

基于椭圆曲线签密的物联网安全通信方案

周宣武^{1,2}, 付 燕^{1,3}, 金志刚¹, 刘开华¹, 李 欣²

(1 天津大学 电子信息工程学院, 天津 300072; 2 武警指挥学院, 天津 300250;

3 烟台保税港区综合服务中心, 山东 烟台 264001)

摘 要: 提出了基于椭圆曲线签密的物联网安全通信与匿名通信方案, 在 Random Oracle 模型下分析了方案的可证明安全性. 与使用典型的签名、加解密算法的交互通信协议进行了效率对比, 提出的方案在计算量与通信量上具有较大优势, 能更好地满足物联网安全通信协议的需求. 方案同样适用于其他计算、存储能力有限, 但要求高效率实现的环境, 有广阔的应用前景.

关键词: 物联网; 签密; 随机预言机; 可证明安全性; 算法效率

中图分类号: TP308

文献标识码: A

文章编号: 1000-7180(2014)11-0023-04

Signcryption-Based Secure Scheme for the Internet of Things

ZHOU Xuan-wu^{1,2}, FU Yan^{1,3}, JIN Zhi-gang¹, LIU Kai-hua¹, LI Xin²

(1 School of Electronics and Information Engineering, Tianjin University, Tianjin 300072, China;

2 Command College of the Armed Police Forces, Tianjin 300250, China;

3 Administrative Center of Yantai Trade-free Port, Yantai 264001, China)

Abstract: We proposed a signcryption based secure communication scheme and anonymous communication scheme for the Internet of things and analyzed the provable security of signcryption, including confidentiality, unforgeability and non-repudiation in Random Oracle model. As to efficiency analysis, the scheme achieves remarkable reduction in computational and communication cost compared with other secure protocols based on typical signature and encryption/decryption algorithms. With its superiority in computing and communication cost, it proves to be more suitable for resource-restricted environment in Internet of things and better satisfies the requirement of secure protocols in Internet of things, such as key management, secure routing, etc.

Key words: Internet of things; signcryption; random oracle; provable security; algorithm efficiency

1 引言

物联网(Internet of Things, IoT)代表了未来计算与通信技术发展的方向, 被认为是继计算机、Internet 之后, 信息产业领域的第三次发展浪潮. 为物联网安全、动态的通信设计专门的安全技术、协议及相关算法是密码学的一个重要研究方向, 具有重要的理论意义与应用价值. 它不仅是密码学的研究需要, 更是物联网飞速发展的迫切需要.

在物联网的安全通信中, 消息的机密性与完整性

是两个基本要求, 但是对称密码中认证码与加密的组合以及公钥密码体制中“签名然后加密(Sign-then-Encrypt)”的算法结构并不是同时实现机密性与完整性有效的方法. 首先随意的方案组合无法保证算法的安全性, 其次效率不高, 不适合物联网无线通信资源受限的环境. 1997 年, 文献[1]中提出了签密的密码原型, 它能够在一个算法步骤内同时实现加密与签名的功能, 而计算与通信量却小于两者之和. 由于签密算法的高效性与安全性, 它成为实现消息机密性与完整性的理想选择, 也一直是密码学的研究热点.

收稿日期: 2014-01-06; 修回日期: 2014-02-21

基金项目: 国家自然科学基金项目(60842006)

为了提高物联网通信的安全性及效率,本文提出了基于签密的物联网安全通信方案与匿名通信方案,在 Random Oracle 模型下证明了方案的机密性、不可伪造性与不可否认性.与其他典型的方案相比,文章中方案在计算量与通信量上具有较大优势,更适合于物联网无线通信资源受限的环境,能更好地满足物联网密钥管理、安全路由等通信过程的安全需求.

2 椭圆曲线签密方案及其安全性

定义 1 (椭圆曲线) 有限域上的椭圆曲线 E 是一个六元组: $T = (q, a, b, P, l, h)$, $P = (x_P, y_P)$ 是 E 上的基点, 点 P 的阶是大素数 l . O 是无限远点, 满足 $lP = O$ 且对于任意点 $G \in E$ 满足 $G + O = G$.

定义 2 (椭圆曲线签密方案) 椭圆曲线签密方案 $\Sigma = (GC, GK, SC, USC)$ 包含如下算法:

(1) 概率性公共参数生成算法 $GC(1^k), GC(1^k)$ 以安全参数 1^k 为输入, 输出公共参数序列, 如计算群的描述、散列函数等.

(2) 概率性密钥生成算法 $GK(ID, 1^k), GK(ID, 1^k)$ 以用户身份与安全参数 1^k 为输入, 输出公私钥对 (sk_{ID}, PK_{ID}) .

$(sk_{ID}, pk_{ID}) \leftarrow GK(ID, 1^k)$ (4)

(3) 签密算法 $SC(sk_A, PK_B, m)$ 以发送方的私钥 sk_A 、接收者公钥 PK_B 与消息 $m \in SP_m(sk_A, PK_B)$ ($SP_m(sk, PK)$ 是消息空间) 作为输入, 输出签密文 C . 签密算法也是概率性的.

$C \leftarrow SC(sk_A, PK_B, m)$ (2)

(4) 确定性解签密算法 $USC(sk_B, PK_A, C)$ 以接收者的私钥 sk_B 、发送方的公钥 PK_A 与签密文 C 为输入, 输出消息 m 或 $\perp$ (拒绝符号).

$m \cup \{\perp\} \leftarrow USC(sk_B, PK_A, C)$ (3)

如果签密方案是公开可验证的, 则方案包含确定性公开验证算法 PV .

(5) 确定性公开验证算法 PV . PV 以公钥对 (PK_A, PK_B) 、签密文 C 、中间参数 R 为输入, 返回 “true” 或者 $\perp$.

“True” $\cup \{\perp\} \leftarrow PV(PK_A, PK_B, C, R)$ (4)

签密方案能够同时实现加密与签名的功能, 为了保证具体签密方案的安全性, 方案的安全分析也不同于一般的公钥加密方案与签名方案, 更不是加密与签名方案的简单复合. 签密方案的安全性同时包括机密性、不可伪造性与不可否认性. 签密方案的机密性证明类似与公钥加密方案; 对于一个具体的签密方案, 如果攻击者的 $\text{ind-cca2 advantage}$ 在合理

的资源限制下是可忽略的, 那么方案就是适应性选择密文下不可区分的, 即方案满足机密性要求. 对于一个具体的签密方案, 如果任何攻击者的 uf-cma advantage 在合理的资源限制下是可忽略的, 那么该签密方案在选择消息攻击下就是不可伪造的, 方案也就满足不可伪造性要求. 若存在确定性多项式时间算法使得可信第三方能够验证签密文生成者身份, 那么方案就满足不可否认性^[2-3].

3 物联网安全通信方案

物联网通信需要安全秘密的信道, 以保证敏感信息的机密性与完整性. 同时, 物联网无线链路、微型终端、资源受限等特殊的网络环境, 要求所使用的方案必须是高效的, 要能够以最小的计算和通信量实现相应功能.

首先是基于签密的基本安全通信方案, 方案如下.

(1) 初始化: 选择系统安全通信参数, 包括签密算法中的系统参数.

(2) 消息签密过程

Step1: 消息发送者终端 A 获取系统参数.

Step2: 终端 A 将消息分组 $\{ID_A, Message\}$ 编码成明文 m , 并对该明文进行签密运算 $C \leftarrow SC(sk_A, PK_B, m)$, 然后将签密文 C 发送给终端 B .

(3) 消息解签密与认证

Step1: 消息接收者终端 B 获取系统参数.

Step2: 终端 B 对 C 进行解签密运算 $m \leftarrow USC(sk_B, PK_A, C)$, 恢复了明文 m 并实现了对 A 的认证及消息完整性检验.

物联网通信中, 在合同、遗嘱等文件需要通过第三方进行公证时, 文件的所有者希望第三方对文件进行签密. 签密后的文件由于带有第三方的认证信息, 具有相应的效力, 同时文件经过签密运算也具有机密性. 但是, 文件的所有者并不希望第三方在对文件签密时得知文件的具体内容, 此时盲签密能很好地适应这种特殊的应用需求

利用盲签密可以高效地实现物联网通信中敏感文件的安全公证, 具体安全协议如下.

(1) 公共参数及密钥生成: 选择系统安全通信参数, 包括签密算法中的系统参数. 利用算法 $GC(1^k)$ 与 $GK(ID, 1^k)$ 与生成系统参数与协议方公私钥对 (sk_{ID}, PK_{ID}) .

(2) 消息签密过程

Step1: 文件内容盲化. 敏感文件拥有者通过盲

化算法 BL 以盲化因子 u 对文件内容 m 进行盲化,
 $m' \leftarrow BL(u, m)$.

Step2:中间签密运算. 第三方利用签密私钥 sk_A 和接收者公钥 PK_B 及盲化消息 m' 进行概率性签密运算,生成中间签密文 C' .

$$C' \leftarrow SC_T(sk_A, PK_B, m') \quad (5)$$

Step3:解盲运算. 文件拥有者得到中间签密文 C' 后,利用解盲算法 DBL 通过中间签密文 C' 及盲化因子 u 得到最终签密文 C .

$$C \in \{0,1\}^* \cup \{\perp\} \leftarrow DBL(u, C') \quad (6)$$

(3) 消息解签密与认证

解签密运算:文件特定接收验证者得到签密文 C 后,以私钥 sk_B 、签密公钥 PK_A 与签密文 C 为输入,利用解签密算法 USC 解签密得到敏感文件信息,并对内容进行验证.

$$m \cup \{\perp\} \leftarrow USC(sk_B, PK_A, C) \quad (7)$$

通过以上密码协议,文件拥有者借助第三方实现了文件的机密传输与可靠认证,但是在协议执行中,第三方并不知道文件的具体内容,也无法将不同文件与其相应的签密文相互关联.

由于签密方案的应用,上述协议实现了机密信息及敏感文件在物联网公开信道的高效安全传输.算法在一个算法步骤内实现加密与签名,同时保证了信息的机密性与完整性及不可否认性,但算法的计算和通信量相对于其他方案却大大降低^[4-6].

4 方案的可证明安全性

本节,我们在 Random Oracle 模型下分析本文方案的可证明安全性主要包括机密性、不可伪造性与不可否认性.

类似于一般签密方案的可证明安全性分析,为了在 Random Oracle 模型下分析本文安全通信方案的可证明安全性,我们从机密性、不可伪造性与不可否认性三个方面分析.

假设 1 (ECDLP 是困难的) 设 $T = (q, a, b, P, l, h)$ 是一个椭圆曲线, AE 一个可以访问椭圆曲线 oracle 且输出一个字符串的算法,考虑如下试验:

$$\text{Experiment } EXP_T^{ECDLP}(AE)$$

$$x \xleftarrow{\$} Z_l^*, Q \leftarrow xP,$$

$$x' \leftarrow A^T(P, Q).$$

If $x' = x$ return 1 and return 0 otherwise.

A 的 ECDLP advantage $\eta(k)$ 定义如下:

$$\eta(k) = Adv_T^{ECDLP}(AE)$$

$$= \Pr(EXP_T^{ECDLP}(AE) = 1) \quad (8)$$

给定椭圆曲线 T 及安全参数 1^k ,在合理的资源限制下(时间复杂度,询问的次数与长度)满足:对于任意 c 存在 k_c ,使得 $\eta(k) \leq k^{-c}$ 对于 $k \geq k_c$ 都成立,即 $Adv_T^{ECDLP}(A)$ 是可忽略的.

定义 3 椭圆曲线签密的机密性 设 ASC 是攻击椭圆曲线签密方案 Σ 机密性的算法,它可以访问 left-or-right 签密 oracle,并且输出一个比特.考虑如下试验:

$$\text{Experiment } EXP_{ESC}^{ind-cca2}(ASC)$$

$$(K, H, T) \leftarrow GC(1^k),$$

$$(sk_A, PK_A) \leftarrow GK(A, 1^k),$$

$$(sk_B, PK_B) \leftarrow GK(B, 1^k),$$

$$C' \leftarrow SC_{sk_A, PK_B}(LR(m_0, m_1, b)), b \leftarrow \{0, 1\},$$

$$b' \leftarrow ASC^{SC_{sk_A, PK_B}(LR(m_0, m_1, b)), USC(sk_A, PK_B)}.$$

If ASC 对于返回的签密文 $SC_{sk_A, PK_B}(LR(m_0, m_1, b))$ 询问 $USC(sk_A, PK_B)$, then return 0,

If $b' = b$ return 1 else return 0.

ASC 的 $ind-cca2$ advantage $\delta(k)$ 定义如下:

$$\delta(k) = Adv_{ESC}^{ind-cca2}(ASC) =$$

$$\Pr(EXP_{ESC}^{ind-cca2}(ASC) = 1) \quad (9)$$

签密方案是适应性选择密文下不可区分的,如果攻击者 ASC 的 $ind-cca2$ advantage $\delta(k)$ 在合理的资源限制下(时间复杂度,询问的次数与长度)满足:对于任意 c 存在 k_c ,使得 $\delta(k) \leq k^{-c}$ 对于 $k \geq k_c$ 都成立.

首先是机密性,本文提出的物联网安全通信及匿名通信方案是适应性选择密文下不可区分的,因为在 ECDLP 困难性基本假设之下,任何攻击者的 $ind-cca2$ advantage 在合理的资源限制下(时间复杂度,询问的次数与长度)是可忽略的,因此安全通信方案能够保证信息的机密性.

假设 2 (理想的散列函数) 散列函数具有 Random Oracle 的性质,即散列函数的输出是均匀随机分布的.

定义 4 椭圆曲线签密的不可伪造性: 设 $\Sigma = (GC, GK, SC, USC)$ 是一个椭圆曲线签密方案, AF 是一个能够访问签密 oracle 并且输出一个字符串的算法,考虑如下试验:

$$\text{Experiment } EXP_{ESC}^{uf-cma}(AF)$$

$$(sk_A, PK_A) \leftarrow GK(A, 1^k),$$

$$(sk_B, PK_B) \leftarrow GK(B, 1^k),$$

$$(m, C') \xleftarrow{\$} AF^{SC(sk_A, PK_B)}(PK_A, PK_B).$$

若下列条件满足 return 1, 否则 return 0:

(1) $m \leftarrow \text{USC}(sk_B, PK_A, C')$

(2) $m \in \text{Message}(sk_A, PK_B)$

(3) m 不是 AF 向签密 oracle 的询问

A 的 $uf\text{-}cma$ advantage $\epsilon(k)$ 定义如下:

$$\begin{aligned} \epsilon(k) &= \text{Adv}_{\text{ESC}}^{uf\text{-}cma}(\text{AF}) \\ &= \Pr(\text{EXP}_{\text{ESC}}^{uf\text{-}cma}(\text{AF}) = 1) \end{aligned} \quad (10)$$

椭圆曲线签密方案在选择消息攻击下是不可伪造的, 如果任何攻击者 AF 的 $uf\text{-}cma$ advantage $\epsilon(k)$ 在合理的资源限制下(时间复杂度, 询问的次数与长度)满足: 对于任意 c 存在 k_c , 使得 $\epsilon(k) \leq k^{-c}$ 对于 $k \geq k_c$ 都成立。

其次是不可伪造性, 本文提出的物联网安全通信方案是选择消息攻击下不可伪造的, 因为在理想散列函数及 ECDLP 困难性的基本假设之下, 任何攻击者的 $uf\text{-}cma$ advantage 在合理的资源限制下(时间复杂度, 询问的次数与长度)是可忽略的。因此, 文中的物联网安全通信及匿名通信方案能够保证物联网信息的不可伪造性。

最后是不可否认性, 可以证明: 存在确定性多项式时间算法使得可信第三方能够验证签密文, 因此文中方案满足不可否认性, 即安全通信及匿名通信方案保证了物联网信息交互的公平性^[7-8]。

5 方案的效率分析

我们将文中提出的方案与其他典型的方案进行效率对比分析。在传统的方案中, 协议方的交互需要签名、加密两个算法, 比较中我们选用典型的 ECD-SA 签名方案和 ElGamal 加密方案, 典型的 RSA 加解密与签名认证算法进行对比分析。在签密方案的计算量分析中, 模指数、模逆、椭圆曲线点加及椭圆曲线标量乘法由于其运算复杂, 应该作为分析计算的依据。而模加、模乘、hash 运算及对称加解密运算, 由于其运算量相对很小, 分析中可以忽略不计。

为了保证算法的基本安全性, 目前推荐的系统参数如下: 对于离散对数 $|p| = 1\,024$ bit, $|q| = 160$ bit; 对于 RSA, $|N| = 1\,024$ bit。而对于椭圆曲线密码 $|q| = 131$ bit (79, 109 bit 也是可行的), $|l| = 160$ bit。分组密码的分组长度是 64 bit (如 IDEA), 安全哈希函数的长度为 128 bit (如 MD5)。在以上最小安全参数下, 本文提出的物联网安全通信及匿名通信方案系统参数仅要求 160 bit, 其安全性就与 1 024 bit 的离散对数方案或者 1 024 bit 的 RSA 方案相当。方案在保证安全性的同时, 大大降低了系统软硬件实现时的计算量、通信量、存储量等

系统开销, 提高了物联网安全通信的效率^[9]。

6 结束语

签密能够在在一个算法步骤内同时实现加密与签名的功能, 而计算与通信量却远小于两者之和, 对于解决物联网通信中的安全与效率问题具有重要意义。研究适用于物联网环境的签密算法, 并将其应用于物联网安全协议是密码学的一个重要研究方向, 它不仅是密码学的研究需要, 更是物联网飞速发展的迫切需要。文中基于椭圆曲线密码提出了适用于物联网安全通信与匿名通信方案同样适用于其他计算、存储能力和集成空间有限、带宽受限、要求高效率实现的其他环境, 有广阔的应用前景。

参考文献:

- [1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost (encryption) [C] // CRYPTO'97. Berlin: Springer-Verlag, 1997: 165-179.
- [2] Xuanwu Zhou, Zhigang Jin. Short signcryption scheme for the internet of things [J]. Informatica, 2011, 35(4): 521-530.
- [3] Xiangxue Li, Haifeng Qian, Jian Weng, et al. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model [J]. Mathematical and Computer Modelling (S0895-7177), 2013, 57(3/4): 503-511.
- [4] Zhao Xiufen, Xu Qiuliang. An efficient multi-PKG ID-based signcryption scheme [J]. Journal of Computer, 2012, 35(4): 673-681.
- [5] Li F, Muhaya F B, Zhang M, et al. Efficient identity-based signcryption in the standard model [C] // Proceedings of ProvSec 2011, LNCS6980. Berlin: Springer-Verlag, 2011: 120-137.
- [6] Huixian Li, Xubao Chen, Liaojun Pang, et al. Certificateless multi-receiver signcryption scheme based on multivariate public key cryptography [J]. Journal of Computer, 2012, 35(9): 1881-1889.
- [7] Xuanwu Zhou, Zhigang Jin, Yan Fu, et al. Dynamic multiple signature with provable security [J]. Journal of System Simulation, 2012, 24(11): 2353-2355.
- [8] Kim I T, Hwang S O. An efficient identity-based broadcast signcryption scheme for wireless sensor networks [C] // Proceedings of 6th International Symposium on Wireless and Pervasive Computing. Beijing, 2011: 1-6.

(下转第 31 页)

nection Update Per Second, CUPS)定义为神经网络每秒钟内可以更新的权值和偏置项的数目。

未使用浮点加速时,参考文献[5]中, 2×3 的结构前向传播的发射频率(Shooting Frequency)为 145 Hz,连接的总数目为 60 000,故其每个核的 CPS 为 1 450 000。

各系统性能对比见表 2。其中,参考文献[5]中的 NoC 平台不具备在线学习的功能,因此其 CUPS 项的数据无效。图 6 为归一化的性能比较图,其中以本系统的性能表现为基准,将其他两个系统的性能进行了归一化表示。

表 2 MPSoC 实现 MLP 性能对比

平台	总连接数	CPS	CPSPC	CUPS
参考文献[6]	67	115 000	115 000	N. A
参考文献[7]	60 000	8 700 000	1 450 000	N. A
本文	3 849	27 069 840	1 691 865	42 949 672

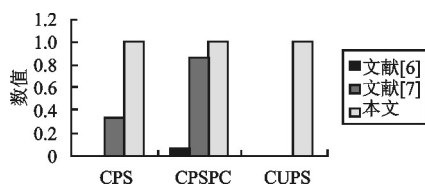


图 6 归一化性能比较

从图 6 中可以看出,未使用硬件浮点加速时,相比于其他两个系统,本系统具有最高的 CPS 值,以及 CPSPC 值,表明本系统性能优于其他两个系统。

5 结束语

基于多核处理器结构和并行编程模型的思想,本文设计并实现了多层感知神经网络。本文所设计的基于多核处理器的多层感知神经网络具有良好的可重构性,编程模型简单,易于维护和扩展。实验结果表明,本文设计的多层感知神经网络具有良

好的性能表现,满足实时性要求,为神经网络在其他

领域的使用提供了良好的解决方法。

参考文献:

- [1] Bengio Y. Learning deep architectures for AI[J]. Foundations and trends in Machine Learning, 2009, 2 (1): 1-127.
- [2] GironÉS R G, Palero R C, Boluda J C, et al. FPGA implementation of a pipelined on-line backpropagation [J]. Journal of VLSI signal processing systems for signal, image and video technology, 2005, 40 (2): 189-213.
- [3] Yiping D, Takahiro W. High performance NoC architecture for two hidden layers BP Neural Network[J]. IEEE, 2008(1):269-272.
- [4] Men shen T, Yao hsien F. Implementation of high performance hardware based toroidal neural network with learning capability[C]//proceeding of the Advanced Intelligent Mechatronics 2009, Singapore, 2009: 180-185.
- [5] Mand N P, Robino F, Oberg J. Artificial neural network emulation on NOC based multi-core FPGA platform[J]. Norchip, 2012(4):4-7.
- [6] Mitcheli T. 机器学习[M]. 曾华军, 张银奎, 译. 北京:机械工业出版社, 2008.
- [7] Duda R O, Hart P E, Stork D G. 模式分类[M]. 李宏东, 译. 北京:机械工业出版社, 2003.
- [8] Dias F M, Antunes A, Mota A M. Artificial neural networks: a review of commercial hardware[J]. Engineering Applications of Artificial Intelligence, 2004, 17(8): 945-952.

作者简介:

朱新召 男, (1990-), 硕士研究生. 研究方向为集成电路工程。

(上接第 26 页)

- [9] 周宣武. 具有附加性质的签密方案及其应用研究[D]. 天津:天津大学, 2013.

作者简介:

周宣武 男, (1980-), 博士后. 研究方向为密码学与信息安全。

付 燕 女, (1985-), 博士研究生. 研究方向为可信计算。

金志刚 男, (1973-), 教授, 博士生导师. 研究方向为计算机网络与信息安全。

刘开华 男, (1956-), 教授, 博士生导师. 研究方向为计算机网络、软件无线电技术。

李 欣 男, (1965-), 副教授. 研究方向为网络安全。