘉教授，2000年取得交通大學電子工程研究所博士學位。後進入聯發科技股份有限公司擔任光儲存產品事業部副理，2003年返回母校擔任教職，並自2010年升任正教授。

張錫嘉教授在2006年2月與李鎮宜教授共同成立OCEAN（OverCome Error And Noise）研究群，分別於2007年、2008年得到行政院國家科學委員會「傑出技術移轉貢獻獎」，2009年榮獲「經濟部大學產業經濟貢獻獎」等肯定。

研究領域

高吞吐量傳輸錯誤更正碼以及高速加解密密碼硬體電路設計與實現。因為錯誤更正碼的技術轉移成功，2009獲得「旺宏電子股份有限公司產業貢獻獎」。