一种改进的并行签密方案

任 参,刘少君,黄道平
(华南理工大学 自动化科学与工程学院,广东 广州 510640)

摘 要:为了缩减"最优并行签密"的数据冗余并提高其效率,在不损害原方案安全性的前提下,利用信息分散算法(IDA),提出了一种改进的并行签密方案。所构建方案的密文长度几乎最优,其约等于最小长度和一小段附加信息的集合,其中附加信息只取决于安全系数而不取决于明文长度。同时,改进并行签密方案保留了"最优并行签密"的优点:在签密和解签密过程均可并行处理,允许使用所有适合的加密和签名算法,且只需要很低的安全性要求。故,尤其在长消息签密中,方案能够更好地满足应用需求。

关键词:签密;并行;密码学;信息安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2010)04-0151-04

An Improved Parallel Signcryption Scheme

REN Shen, LIU Shao-jun, HUANG Dao-ping
(Dept. of Automation, South China University of Technology, Guangzhou 510640, China)

Abstract: In order to reduce the message redundancy of the "Optimal Parallel Signcryption" and make it more efficient, proposed a improved parallel signcryption scheme by using information dispersal algorithms, while leaving the security conclusions intact. The size of the signed-ciphertext is nearly minimal; it is equal to the minimal bound plus a piece of information whose length does not depend on the secret size but on the security parameter. Besides, the improved parallel signcryption scheme preserve the original advantages of "Optimal Parallel Signcryption": signcryption and de-signcryption both in parallel, any suitable encryption and signature schemes could be used, very weak security requirement of the shemes. Therefore, the proposition could be more applicable especially when used in long-message signcryption.

Key words: signcryption; parallel; cryptography; information security

0 引 言

随着当今互联网与多媒体技术的发展,视频电话、远程会议、网络电视等远距离通信技术逐渐走入人们主流视野。这就要求密码学在满足传统的数据传输安全的同时,满足对身份验证的要求。1997年,为了适应这种要求,Zheng提出了签密的概念[1],它在一个逻辑步骤内可同时完成加密和签名两个功能,在计算时间和消息扩展率方面要远远低于"加密后签名"(EtS)或"签名后加密"(StE)的方法。在此之后,许多签密方案纷纷出现。与此同时,由于互联网传输在大多数时间做的是实时在线的处理,对于大规模数据的加密与多用户身份的验证有很高的效率要求。根据文献[2],提高密码转换效率有两种观点:一是设计更快的加密算法;二是设计并行处理方案,使得耗费大的加密部分与签名部分(或解密部分与签名验证部分)能够同时并行的处理,从而减少所耗时间,提高效率。前者在大多数情况下是不甚现实的,因为一个加密算法从设计出来,经过无数的修改验证,直到形成标准,需要一个很长的时间过程。故选择后者作为提高效率的方法。

密码方案的效率包括计算、传输和存储所需要的代价,称一种方案优于另一种是指其计算代价和传输带宽要求较小。相对于原始消息引入消息扩展率后,利用密码技术对消息进行操作的代价是用消息的扩展率和接收发送双方的计算时间来度量的。当必须保密的数据长度增加,系统的计算代价和传输代价上升,安全级别则随之降低。故在进行密码方案设计时,应尽量缩减所要加密或签密的数据冗余,从而提高效率与安全性。文中构建了一种基于信息分散算法(IDA)的并行签密改进方案。与改进前的"最优并行签密[2]"相比,在保证安全性的同时大幅度降低了消息扩展率,从而在对长消息签密时具有更高的实用价值。

收稿日期:2009-07-13;**修回日期**:2009-10-06
作者简介:任 参(1987-),女,河南新乡人,硕士研究生,研究方向为信息安全、软件安全、插补算法等;黄道平,博士生导师,博士,研究方向为神经网络、Matlab教学与仿真等。

1 有关签密以及并行处理的基本原理与相关研究

1.1 签密的基本概念

传统的密码学中,加密和身份验证是不可分割的,直到公钥密码体系的出现将两者分开。于是,加密和签名方案成为分别用于满足私密性和真实性的基本密码学工具。然而在许多情况下,需要同时满足私密性和真实性,且需要使用到公钥体系,如网络会议或安全 E-mail。于是,Zheng 在 1997 年提出了签密的概念[1],目的在于构建一种效率更高的加密与签名复合体系。在之后的研究中,签密成为能够同时满足私密性与真实性的复合体系的统称。

1.2 签密模型

签密方案模型由以下三个算法定义而成[3]:

1)GenSigEnc:密钥生成算法。通过安全参量 k,输出一对公钥密钥(SDK,VEK)。SDK 是用于签名/解密的密钥,VEK 是用于验证/加密的公钥。

2)SigEnc:加密签名算法。通过接收端的公钥 VEK_R 和发送端的密钥 SDK_S,由明文 m 产生密文 $c = SigEnc_{SDK_S VEK_R}(m)$。

3)VerDec:验证解密算法。通过接收端的密钥 SDK_R 和发送端的公钥 VEK_S,由密文 c 恢复为明文 $m = VerDec_{SDK_R VEK_S}(c)$。如果不能解密或验证不通过,则返回错误信息。

当签密方案的加密部分保证不可分辨性(Indistinguishability),签名部分能够抵御存在伪造(Existential Forgery)时,方案可证明为安全。

1.3 并行签密的相关研究

并行处理方式的概念首先是由文献[3]提出的,作为区别有着严格先后顺序的"加密后签名"(EtS)或"签名后加密"(StE)的方式而存在。最简单的并行签密即为明文同时进行加密和签名(E&S)。这种方案虽然使得耗费较大的加密部分和签名部分并行处理,大幅度提高了效率,但签名过程却容易透露明文信息,影响了其安全性[4]。

另一种并行签密方案叫做"委托后加密并签名[3]"(CtE&S)。这种方案首先对明文 m 进行委托和解委托,生成一对结果(c,d),之后将 d 加密成 e,将 c 签名成 s,这个过程可并行处理。密文的恢复可以通过验证 (c,s) 合法后,对 e 解密出 d 后,由解委托结果 d 恢复明文 m。这种方案经验证是安全的,但只有签密过程可并行处理,且解签密过程中由 d 恢复到 m 的过程效率很低。

随后,一种在签密和解签密过程中都可并行处理的"最优并行签密[2]"(Optimal Parallel Signcryption)出现了。这种设计采用散列函数、Shamir 的秘密分享方案[5]和拉格朗日插值法作为 CtE&S 中的委托部分。在这种方案中,签密过程和解签密过程均可并行处理,从而提高了效率。然而由于 Shamir 秘密共享方案的特性,"最优并行签密"的密文长度相对于明文长度扩展了 2 倍以上,严重增加了数据冗余。

文中的并行签密方案基于"最优并行签密"设计,在签密和解签密过程中都可并行处理,同时在不损害方案安全性的前提下,缩减数据冗余,使得密文长度几乎达到最小。即,密文长度约等于最小长度和一小段附加信息的集合,其中附加信息只取决于安全系数而不取决于明文长度。从而在长信息签密中,大规模缩减了计算和传输代价。

2 改进的并行签密方案

"最优并行签密[2]"方案的设计中采用了 Shamir 的完美秘密分享方案[6],保证了在理论信息层面,单个分享不会透露明文的任何信息。然而,在这种方案下,每份分享的长度都会大于明文的长度,从而在接下来的签密环节和传输环节大大影响了效率。文中采用了 M.O.Rabin 的信息分散算法(IDA)[5]、对称加密模块和完美秘密分享方案构建方案,保证了单个分享不会透露明文信息,同时分享长度大规模缩短。

信息分散算法的设计是用于在数量为 n 的活动接收者中分享信息,当 m 个活动接收者提交合法分享时可重构信息,且接收者诚实,所提交信息未被修改,其中参数 $1 \leq m \leq n$。基本思想是对所分享信息 F 加入冗余,之后将其分成 n 份分别传送给对应接收者。存在 m 份合法分享时可重构信息,且每份分享长度为最优的 $\frac{|F|}{m}$。信息分散算法有多种实现形式[5,7],均可应用于方案中间。

为完整起见,此处简述基于里德所罗门纠删码(Reed Solomon erasure codes)的简单信息分散算法。所分享信息被分成相等的 m 份,其中每一份信息都是有限集的元素。这 m 个元素构成了 $m-1$ 阶多项式的系数,用于分享的 n 个部分则是求该多项式在 n 个不同点的值。从而,通过 m 份分享可插值得到原多项式。信息分散算法和完美秘密分享方案的区别在于分享信息是由系数而不是由整个多项式表示。然而,通过与安全的对称加密模块和完美秘密分享方案相连接后,可保证 $m-1$ 份分享不会透露任何明文信息。

改进方案的具体构成如下:

(1) 加密方案,其中包括 5 个算法部分:密钥生成

(GenEnc)、加密算法(Enc)、解密算法(Dec)、对称加密算法(SymEnc)、对称解密算法(SymDec);

(2) 签名方案,其中包括 3 个算法部分:密钥生成(GenSig)、签名算法(Sig)、验证算法(Ver);

(3) 信息分散算法 IDA:包括分割和重构两部分;

(4) 三个散列函数序列 f、g、h(假设其工作状态类似于随机预言模型[8])。

将以上各算法组合起来,构成文中所设计的并行签密方案如下:

1) 密钥生成部分:$\mathrm{GenSigEnc}(1^k) = \mathrm{GenSig} \times \mathrm{GenEnc}(1^k)$

通过签名密钥生成算法 GenSig 和加密密钥生成算法 $\mathrm{GenEnc}(1^k)$ 产生 $(pk_1, sk_1)(pk_2, sk_2)$,且密钥 $\mathrm{SDK} = (sk_1, sk_2)$,公钥 $\mathrm{VEK} = (pk_1, pk_2)$。

2) 加密签名部分:$\mathrm{SigEnc}_{\mathrm{SDK}_S \mathrm{VEK}_R}(m)$

其中 m 为发送端欲加密并签名的明文,SDK_S 为发送端的签名密钥,VEK_R 为接收端的加密公钥,之后分为五个步骤。

a) 选择对称加密密钥 K,对明文 m 进行对称加密,$E = \mathrm{SymEnc}_K(m)$;

b) 采用信息分散算法 IDA 将 E 分割成 2 份:E_1,E_2;

c) 采用 OAEP 模块,计算 $r_1 = E_1 \oplus f(E_2)$,$r_2 = E_2 \oplus g(r_1)$;

d) 采用(2,2) 的 Shamir 完美秘密共享方案,构造多项式 $F(x) = K + h(K)x$。取 x 分别等于 1、2,带入上式,得 $k_1 = F(1)$,$k_2 = F(2)$;

e) 并行计算 $c_1 = \mathrm{Enc}(r_1)$,$c_2 = \mathrm{Sig}(r_2)$,$c_3 = \mathrm{Enc}(k_1)$,$c_4 = \mathrm{Sig}(k_2)$,得密文 c_1、c_2、c_3、c_4 并发送到接收端。

3) 解密验证部分:$\mathrm{VerDec}_{\mathrm{SDK}_R \mathrm{VEK}_S}(c_1, c_2, c_3, c_4)$

其中 c_1、c_2、c_3、c_4 为接收端欲解密和验证身份的密文,SDK_R 为接收端的解密密钥,VEK_S 为发送端的验证公钥,之后分为五个步骤。

a) 并行计算 $r'_1 = \mathrm{Dec}(c_1)$,$r'_2 = \mathrm{Ver}(c_2)$,$k'_1 = \mathrm{Dec}(c_3)$,$k'_2 = \mathrm{Ver}(c_4)$,如解密或验证不成功则给出错误信息并退出;

b) 利用拉格朗日插值法将 $(1, k'_1)$、$(2, k'_2)$ 插值为多项式 $\tilde{F}(x) = a_0 + a_1 x$,若 $a_1 = h(a_0)$,则对称解密密钥 $K = a_0$,如非则返回错误信息;

c) 计算 $E_2 = r'_2 \oplus g(r'_1)$,$E_1 = r'_1 \oplus f(E'_2)$;

d) 利用 IDA,将 E_1,E_2 重构为 E;

e) 利用以上所得的 K,获得明文信息 $m = \mathrm{SymDec}_K(E)$。

3　性能与安全性分析

3.1　改进方案的性能分析

"最优并行签密"实现了在签密和解签密过程中,所消耗时间约为单独运行加密和签名部分(或解密和验证部分)时两部分的最大值。即:

$\mathrm{Time}(\mathrm{Enc} \,\&\, \mathrm{Sig}) \approx \max(\mathrm{Time}(\mathrm{Enc}), \mathrm{Time}(\mathrm{Sig}))$

$\mathrm{Time}(\mathrm{Dec} \,\&\, \mathrm{Ver}) \approx \max(\mathrm{Time}(\mathrm{Dec}), \mathrm{Time}(\mathrm{Ver}))$

且在并行计算加密和签名部分前仅有一个 OAEP 模块,一个散列函数和其他相关操作。文中改进的并行签密方案比较"最优并行签密"仅多了一个对称加解密算法和一个信息分散算法 IDA。在签密方案的效率考量方面,公钥算法中的模指数运算是最主要的运算。相对于模指数运算,对称加解密算法和 IDA 的计算量均可忽略不计。

与此同时,改进算法中明文的分割序列 E_1,E_2 比较"最优并行签密"中利用完美秘密共享方案的分割序列,其长度缩减了约一半左右。这在接下来的并行签密过程中大大减少了运算量,并减小了所需传输密文的长度。

3.2　改进方案的安全性分析

文献[9]中已证明,当对称加解密算法安全,且其密钥采用完美信息分享方案分割时,利用 IDA 进行信息分享语义安全。即,在计算层面上,两份分享可以还原出原信息,而单份分享则不会透露原信息的任何内容。完美信息分割保证了密钥 K 的安全,故改进方案所采用的方法在安全性上不弱于"最优并行签密"。

改进的并行签密方案本身只需要安全级别很低的算法(如普通 RSA 加密或 RSA 签名)即可满足安全性要求。

定理一　假设改进的并行签密方案所使用的加密算法满足确定性和单向抵抗选择明文攻击(OW-CPA),签名算法可在随机信息攻击下抵御全局伪造(NUF-RMA),则方案安全(IND/NEF)。

证明过程可分为两部分,第一部分证明方案满足不可分辨性(IND),第二部分则证明其能抵御存在伪造(NEF),证明过程假设散列函数随机。

由于随机预言模型 f,g 的随机性,欲破解不可分辨性获得部分明文信息,攻击者必须从密文、明文与随机序列中获取 E_1、E_2、k_1、k_2 的信息。欲获得 E_1、E_2,只可能通过问询 g 得到 r_1,如此则须首先破解满足 OW-CPA 的加密算法(GenEnc、Enc、Dec);欲获得 k_1、k_2,攻击者须破解加密算法或问询散列函数 $h(K)$。根据文献[2]中的证明方法,可证明方案满足不可分辨性。

为了达到对指定信息产生正确签名的目的,攻击者首先须对 SigEnc、VerDec 问询从而获得合法的签密

$(c_1、c_2、c_3、c_4)$，破解OAEP和抵御NUF－RMA的签名算法，从而得到可能正确的签名对$(r_2,c_2)(k_2,c_4)$。通过文献[2]可得，方案可抵御存在伪造，故定理一成立。

4 结束语

文中在不影响方案安全性的前提下，对J. Pieprzyk所提出的“最优并行签密”进行了改进，大规模地缩减了签密过程中的数据冗余和密文长度，使得密文长度几乎最优，从而有效地提高了方案效率。同时它保留了“最优并行签密”原有的优点：可以在签密和解签密过程中并行处理，方案的普遍性允许使用所有适合的加密和签名算法，且对所使用算法只需要很低的安全性要求(OW－CPA&NUF－RMA)。因此，改进方案可更好地满足应用需求。

参考文献：

[1] ZHENG Y. Signcryption or How to Achieve Cost (Signature & Encryption) ≪ Cost (Signature) + Cost (Encryption) [C]//Crypto 1997, LNCS 1294. Berlin: Springer－Verlag, 1997:165－179.

[2] Pieprzyk J, Pointcheval D. Parallel Authentication and Public－Key Encryption [C]//ACISP 2003, LNCS. Berlin: Springer－Verlag, 2003:387－401.

[3] An J H, Dodis Y, Rabin T. On the Security of Joint Signatures and Encryption[C]//Eurocrypt 2002, LNCS 2332. Berlin: Springer－Verlag, 2002:83－107.

[4] Bellare M, N amprempre C. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm[C]//Asiacrypt 2000, LNCS Vol. 1976. Berlin: Springer, 2000:531－545.

[5] Rabin M O. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance[J]. Journal of ACM, 1989, 36(2):335－348.

[6] Shamir A. How to Share a Secret[J]. Communications of the ACM, 1979, 22:612－613.

[7] Krawczyk H. Distributed Fingerprints and Secure Information Dispersal[C]//Proceedings of 12th PODC. New York: ACM press, 1993:207－218.

[8] Bellare M, Rogaway P. Random Oracles Are Practical: a Paradigm for Designing Efficient Protocols[C]//Proceedings of the 1st CCS. New York: ACM Press, 1993:62－73.

[9] Krawczyk H. Secret Sharing Made Short[C]//Advances in Cryptography－CRYPTO 93. Berlin: Springer, 1994:136－146.

(上接第 150 页)

然，本算法也有一定的局限性。当抓取的点不在血管交叉点或分支处时，会出现找错最佳匹配点的情况，从而导致拼接精度降低。

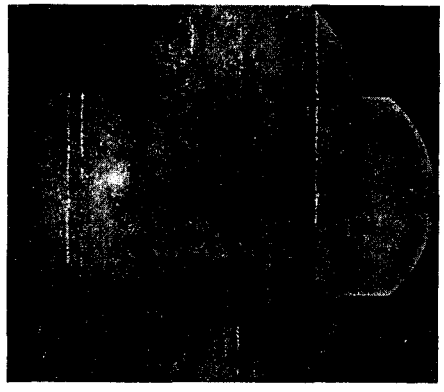

图 5 拼接效果图

3 结束语

由于眼底图像对灰度的敏感性，直接采用模板匹配法对眼底图像进行拼接，可能造成误匹配，且计算量太大。文中根据眼底图像血管信息丰富的特点，提出先抓取初始匹配点，然后在小区域内用模板匹配法的原理找到最佳匹配点，再通过重叠区域线性过渡的方法消除拼缝，最终实现拼接的方法。经实验验证，此方法拼接精度高，且易于实现。

参考文献：

[1] 宋余庆. 数字医学图像[M]. 北京：清华大学出版社，2008.

[2] 解 凯，郭恒业，张田文. 图像 Mosaics 技术综述[J]. 电子学报，2004，32(4)：630－634.

[3] 徐正光，田 清，张利欣. 图像拼接方法探讨[J]. 微计算机信息，2006，22(30)：255－256.

[4] 张少辉，沈晓蓉，范耀祖. 一种基于图像特征点提取及匹配的方法[J]. 北京航空航天大学学报，2008，34(5)：516－519.

[5] 李 寒，牛纪桢，郭 禾. 基于特征点的全自动无缝图像拼接方法[J]. 计算机工程与设计，2007，28(9)：2083－2085.

[6] 胡社教，涂桂林，江 萍. 基于灰度相关图像拼接的改进算法[J]. 合肥工业大学学报：自然科学版，2008，31(6)：863－865.

[7] 高 军，李学伟，张 建，等. 基于模板匹配的图像配准算法[J]. 西安交通大学学报，2007，41(3)：307－311.

[8] Stewart C V, Tsai Chia－Ling, Roysam B. The Dual－Bootstrap Iterative Closest Point Algorithm with Application to Retinal Image Registration[J]. IEEE Transactions on Medical Imaging, 2003, 22(11):1379－1394.