基于双管道结构的在线加密方案

眭 晗 吴文玲 张立廷

(中国科学院软件研究所可信计算与信息保障实验室 北京 100190)

摘 要 在线加密以串行的方式逐块处理输入,为数据提供安全性保护.近年来,设计具有在线性的认证加密方案成为研究热点,大量基于分组密码或固定置换设计的在线认证加密方案被提出.压缩函数和杂凑函数在信息安全领域具有广泛的应用基础,目前却少有方案基于此进行构建.该文选取压缩函数作为底层模块,通过对杂凑函数基本结构之一的双管道结构进行适应性的修改,解决了加密过程中状态链值泄露与安全性需求之间的矛盾,提出了一族基于压缩函数与双管道结构构建的具有在线性的加密方案,称为 DPE.DPE 族方案适用于具有压缩函数或基于压缩函数构建的杂凑函数的应用背景的环境,为数据提供机密性和完整性的保护.具体地,我们提出三个方案,分别是 DPE、DPAE 和 DPAE-I.DPE 方案是在线加密方案,可以提供在线加密和在线解密的功能,利用底层压缩函数的迭代更新状态链值,并截取部分状态链值作为密钥流进行加密和解密操作;DPAE 方案是在线认证加密方案(OAE1 方案),在 DPE 方案的基础上添加了认证操作,使得消息的接收方可以利用标签验证消息的完整性;DPAE-I 方案是在线的分块认证加密方案(OAE2 方案),利用 DPAE 方案支持使用中间标签的性质,将长消息划分为若干个短消息调用 DPAE 进行加密,将每一个短消息视为一个分块.前一个分块加密得到的状态将作为加密下一个分块的初始状态,当工作存储足够大时,DPAE-I 方案可以在加密和解密方向同时具有在线性.为降低软硬件实现代价,当压缩函数满足输出长度是输入长度一半时,可以使用一个底层压缩函数以及一个密钥实现该族方案.该族方案继承了压缩函数与基于压缩函数构造的专用杂凑函数单向性好、运行速度快等特点,同时具有在线性、灵活性、适应性以及安全性强 4 个主要特点:(1)当工作存储足够大时,DPE 族方案可以在读取输入分块后,计算并输出相应的分块;(2)根据用户对数据机密性和完整性保护的不同需求,可以通过简单的操作实现族内不同类型方案之间的转换;通过选择不同的底层压缩函数,可以在方案的数据吞吐率与安全性之间进行调节;(3)可以使用 SHA-256、SHA-512、WHIRLPOOL 以及 SM3 等杂凑函数中的压缩函数作为底层模块;(4)借由压缩函数的特点,相比于基于分组密码构造的认证加密方案,该族方案可以通过使用规模大的压缩函数作为底层模块为数据提供更强的安全性保护;另一方面,借由双管道结构的特点,相对于同类基于压缩函数构建的方案,该族方案在安全性上同样具有一定的优势.

关键词 在线加密;认证加密;在线认证加密;双管道结构;压缩函数

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2018.01143

Double-Pipeline Online Encryption

SUI Han WU Wen-Ling ZHANG Li-Ting

(*Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

Abstract An online cipher supplies data incrementally in a serial fashion, and ensures data security. In recent years, designing authenticated encryption schemes with online property has become popular, and many online authenticated encryption schemes based on blockciphers and permutations have been proposed. Compression functions and hash functions are applied widely in information security, while few of schemes are built with them. In this paper, the authors take compression functions as the underlying primitive, a family of online scheme to be given. By

收稿日期:2016-08-15;在线出版日期:2017-08-19.本课题得到国家自然科学基金(61672509,61572484)、国家密码发展基金(MMJJ20170101)资助.**眭 晗**,女,1986 年生,博士研究生,主要研究方向为可证明安全理论、认证加密方案的设计与分析.E-mail:suihan@tca.iscas.ac.cn.**吴文玲**,女,1966 年生,博士,研究员,博士生导师,主要研究领域为分组密码的设计与分析、分组密码工作模式和可证明安全理论的研究.E-mail:wwl@tca.iscas.ac.cn.**张立廷**,男,1982 年生,博士,副研究员,硕士生导师,主要研究领域为可证明安全理论、消息鉴别码与认证加密方案的设计.

modifying the double pipe construction which is one of basic constructions of hash functions, this paper solves the contradiction between state leakage and security requirement in encryption, and proposes a family of online ciphers, called DPE, based on compression function and double pipe construction. The DPE family is dedicated to applying conveniently in environments which already have components such as compression function-based hash functions or compression functions, and is shown to preserve privacy and integrity of data. Practically, we present three family members, i. e., DPE, DPAE, and DPAE-I. DPE is an online cipher, providing online encryption and online decryption. States update with calling for underlying compression functions, and parts of the states are used as a key stream which will be exclusive-or with plaintext to generate ciphertext in enciphering, and exclusive-or with ciphertext to generate plaintext in deciphering. DPAE is an online authenticated encryption scheme (an OAE1 scheme), based on DPE, which adds an extra authenticating process and in which a receiver could ensure integrity of a message by verifying its tag. DPAE-I is a segment online authenticated encryption scheme (an OAE2 scheme). With respect to DPAE's property of incremental tags acceptable, DPAE-I partitions long messages into several short messages, which can be seen as segments and encrypted with DPAE. The internal state after encrypting a former segment will be used as the initial state for encrypting a latter message. When work memory is large enough, DPAE-I is online in both encryption and decryption. To reduce the cost of hardware and software, when the output length of the compression function is half of the input length, we use one single underlying compression function and one key to build a scheme of the DPE family. The DPE family inherits characteristics of compression functions and dedicated hash functions based on compression functions, such as one-way and high-efficiency. The properties of the family include online, flexible, adoptable, and high secure: (1) When work memory is large enough, a scheme in DPE family calculates and outputs the corresponding segment after reading input segment. (2) Users transports one scheme into another in the family by simple operations according to needs for confidentiality and integrity protection; and adjusts between efficiency and security of a DPE/DPAE scheme by flexibly choosing different compression functions. (3) Compression functions used in hash functions, such as SHA-256, SHA-512, WHIRLPOOL and SM3, are adoptable as the underlying primitive. (4) Higher security protection is provided by the DPE family with large scale compression functions, compared with those schemes based on blockciphers; and with the use of the double pipeline structure, the family has some advantages in the security over other schemes based on compression functions.

Keywords online cipher; authenticated encryption; online authenticated encryption; double-pipeline construction; compression function

1 引 言

在线算法,指可以用串行的方式逐块地处理输入,换言之,算法无需在开始执行时就获得全部输入,它可以在读取 t 个输入块之后就相应地输出 t 个块. 相应地,在线加密应该可以在获知输入块 $M_1 \cdots M_i$ 之后计算出输入块 C_i;而在线解密应该可以在获知输入块 $C_1 \cdots C_i$ 之后计算出 M_i.

遵循这个原则,2001 年,Bellare 等人[1]形式化地定义了在线加密(online cipher)的概念,并提出了第一个在线加密方案 HCBC. 2012 年,Fleischmann 等人[2]将在线加密的定义与密文完整性的定义相结合,首次提出在线认证加密(Online Authenticated Encryption,OAE1)的概念. 在这一概念下,包括 McOE[2]、COPA[3]、COBRA[4]等在内的一系列认证

加密方案被提出. 2014 年，在针对认证加密算法开展的 CAESAR① 竞赛的第一轮候选方案中，有 50 个方案声称具有在线性.

然而，受密文末尾跟随标签这一形式的限制，OAE1 在解密方向并不能实现在线. 即 M_i 可以根据 $C_1 \cdots C_i$ 计算得到，但需要在末尾的标签验证通过后才能被输出. 针对 OAE1 存在的问题，Hoang 等人[5] 于 2015 年提出了 OAE2 的概念，要求方案在加密和解密方向同时满足在线的性质.

杂凑函数是将任意长度的数据映射到固定长度的一类函数，被应用于数字签名、消息认证码以及数据库检索等多个领域. 基于压缩函数构建的杂凑函数作为其中的重要类别有着广泛的应用背景，其中包括国际标准 ISO/IEC 10118-3：2004 中推荐的 RIPEMD-160、RIPEMD-128、SHA-1、SHA-256、SHA-512、SHA-384 和 WHIRLPOOL 以及国密算法 SM3 等. 针对使用杂凑函数的应用环境，将杂凑函数或其中的压缩函数，作为底层模块设计密码方案，可以降低新密码方案的实现代价. 在目前已公布的认证加密方案中，基于压缩函数构建的方案包括结合压缩函数与分组密码构建的方案 HBS[6]、基于压缩函数构建的 MD 结构方案 OMD[7-8] 与 FWPAE[9] 以及基于 TriviA-SC 和 VPN-Hash 构建的流密码算法 TriviA-ck[10].

另一方面，Hoang 等人[5] 在提出 OAE2 的概念的同时提出了两种将现有方案转化为 OAE2 的协议：CHAIN 和 STREAM，前者可以将抵抗重用的认证加密方案转化为 OAE2 方案，后者可以将基于唯一值的认证加密方案转化为基于唯一值的 OAE 方案. 协议的实现需要根据原始方案构造一个编码函数，而通用的构造方法在文中并没有给出. 换言之，目前仍未有满足 OAE2 定义并被证明是 OAE2-安全的方案被正式提出.

我们希望构造一个新的认证加密方案，其底层模块仅为杂凑函数或压缩函数，并结合不同结构的特点，使得新方案能够适用于具有杂凑函数应用基础的环境，并且可以扩展为一个 OAE2 方案.

本文提出了一族基于压缩函数和双管道结构设计的在线加密方案，称为双管道加密方案(Double-Pipeline Encryption，简称 DPE). 该族方案包含三类方案，分别提供加密或认证加密的功能，包括 DPE、DPAE 和 DPAE-I. 其中，DPE 为在线加密方案，DPAE 与 DPAE-I 为认证加密方案. DPAE 仅在加密方向具有在线性，满足 OAE1-安全；DPAE-I 在加密和解密方向上均具有在线性，满足 OAE2-安全.

DPE-族方案具有在线性、灵活性和适应性三个主要特点. 在线性表现在：当工作存储足够大时，DPE-族方案可以在读取输入分块后，计算并输出相应的分块. 其灵活性表现在两方面：根据用户对数据机密性和完整性保护的不同需求，可以通过简单的操作实现三类方案之间的转换；通过选择不同的底层压缩函数，可以在方案的数据吞吐率与安全性之间进行调节. 适应性表现在：可以使用国际标准 ISO/IEC 10118-3：2003 中推荐的杂凑算法 SHA-256、SHA-512、WHIRLPOOL 以及国密算法 SM3 等杂凑函数中的压缩函数作为底层模块.

双管道结构(double-pipe construction)来自于杂凑函数的结构设计，此前并未被应用于设计加密方案或认证加密方案. 在该结构中，每次并行地调用两个压缩函数，将输出两个压缩值作为状态链值，每块消息与两个压缩值分别级联作为两个压缩函数的输入. DPE-族方案利用双管道结构的特点，使用两个带密钥的压缩函数作为底层模块，要求两个压缩函数满足以下性质：输入长度相同，并且输出长度之和等于输入长度. 将两个压缩函数的输出 (A, B) 作为方案中的状态链值. 与利用双管道结构构造杂凑函数时的链值组成不同，DPE-族方案将 A 作为外部状态，与明文分组进行异或得到密文并输出，B 作为内部状态不进行输出以保证方案的安全性. 为降低软硬件实现代价，当压缩函数满足输出长度是输入长度一半时，可以仅使用一个底层压缩函数以及一个密钥实现该族方案.

在线加密方案 DPE 中包括两个阶段：第一阶段输入唯一值(nonce)并利用压缩函数对初始状态进行更新，获得初始化后的状态；第二阶段，将明文分组与外部状态异或生成密文分组并输出，同时将新的外部状态与内部状态输入压缩函数，更新状态链值. OAE1 方案 DPAE 则是在 DPE 的基础上添加了第三阶段，将外部链值输出作为标签，以实现认证的功能. 如果我们将生成标签之后的状态链值作为新的初始状态，用于加密下一组明文，则此时的标签被称为中间标签(intermediate tags). 将每组明文视为一个分块(segment)，并将相应的密文与标签视为带扩展的密文，则可以将 DPAE 自然地转化为一个分块认证加密方案，并可以证明方案达到

① Competition for authenticated encryption: Security, applicability, and robustness(CAESAR). https://competitions.cr.yp.to/caesar.html 2012,7,5

OAE2-安全.

当使用的两个带密钥的底层压缩函数相互独立且随机时,加密方案 DPE 可以为消息提供机密性保护,OAE1/OAE2 方案 DPAE 可以为消息提供机密性与完整性的保护.并且通过选择具有不同输入输出长度的压缩函数作为底层模块,可以在方案的数据吞吐率与安全性之间进行调节.

此外,我们讨论了使用压缩函数作为底层模块的原因;并将 DPE 族方案与同类的方案进行比较,指出该族方案在对压缩函数的适应性和安全性上都具有一定的优势.

2 相关工作

2011 年,Bertoni 等人[11]基于带密钥的海绵结构设计了一个基于固定置换的认证加密方案 SpongeWrap,其结构 Duplex 之后被广泛应用于认证加密方案的设计,包括 APE[12]、Jambu[13]、Artemia[14-15]、Ascon[16]、CBEAM[17]、ICEPOLE[18]、Ketje[19]、Keyak[20]、NORX[21]、π-Cipher[22]、STRIBOB[23-24]等在内的方案都使用或借鉴了 Duplex 结构的设计.同时,Bertoni 等人[12]还提出了中间标签的概念,指出 SpongeWrap 可以通过在加密过程中插入中间标签,实现在解密过程中验证过中间标签后即释放标签以前的部分明文,而不用在最后验证成功后再释放整个明文.ELmD[25]、iFeed[26]等方案声称支持使用中间标签.Hoang 等人[5]在提出 OAE2 方案的概念时,指出利用中间标签可以使 SpongeWrap 满足 OAE2 方案的要求,但并未深入讨论.

双管道结构由 Lucks[27]于 2005 年提出,与 MD 结构(Merkle-Damgärd construction)、宽管道结构(wide-pipe construction)等同为杂凑函数的基础结构.Yasuda 利用双管道结构设计构造了一个超越生日界的 MAC 方案[28];经过重新审视 Lucks 提出的原始的双管道结构,Yasuda 将需求的密钥个数降低到一个,同时令新构造的 MAC 方案可以达到超越生日界的安全性[29].Lee 和 Steinberger[30]利用 Stam[31-32]设计的基于多项式的压缩函数,将 Lucks 提出的原始的双管道结构的速度提高了一倍,同时保持了同等的安全性.

3 预备知识

本节介绍文中使用到的符号定义以及基本概念.为统一在线加密以及在线认证加密的概念描述,我们参考 Hoang 等人[5]给出的"分块"的概念,对在线函数等进行定义和描述.

3.1 符号与定义

令 0^a 表示由 a 个 0 组成的串,$\{0,1\}^a$ 表示由所有长度为 a 的比特串组成的集合;$\{0,1\}^*$ 表示由所有比特串组成的集合.对于比特串 $A\in\{0,1\}^*$,$|A|$ 表示其比特长度.当 $|A|\geq a$ 时,$A|_a$ 表示截取 A 最左侧的 a 位比特,$A|^a$ 表示截取 A 的最右侧 a 位比特.对于比特串 $A,B\in\{0,1\}^*$,令 $A\|B$ 表示 A 和 B 的级联,$\overline{A\|B}$ 表示交换 A 和 B 的位置所得到的比特串 $B\|A$.对于 $X=A\|B$,在不引起歧义的情况下,令 $\overline{X}=B\|A$.假设 $\mathcal{A}$ 为一个集合,则 $A\leftarrow\mathcal{A}$ 表示从集合 $\mathcal{A}$ 中均匀随机地选取一个元素 A.对于正整数 i,令 $[i]_a$ 表示 i 的长度为 a 的二进制表示,其中低位在左.

假设比特串 $S\in\{0,1\}^*$,定义划分函数 $Partition(S,a)$ 为将 S 划分成 $S_1S_2\cdots S_s$,其中 $|S_i|=a$ 对 $i=1,2,\cdots,s-1$ 成立,且 $|S_s|\leq a$.在不引起歧义的情况下,简写 $Partition(S,a)$ 为 $Partition(S)$.定义两种不同的填充规则如下:

$$Pad_1(S)=(S_1\|[0]_b)\|(S_2\|[0]_b)\|\cdots\|(S_s\|10^{a-|S_s|-1}\|[1]_b),$$

$$Pad_2(S)=(S_1\|[1]_b)\|(S_2\|[1]_b)\|\cdots\|(S_s\|10^{a-|S_s|-1}\|[0]_b),$$

其中,$|S_i|=a$ 对于所有 $i<s$ 都成立,且 $0<|S_s|\leq a$.

令 $\{0,1\}^{**}=(\{0,1\}^*)^*$ 表示由分块串(segmented-strings)组成的集合.分块串 $\boldsymbol{S}\in\{0,1\}^{**}$ 是一个由比特串构成的向量,其中的每一个元素都是一个比特串,这里称其为一个分块(segment).对于 $\boldsymbol{S}=\boldsymbol{S}_1\|\cdots\|\boldsymbol{S}_s$,令 $\boldsymbol{S}_i$ 表示 $\boldsymbol{S}$ 的第 i 个分块;$\boldsymbol{S}_{i..j}$ 表示 $\boldsymbol{S}$ 的第 i 个到第 j 个分块,即 $\boldsymbol{S}_i\|\cdots\|\boldsymbol{S}_j$,其中 $1\leq i\leq j\leq s$.注意到,当每一个分块的比特长度都为 n 时,$\boldsymbol{S}$ 就是一个由 n-bit 的分组组成的串.在一般情况下,本文中不特别区分 $\boldsymbol{S}$ 与 S.

3.2 伪随机函数

令 $\mathrm{Func}(n,m)$ 为所有从 $\{0,1\}^n$ 到 $\{0,1\}^m$ 的函数组成的集合.如果 $f\leftarrow\mathrm{Func}(n,m)$,则称 f 是一个随机函数.对于一个从 $\{0,1\}^n$ 到 $\{0,1\}^m$ 的带密钥的函数族 F,其中密钥长度为 k,我们用下式定义的区分优势衡量其安全性:

$$\boldsymbol{Adv}_F^{\mathrm{prf}}=|\Pr[K\leftarrow\{0,1\}^k:\mathcal{A}^{F_K(\cdot)}=1]-\Pr[\mathcal{A}^{\$(\cdot)}=1]|,$$

其中第一个概率在 $K\leftarrow\{0,1\}^k$ 与随机选择的攻击者 $\mathcal{A}$ 上取值,而第二个概率在 $\$\leftarrow\mathrm{Func}(n,m)$ 与随

机选择的攻击者$\mathcal{A}$上取值.我们令$\boldsymbol{Adv}_F^{\mathrm{prf}}(t,q)$表示，在所有计算时间至多为$t$且询问次数至多为$q$的攻击者中，区分优势的最大值.

3.3　在线函数

对于一个从$\{0,1\}^{**}$到$\{0,1\}^{**}$的函数f，如果其输出的第i个分块完全由其输入的前i个分块决定，则称f是在线的.形式化地，对于一个函数族$f:\mathcal{K}\times\{0,1\}^{**}\to\{0,1\}^{**}$，如果存在函数$g^{(i)}:\mathcal{K}\times\{0,1\}^{**}\to\{0,1\}^{*}$，使得

$$(f_K(M))_i=g_K^{(i)}(M_1\|\cdots\|M_i),$$

对于任意的消息$M=M_1\|\cdots\|M_m\in\{0,1\}^{**}$以及所有的$i\in\{1,\cdots,m\}$，$K\in\mathcal{K}$都成立，则称函数族$f$是在线的.令$\mathrm{OFunc}(a,b)$表示所有从$(\{0,1\}^a)^*$到$(\{0,1\}^b)^*$的在线函数组成的集合.特别地，当$a=b$时，$\mathrm{OFunc}(a,b)$是所有$(\{0,1\}^a)^*$上的在线置换组成的集合，记为$\mathrm{OPerm}(a)$.

对于一个加密方案，如果其加密函数是在线的，则称该方案是在线加密的.

3.4　认证加密方案

一个认证加密方案(Authenticated Encryption scheme，简称AE方案)可以形式地描述为一个三元组$\Pi=(\mathcal{K},\mathcal{E},\mathcal{D})$，与之相关的有比特串集合$N\in\{0,1\}^*$和$M\in\{0,1\}^*$.其中，$\mathcal{K}$是密钥空间，$\mathcal{E}$和$\mathcal{D}$分别是加密算法与解密算法.加密算法$\mathcal{E}$以$K\in\mathcal{K}$，$N\in\mathcal{N}$和$M\in\mathcal{M}$为输入，输出一个比特串$C=E_K(N,M)$；解密算法$\mathcal{D}$以$K\in\mathcal{K}$，$N\in\mathcal{N}$和$C\in\{0,1\}^*$为输入，输出$D_K(N,C)$，其中$D_K(N,C)$可能是属于$\mathcal{M}$的比特串或符号$\perp$.要求对于任意的$K\in\mathcal{K}$、$N\in\mathcal{N}$和$M\in\mathcal{M}$，都有$D_K(N,(E_K(N,M))=M$，存在某线性时间的可计算的长度函数$l$，使得$|\mathcal{E}_K(N,M)|=l(|M|)$.

OAE1是指在在线加密的末尾添加认证操作，使得认证加密方案同时具有在线加密的性质.认证成功时，输出与密文相对应的明文；认证失败时，则仅输出符号$\perp$.OAE2方案则是基于分块认证加密方案定义的在加密和解密方向同时具有在线性的一类方案.

分块认证加密方案是在认证加密方案的基础上添加一个状态空间$\mathcal{S}$，并将加密和解密扩展为由三个确定性算法组成的三元组：

$$\mathcal{E}=(\mathcal{E}.\mathrm{init},\mathcal{E}.\mathrm{next},\mathcal{E}.\mathrm{last}),$$

$$\mathcal{D}=(\mathcal{D}.\mathrm{init},\mathcal{D}.\mathrm{next},\mathcal{D}.\mathrm{last}).$$

其中，$\mathcal{M}=\{0,1\}^*$和$\mathcal{C}=\{0,1\}^*$分别为消息空间和密文空间.$\mathcal{E}$和$\mathcal{D}$中元素的表述如下：

$\mathcal{E}.\mathrm{init}:\mathcal{K}\times\mathcal{N}\to\mathcal{S}$；

$\mathcal{E}.\mathrm{next}:\mathcal{S}\times\mathcal{M}\to\mathcal{C}\times\mathcal{S}$；

$\mathcal{E}.\mathrm{last}:\mathcal{S}\times\mathcal{M}\to\mathcal{C}$；

$\mathcal{D}.\mathrm{init}:\mathcal{K}\times\mathcal{N}\to\mathcal{S}$；

$\mathcal{D}.\mathrm{next}:\mathcal{S}\times\mathcal{C}\to(\mathcal{M}\times\mathcal{S})\cup\{\perp\}$；

$\mathcal{D}.\mathrm{last}:\mathcal{S}\times\mathcal{C}\to\mathcal{M}\cup\{\perp\}$.

对于一个分块认证加密方案$\Pi=(\mathcal{K},\mathcal{E},\mathcal{D})$，如果$\tau$为常数，且$|C_i|=|M_i|+\tau$对所有的$i$都成立，则称其带有常数的分块扩展，并称$\tau$为$\Pi$的分块扩展.如果$\Pi$的状态空间是有限的，且存在一个常数$\omega$，使得$\mathcal{E}.\mathrm{next}$($\mathcal{D}.\mathrm{next}$)和$\mathcal{E}.\mathrm{last}$($\mathcal{D}.\mathrm{last}$)使用至多$\omega$个比特的工作存储，则称$\Pi$具有在线加密(在线解密)的性质.如果$\Pi$同时具有在线加密与在线解密的性质，则称$\Pi$是在线的.

4　DPE方案与DPAE方案

本节给出DPE方案与DPAE方案的描述.DPE方案是一个在线加密方案，每处理一个分组消息需要调用两个底层压缩函数，在选择明文攻击下可达到安全.DPAE方案是一个在线认证加密方案，相比于DPE增加了标签的认证操作，利用中间标签的性质可以分别满足OAE1方案和OAE2方案的要求，提供机密性和完整性的保护.

4.1　DPE方案

令$F_1:\mathcal{K}\times\{0,1\}^{a+b}\to\{0,1\}^a$，$F_2:\mathcal{K}\times\{0,1\}^{a+b}\to\{0,1\}^b$为两个相互独立的压缩函数族.令$f_1(\cdot)\triangleq F_1(K_1,\cdot)$，$f_2(\cdot)\triangleq F_2(K_2,\cdot)$，其中$K_1,K_2\in\mathcal{K}$.

一个DPE方案以一个唯一值N、一个明文M以及一对密钥(K_1,K_2)为输入，输出一个与明文M具有相同长度的密文C.其中，N和M的总长度至多为$2^{a/2}$比特.具体的加密与解密算法描述如下.

算法1.　$\mathrm{DPE.Enc}_K$.

输入：(N,M)

输出：C

$N_1\|\cdots\|N_n\leftarrow Partition(Pad_1(N))$

$M_1\|\cdots\|M_m\leftarrow Partition(Pad_2(M))$

$A\leftarrow 0^a$；$B\leftarrow 1^b$

$X\leftarrow A\|B$

$A\leftarrow f_1(X)$；$B\leftarrow f_2(\overline{X})$

FOR $i\leftarrow 1$ TO n DO

　$X\leftarrow(A\|B)\oplus N_i$

　$A\leftarrow f_1(X)$；$B\leftarrow f_2(\overline{X})$

FOR $i\leftarrow 1$ TO $m-1$ DO

　$X\leftarrow(A\|B)\oplus M_i$

$C_i \leftarrow X|_b$
$A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
$X \leftarrow (A \| B) \oplus M_m$
$C_m \leftarrow X|_{|M_m|}$
$C \leftarrow C_1 \| \cdots \| C_m$
RETURN C

算法 2. $\mathrm{DPE.Dec}_K$.

输入：(N, C)
输出：M
$N_1 \| \cdots \| N_n \leftarrow Partition(Pad_1(N))$
$C_1 \| \cdots \| C_c \leftarrow Partition(Pad_2(C))$
$A \leftarrow 0^a; B \leftarrow 1^b$
$X \leftarrow A \| B$
$A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
FOR $i \leftarrow 1$ TO n DO
  $X \leftarrow (A \| B) \oplus N_i$
  $A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
FOR $i \leftarrow 1$ TO $c-1$ DO
  $M_i \leftarrow A \oplus C_i|_b$
  $X \leftarrow C_i|_b \| (B \oplus C_i|^a)$
  $A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
$M_c \leftarrow (A \oplus C_c|_b)|_{|C_c|}$
$X \leftarrow A \| (B \oplus C_c|^a)$
$M \leftarrow M_1 \| \cdots \| M_c$
RETURN M

算法 1 和算法 2 分别描述了 DPE 方案的加密与解密的具体操作. 其中，两个压缩函数 (f_1, f_2) 的输出组成状态链值 $(A \| B)$. 操作流程可参见图 1.

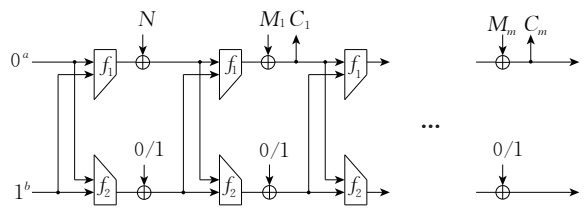

图 1 DPE 方案图示

4.2 DPAE 方案

DPAE 方案在 DPE 方案的基础上添加了标签的生成和认证，在加密完成后继续调用底层压缩函数更新状态链值，并输出外部状态作为标签. 具体的算法描述如下. 其中，算法 1 和算法 2 分别描述了 DPAE 方案的加密与解密的具体操作.

算法 3. $\mathrm{DPAE.Enc}_K$.

输入：(N, M)
输出：(C, T)
$N_1 \| \cdots \| N_n \leftarrow Partition(Pad_1(N))$
$M_1 \| \cdots \| M_m \leftarrow Partition(Pad_2(M))$
$A \leftarrow 0^a; B \leftarrow 1^b$
$X \leftarrow A \| B$
$A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
FOR $i \leftarrow 1$ TO n DO
  $X \leftarrow (A \| B) \oplus N_i$
  $A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
FOR $i \leftarrow 1$ TO $m-1$ DO
  $X \leftarrow (A \| B) \oplus M_i$
  $C_i \leftarrow X|_b$
  $A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
$X \leftarrow (A \| B) \oplus M_m$
$C_m \leftarrow X|_{|M_m|}$
$A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
$C \leftarrow C_1 \| \cdots \| C_m$
$T \leftarrow A$
RETURN (C, T)

算法 4. $\mathrm{DPAE.Dec}_K$.

输入：(N, C, T)
输出：$M/\perp$
$N_1 \| \cdots \| N_n \leftarrow Partition(Pad_1(N))$
$C_1 \| \cdots \| C_c \leftarrow Partition(Pad_2(C))$
$A \leftarrow 0^a; B \leftarrow 1^b$
$X \leftarrow A \| B$
$A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
FOR $i \leftarrow 1$ TO n DO
  $X \leftarrow (A \| B) \oplus N_i$
  $A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
FOR $i \leftarrow 1$ TO $c-1$ DO
  $M_i \leftarrow A \oplus C_i|_b$
  $X \leftarrow C_i|_b \| (B \oplus C_i|^a)$
  $A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
$M_c \leftarrow (A \oplus C_c|_b)|_{|C_c|}$
$M \leftarrow M_1 \| \cdots \| M_c$
$X \leftarrow A \| (B \oplus C_c|^a)$
$A \leftarrow f_1(X); B \leftarrow f_2(\overline{X})$
$T' \leftarrow A$
IF $T = T'$ THEN RETURN M
  ELSE RETURN $\perp$

算法 3 和算法 4 分别描述了 DPAE 方案的加密与解密的具体操作. 操作流程可参见图 2.

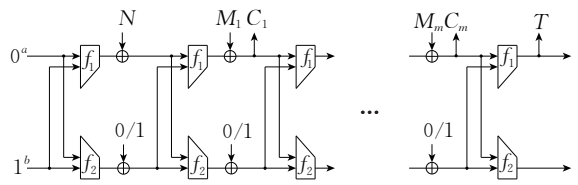

图 2 DPAE 方案图示

需要说明的是，在上述算法描述中，标签 T 的长度与外部状态 A 的长度相同. 当需要较高的完整

性保护时，可以通过重复调用底层压缩函数对状态链值进行更新，并输出相应的外部状态获得长标签. 例如，当标签长度大于 a 时，可以将下列语句插入到算法中 $T\leftarrow A$ 之后.

WHILE $|T|<\tau$ DO

$X\leftarrow A\|B$

$A\leftarrow f_1(X)$；$B\leftarrow f_2(\overline{X})$

$T\leftarrow T\|A$

END WHILE

$T\leftarrow T|_\tau$

与 DPE 方案类似，对于加密算法，N 和 M 的总长度至多为 $2^{a/2}$ 比特；对于解密算法，N 和 C 的总长度至多为 $2^{a/2}$ 比特.

4.3　DPAE-I 方案

为将 DPAE 从OAE1方案转换为 OAE2 方案，我们通过以下方法分别对加密和解密算法构造初始化函数、迭代函数、末尾函数. 首先，我们将由初始向量 $\mathbf{0}^a\mathbf{1}^b$ 经底层压缩函数作用得到状态 $S(=(f_1(\mathbf{0}^a\mathbf{1}^b),f_2(\mathbf{1}^b\mathbf{0}^a)))$ 的过程记为 $\mathcal{E}.\mathrm{init}(K)$. 其次，将状态链值 S 视为变量，并在加密算法 $\mathrm{DPAE.Enc}_K(N,M)$ 生成标签 T 之后添加一次状态更新操作，即“$A\leftarrow f_K(X)$；$B\leftarrow f_K(\overline{X})$”，将得到的新算法记为 $\mathcal{E}.\mathrm{next}(S,N,M)$. 此时算法 $\mathcal{E}.\mathrm{next}(S,N,M)$ 的输出为三元组 (C,T,S'). 其中，S' 留作下一次加密的初始状态保留，不输出给询问者. 再次，我们修改 $\mathcal{E}.\mathrm{next}(S,N,M)$，增加一步对内部状态 B 异或进 $0^{b-2}10$ 的操作，使得构造所得的 $\mathcal{E}.\mathrm{last}(S,N,M)$ 与 $\mathcal{E}.\mathrm{next}(S,N,M)$ 有所区别. 由于 $\mathcal{E}.\mathrm{last}(S,N,M)$ 输出的状态链值 S 将不再进行更新使用，因此可以将 $\mathcal{E}.\mathrm{last}(S,N,M)$ 的输出省略为二元组 (C,T). 最后，我们为加密算法的三个组成函数定义相应的解密函数：$\mathcal{D}.\mathrm{init}(K)$，$\mathcal{D}.\mathrm{next}(S,N,C,T)$ 以及 $\mathcal{D}.\mathrm{last}(S,N,C,T)$.

我们将得到的新方案称为 DPAE-I.

此时，保持密钥空间 $\mathcal{K}$、明文空间 $\mathcal{M}$、密文空间 $\mathcal{C}$ 以及状态空间 $\mathcal{S}$ 定义如前，可以将 DPAE-I 方案的加密和解密分别形式化描述为三个阶段.

$\mathcal{E}.\mathrm{init}$：$\mathcal{K}\rightarrow\mathcal{S}$；

$\mathcal{E}.\mathrm{next}$：$\mathcal{S}\times\mathcal{N}\times\mathcal{M}\rightarrow\mathcal{C}\times\mathcal{T}\times\mathcal{S}$；

$\mathcal{E}.\mathrm{last}$：$\mathcal{S}\times\mathcal{N}\times\mathcal{M}\rightarrow\mathcal{C}\times\mathcal{T}$；

$\mathcal{D}.\mathrm{init}$：$\mathcal{K}\rightarrow\mathcal{S}$；

$\mathcal{D}.\mathrm{next}$：$\mathcal{S}\times\mathcal{N}\times\mathcal{C}\times\mathcal{T}\rightarrow(\mathcal{M}\times\mathcal{S})\cup\{\perp\}$；

$\mathcal{D}.\mathrm{last}$：$\mathcal{S}\times\mathcal{N}\times\mathcal{C}\times\mathcal{T}\rightarrow\mathcal{M}\cup\{\perp\}$.

在 DPAE-I 方案中，加密时，输入的消息 (N,M) 首先被切分成同样数量的分块，得到 $(N^{(1)},M^{(1)},N^{(2)},M^{(2)},\cdots,N^{(\alpha)},M^{(\alpha)})$. 其中，每个分块的长度可以根据用户需求取不同的数值，但要求交互的双方提前约定.

首先，调用 $\mathcal{E}.\mathrm{init}(K)$ 生成初始状态 $S^{(0)}$. 其次，调用 $\mathcal{E}.\mathrm{next}$ 作用于 $(S^{(0)},N^{(1)},M^{(1)})$，生成 $(C^{(1)},T^{(1)},S^{(1)})$. 再次，调用 $\mathcal{E}.\mathrm{next}$ 作用于 $(S^{(1)},N^{(2)},M^{(2)})$，生成 $(C^{(2)},T^{(2)},S^{(2)})$，以此类推. 最后调用 $\mathcal{E}.\mathrm{last}$ 作用于 $(S^{(\alpha-1)},N^{(\alpha)},M^{(\alpha)})$，生成 $(C^{(\alpha)},T^{(\alpha)})$.

相应地，在执行解密算法时，输入的密文 (N,C,T) 被切分成具有同样数量的分块，可以得到 $(N^{(1)},C^{(1)},T^{(1)},N^{(2)},C^{(2)},T^{(2)},\cdots,N^{(\alpha)},C^{(\alpha)},T^{(\alpha)})$. 其中，$N^{(i)},C^{(i)},T^{(i)}(i=1,\cdots,\alpha)$ 的长度与加密中的规定相一致.

首先，调用 $\mathcal{D}.\mathrm{init}(K)$ 生成初始状态 $S^{(0)}$. 其次，调用 $\mathcal{D}.\mathrm{next}$ 作用于 $(S^{(0)},N^{(1)},C^{(1)},T^{(1)})$，若验证成功，则输出 $M^{(1)}$；若验证失败，则输出 $\perp$，并终止操作. 再次，调用 $\mathcal{D}.\mathrm{next}$ 作用于 $(S^{(1)},N^{(2)},C^{(2)},T^{(2)})$，若验证成功，则输出 $M^{(2)}$；若验证失败，则输出 $\perp$，以此类推. 最后调用 $\mathcal{D}.\mathrm{last}$ 作用于 $(S^{(\alpha-1)},N^{(\alpha)},C^{(\alpha)},T^{(\alpha)})$，若验证成功，则输出 $M^{(\alpha)}$；若验证失败，则输出 $\perp$.

通过这种方式，DPAE-I 方案作为分块认证加密方案，可以在加密和解密方向上都满足在线性的需求.

5　安全性分析

本节分别给出 DPE 方案和 DPAE 方案的安全性证明.

在衡量安全性时，我们假设攻击者是具有访问预言机能力的一个程序. 如果攻击者不会向预言机重复询问中的第一个元素，即唯一值 N，则称该攻击者是遵循唯一值的(nonce-respecting). 在本文中，我们始终假设攻击者是遵循唯一值的. 为使证明较为简洁，我们假设攻击者 $\mathcal{A}$ 向加密预言机 $\mathcal{O}$ 询问的消息 (N,M) 满足填充规则(即是填充后的消息)；对于认证加密方案，$\mathcal{A}$ 向解密预言机 $\mathcal{O}$ 询问的消息 (C,T) 也满足填充规则，并且，此前并未做过答复为 (C,T) 的询问 (N,M). 此外，不失一般性，我们假设明文的比特长度恰是 a 的整数倍，标签长度为 a.

5.1　DPE 方案的安全性

我们首先给出在线加密的安全性定义，进而证明 DPE 方案的安全性. 该定义参考了 Bellare 等人最早提出的在线密码的安全性定义[1] 以及 Rogoway 和

Zhang[33]的描述方式.

令 $\Pi=(\mathcal{K},\mathcal{E},\mathcal{D})$为一个在线密码.假设攻击者 $\mathcal{A}$可以访问两种预言机之一:"真实"的加密预言机或"虚伪"的加密预言机.一个真实的加密预言机 $\mathcal{E}_K(\cdot,\cdot)$,以$(N,M)$为输入,以 $C\leftarrow\mathcal{E}_K(N,M)$为输出.一个虚伪的加密预言机 $\pi\leftarrow\mathrm{OPerm}(a)$,以$(N,M)$为输入,以 $C\leftarrow\pi(N,M)$为输出.给定攻击者 $\mathcal{A}$以及加密方案 Π,定义

$$\boldsymbol{Adv}_{\Pi}^{\mathrm{cpa}}(\mathcal{A})=|\Pr[K\leftarrow\mathcal{K}:\mathcal{A}^{\mathcal{E}_K(\cdot,\cdot)}\Rightarrow 1]-\Pr[\pi(\cdot,\cdot)\leftarrow\mathrm{OPerm}(a):\mathcal{A}^{\pi(\cdot,\cdot)}\Rightarrow 1]|.$$

令 $\boldsymbol{Adv}_{\Pi}^{\mathrm{cpa}}(t,q,\sigma)$表示所有运行时间至多为 t、询问次数至多为 q 且总询问长度至多为 σ 个分块的攻击者中攻击优势的最大值.当 $\boldsymbol{Adv}_{\Pi}^{\mathrm{cpa}}(t,q,\sigma)$取值可忽略时,我们称在线加密方案 Π 是安全的.

假设一个 DPE 方案的底层压缩函数 f_1和 f_2相互独立,其输入均为$(a+b)$位的比特串,输出长度分别为 a 位和 b 位的比特串.假设攻击者 $\mathcal{A}$区分 f_1(或 f_2)与一个伪随机函数的区分优势上界为 $\boldsymbol{Adv}_{f_1}^{\mathrm{prf}}$(或 $\boldsymbol{Adv}_{f_2}^{\mathrm{prf}}$).如果 $\boldsymbol{Adv}_{f_1}^{\mathrm{prf}}$与 $\boldsymbol{Adv}_{f_2}^{\mathrm{prf}}$都是可忽略的,我们可以证明以 f_1,f_2为底层压缩函数的 DPE 方案 DPE_{f_1,f_2}是安全的.

定理 1. 假设压缩函数 f_1和 f_2不同且相互独立,并满足 DPE 方案底层模块的要求.对于任意运行时间至多为 t、询问次数至多为 q 且总询问长度(包含唯一值与消息)至多为 σ 个分块的攻击者 $\mathcal{A}$,有以下结果成立:

$$\boldsymbol{Adv}_{DPE_{f_1,f_2}}^{\mathrm{cpa}}(t,q,\sigma)\leq \boldsymbol{Adv}_{f_1}^{\mathrm{prf}}(t,\sigma+1)+\boldsymbol{Adv}_{f_2}^{\mathrm{prf}}(t,\sigma+1)+\frac{\sigma^2}{2^{a+b-1}}.$$

当函数 $f_1=f_2$且 $a=b$ 时,DPE 方案 DPE_{f_1,f_2}(简记为 DPE_f)的安全性分析相对于 f_1,f_2不同且相互独立的情况要复杂.首先,当询问次数为 q,且总询问长度至多为 σ 个分块时,DPE_{f_1,f_2}中 f_1和 f_2分别被调用了 $\sigma+1$ 次;而 DPE_f中 f 被调用了 $2\sigma+2$ 次.假设 f,f_1,f_2具有相同的安全性,则显然攻击者在询问 DPE_f时具有更强的区分优势.其次,假设 A,B 定义如算法描述,考虑 $A\|B=B\|A$ 的情况,其中$|A|=|B|$.在 DPE_f中,根据 $A'\leftarrow f(A\|B)$和 $B'\leftarrow f(B\|A)$,可以得到 $A'=B'$,即攻击者可以通过计算 A'的取值获得内部状态 B'的值,进而攻击该方案.在 DPE_{f_1,f_2}中,$A\|B$ 与 $B\|A$ 分别作为 f_1和 f_2的输入,并不会导致这样的攻击.因此我们特别给出这一特殊情况下的安全性证明.

定理 2. 假设压缩函数 f 输入长度为 $2b$ 比特,输出长度为 b 比特.对于任意运行时间至多为 t、询问次数至多为 q 且总询问长度(包含唯一值与消息)至多为 σ 个分块的攻击者 $\mathcal{A}$,有以下结果成立:

$$\boldsymbol{Adv}_{DPE_f}^{\mathrm{cpa}}(t,q,\sigma)\leq \boldsymbol{Adv}_{f}^{\mathrm{prf}}(t,2\sigma+2)+\frac{\sigma^2}{2^{2b-1}}+\frac{\sigma}{2^b}.$$

证明. 考虑如算法 5 所示的游戏 G_1,G_2,G_3:G_3包含方框中的代码,而 G_1和 G_2则不包含.G_1与 G_2基本相同,差别仅在于 G_1中的 f 是压缩函数,而 G_2中的 f 是随机选择的函数.G_3中的 f 也是随机选择的函数.攻击者 $\mathcal{A}$至多进行 q 次询问,并且询问的总长度不超过 σ 个分块,这里分块长度固定为 b 个比特.

定义两个集合 $\overline{Dom}=\{\overline{X}\mid X\in Dom\}$ 以及 $Twofold=\{A\|A\mid A\in\{0,1\}^b\}$.

算法 5. Game G_1,G_2,Game G_3.

输入:(N,M)

输出:C

Initialization

1. $bad\leftarrow$false
2. $K\leftarrow\mathcal{K}$
3. $Dom\leftarrow\{0^b\|1^b\}$

When $\mathcal{A}$ asks query (N,M) //q such queries will be asked

10. $N_1\|\cdots\|N_n\leftarrow Partition(Pad_1(N))$
11. $M_1\|\cdots\|M_m\leftarrow Partition(Pad_2(M))$
12. $A\leftarrow 0^b$;$B\leftarrow 1^b$
13. $X\leftarrow A\|B$
14. $A\leftarrow f(X)$;$B\leftarrow f(\overline{X})$
15. FOR $i\leftarrow 1$ TO n DO
16. $X\leftarrow(A\|B)\oplus N_i$
17. IF $(X\in Dom)\cup(\overline{X}\in Dom)\cup(X|^b=X|_b)$
18. THEN $bad\leftarrow$true

    $X\leftarrow\{0,1\}^{2b}/(Dom\cup\overline{Dom}\cup Twofold)$
19. $Dom\leftarrow Dom\cup\{X,\overline{X}\}$
20. $A\leftarrow f(X)$;$B\leftarrow f(\overline{X})$
21. FOR $i\leftarrow 1$ TO $m-1$ DO
22. $X\leftarrow(A\|B)\oplus M_i$
23. IF $(X\in Dom)\cup(\overline{X}\in Dom)\cup(X|^b=X|_b)$
24. THEN $bad\leftarrow$true

    $X\leftarrow\{0,1\}^{2b}/(Dom\cup\overline{Dom}\cup Twofold)$
25. $Dom\leftarrow Dom\cup\{X,\overline{X}\}$
26. $C_i\leftarrow X|_b$
27. $A\leftarrow f(X)$;$B\leftarrow f(\overline{X})$
28. $X\leftarrow(A\|B)\oplus M_m$
29. IF $(X\in Dom)\cup(\overline{X}\in Dom)\cup(X|^b=X|_b)$

30. THEN $bad \leftarrow$ true

$\boxed{X \xleftarrow{} \{0,1\}^{2b} / (Dom \cup \overline{Dom} \cup Twofold)}$

31. $Dom \leftarrow Dom \cup \{X, \overline{X}\}$

32. $C_m \leftarrow X|_{|M_m|}$

33. $C \leftarrow C_1 \| \cdots \| C_m$

34. RETURN C

观察 G_1 可以看到，G_1 为 $\mathcal{A}$ 完美地模拟了 DPE_f，其中 f 是选定的压缩函数. 如果我们将压缩函数 f 替换为一个随机函数 $f \in \mathrm{Func}(2b,b)$，则可以得到 G_2. 替换函数 f 导致的差异可以由 f 的安全性描述，即攻击优势的变化受 $\boldsymbol{Adv}_f^{\mathrm{prf}}$ 绑定. 注意到，在 q 次询问中，f 一共需要被调用 $2\sigma+2$ 次，因此有

$$|\Pr[\mathcal{A}^{G_1} \Rightarrow 1] - \Pr[\mathcal{A}^{G_2} \Rightarrow 1]| \leq \boldsymbol{Adv}_f^{\mathrm{prf}}(t, 2\sigma+2).$$

注意到，G_3 中的输出始终是随机比特串，也就是 G_3 为攻击者 $\mathcal{A}$ 完美地模拟了 π. 注意到 G_3 与 G_2 仅在 $(X \in Dom) \cup (\overline{X} \in Dom) \cup (X|^b = X|_b)$ 为真时有所不同，此时 G_3 中的 X 是随机选自 $\{0,1\}^{2b}/(Dom \cup \overline{Dom} \cup Twofold)$ 的比特串. 从而，G_2 与 G_3 是“直到 bad 发生前相同”(identical-until-bad)，即

$$|\Pr[\mathcal{A}^{G_2} \Rightarrow 1] - \Pr[\mathcal{A}^{G_3} \Rightarrow 1]| \leq \Pr[\mathcal{A}^{G_3} \text{将 } bad \text{ 设为真}].$$

在 G_3 中，当且仅当对 $\mathcal{O}$ 的询问中有以下三种情况之一出现，bad 才会被设为真：X 在 Dom 中存在；$\overline{X}$ 在 Dom 中存在；或者，$X|^b = X|_b$. 分别定义这三种情况为 coll，bcoll 和 twofold.

注意到，在向 $\mathcal{O}$ 进行询问期间，函数 f 的调用次数为 $2\sigma+2$. 每次状态链值 X 更新至多向集合 Dom 添加 2 个元素. 由于 f 是一个随机函数，可以证明

$$\Pr[\mathrm{coll}] \leq \sum_{i=1}^{\sigma} \frac{2(i-1)+1}{2^{2b}} \leq \frac{\sigma^2}{2^{2b}}.$$

类似地，我们可以计算出 bcoll 被设为真的概率上界.

$$\Pr[\mathrm{bcoll}] \leq \frac{\sigma^2}{2^{2b}}.$$

接下来计算，在向 $\mathcal{O}$ 进行询问期间，twofold 被设为真的概率上界. 由于 f 是一个随机函数，容易得到

$$\Pr[\mathrm{twofold}] \leq \frac{\sigma}{2^b}.$$

将上述结果进行加和，可以得到

$$\Pr[\mathcal{A}^{G_3} \text{将 } bad \text{ 设为真}] \leq \frac{\sigma^2}{2^{2b-1}} + \frac{\sigma}{2^b}.$$

通过将以上相互独立的界相加，即得到

$$\Pr[\mathcal{A}^{G_1} \Rightarrow 1] \leq \boldsymbol{Adv}_f^{\mathrm{prf}}(t, 2\sigma+2) + \frac{\sigma^2}{2^{2b-1}} + \frac{\sigma}{2^b}.$$

证毕.

5.2 DPAE 方案的安全性

我们沿用 Rogaway 和 Shrimpton[34] 提出的 CCA3 定义，以衡量 OAE1 方案的安全性. Fleischemann 等人[2] 证明了 CCA3 可以由 CPA 与 INT-CTXT 组合得到. 即对于认证加密方案 $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$，假设 $\mathcal{A}$ 是一个运行时间为 t、询问次数为 q 且总询问分块数至多为 σ 的攻击者. 则存在一个 CPA-攻击者 $\mathcal{A}_1$ 和一个 INT-CTXT-攻击者 $\mathcal{A}_2$ 使得

$$\boldsymbol{Adv}_{\Pi}^{\mathrm{cca3}}(\mathcal{A}) \leq \boldsymbol{Adv}_{\Pi}^{\mathrm{cpa}}(\mathcal{A}_1) + \boldsymbol{Adv}_{\Pi}^{\mathrm{int\text{-}ctxt}}(\mathcal{A}_2),$$

其中，$\mathcal{A}_1$ 和 $\mathcal{A}_2$ 的运行时间为 $O(t)$，且询问次数至多为 q. INT-CTXT 的定义是，如果攻击者 $\mathcal{A}$ 输出一组 (N,C,T)，使得 $\mathcal{D}_K(N,C,T) \neq \perp$，并且 $\mathcal{A}$ 此前并未做过答复为 (C,T) 的询问 (N,M)，则称 $\mathcal{A}$ 伪造(forge)成功. 定义

$$\boldsymbol{Adv}_{\Pi}^{\mathrm{int\text{-}ctxt}} = \Pr[K \xleftarrow{} \mathcal{K} : \mathcal{A}^{\mathcal{E}_K(\cdot,\cdot)} \text{伪造成功}].$$

根据这一结论，我们可以分别衡量 DPAE 的机密性与完整性. 注意到，DPAE 方案是在 DPE 方案的基础上添加了标签生成阶段构成的. 也就是说，当攻击者向 DPAE 方案下的正向(加密)预言机进行询问时，获得的密文等价于向 DPE 方案下的正向预言机进行询问所获得的密文. 利用这一性质，我们将证明 DPE 方案的安全性时所用的游戏进行扩展，通过补充增加末尾认证操作后的影响，我们可以容易地将 DPE 方案的机密性结果扩展到 DPAE 方案中.

定理 3.　假设压缩函数 f_1 和 f_2 不同且相互独立，并满足 DPAE 方案底层模块的要求. 对于任意运行时间至多为 t、询问次数至多为 q 且总询问长度(包含唯一值与消息)至多为 σ 个分块的攻击者 $\mathcal{A}$，有以下结果成立：

$$\boldsymbol{Adv}_{DPAE_{f_1,f_2}}^{\mathrm{cpa}}(t,q,\sigma) \leq \boldsymbol{Adv}_{f_1}^{\mathrm{prf}}(t,\sigma+q+1) + \boldsymbol{Adv}_{f_2}^{\mathrm{prf}}(t,\sigma+q+1) + \frac{(\sigma+q)^2}{2^{a+b-1}}.$$

当函数 $f_1 = f_2$ 且 $a = b$ 时，结论如下.

定理 4.　假设压缩函数 f 输入长度为 $2b$ 比特，输出长度为 b 比特. 对于任意运行时间至多为 t、询问次数至多为 q 且总询问长度(包含唯一值与消息)至多为 σ 个分块的攻击者 $\mathcal{A}$，有以下结果成立：

$$\boldsymbol{Adv}_{DPAE_f}^{\mathrm{cpa}}(t,q,\sigma) \leq \boldsymbol{Adv}_f^{\mathrm{prf}}(t,2\sigma+2q+2) + \frac{(\sigma+q)^2}{2^{2b-1}} + \frac{\sigma+q}{2^b}.$$

证明. 令 G_1, G_2, G_3 定义如前，并用下列算法代替第 34 行以及其后的算法内容.

34. $A \leftarrow f(X); B \leftarrow f(\overline{X})$
35. $X \leftarrow A \| B$
36. IF $(X \in Dom) \cup (\overline{X} \in Dom) \cup (X|^b = X|_b)$
37. THEN $bad \leftarrow$ false

$$\boxed{X \twoheadleftarrow \{0,1\}^{2b} / (Dom \cup \overline{Dom} \cup Twofold)}$$

38. $Dom \leftarrow Dom \cup \{X, \overline{X}\}$
39. $T \leftarrow A$
40. RETURN (C, T)

注意到，G_1 为 $\mathcal{A}$ 完美地模拟了 $DPAE_f$；而 G_3 为攻击者 $\mathcal{A}$ 完美地模拟了 π. 在 q 次询问中，f 一共需要被调用 $2\sigma+2q+2$ 次，因此有

$$\Pr[\mathcal{A}^{G_1} \Rightarrow 1] \leq \boldsymbol{Adv}_f^{\mathrm{prf}}(t, 2\sigma+2q+2) + \Pr[\mathcal{A}^{G_3} \text{将 } bad \text{ 设为真}].$$

在 G_3 中，bad 被设为真仍可分为 coll，bcoll 和 twofold 三种情况.

$$\Pr[\mathrm{coll}] \leq \sum_{i=1}^{\sigma+q} \frac{2(i-1)+1}{2^{2b}} \leq \frac{(\sigma+q)^2}{2^{2b}},$$

$$\Pr[\mathrm{bcoll}] \leq \frac{(\sigma+q)^2}{2^{2b}},$$

$$\Pr[\mathrm{twofold}] \leq \frac{\sigma+q}{2^b}.$$

将上述结果进行加和，可以得到

$$\Pr[\mathcal{A}^{G_3} \text{将 } bad \text{ 设为真}] \leq \frac{(\sigma+q)^2}{2^{2b-1}} + \frac{\sigma+q}{2^b}.$$

通过将以上相互独立的界相加，即得到

$$Pr[\mathcal{A}^{G_1} \Rightarrow 1] \leq \boldsymbol{Adv}_f^{\mathrm{prf}}(t, 2\sigma+2q+2) + \frac{(\sigma+q)^2}{2^{2b-1}} + \frac{\sigma+q}{2^b}.$$

证毕.

完整性主要受标签的验证方式与标签长度影响. 我们建议使用与明文块相同的标签长度，即取状态链值中外部状态的 a 位比特串作为标签. 需要说明的是，选用长标签可以适当地增加方案对消息的完整性保护.

定理 5. 假设压缩函数 f_1 和 f_2 不同且相互独立，并满足 DPAE 方案底层模块的要求. 对于任意正向询问运行时间至多为 t、次数至多为 q 且总询问长度（包含唯一值与明文）至多为 σ 个分块，而逆向询问运行时间至多为 t_v、次数至多为 q_v 且总询问长度（包含唯一值与密文）至多为 σ_v 个分块的攻击者 $\mathcal{A}$，有以下结果成立：

$$\boldsymbol{Adv}^{\text{int-ctxt}}_{DPAE_{f_1,f_2}}(t, t_v, q, \sigma, q_v, \sigma_v) \leq \boldsymbol{Adv}^{\mathrm{prf}}_{f_1}(t+t_v, \sigma+\sigma_v+2q+2q_v+1) + \boldsymbol{Adv}^{\mathrm{prf}}_{f_2}(t+t_v, \sigma+\sigma_v+2q+2q_v+1) + \frac{(\sigma+\sigma_v+q+q_v)^2}{2^{a+b-1}} + \frac{q_v}{2^a}.$$

当函数 $f_1 = f_2$ 且 $a = b$ 时，结论如下.

定理 6. 假设压缩函数 f 输入长度为 $2b$ 比特，输出长度为 b 比特. 对于任意正向询问运行时间至多为 t、次数至多为 q 且总询问长度（包含唯一值与明文）至多为 σ 个分块，而逆向询问运行时间至多为 t_v、次数至多为 q_v 且总询问长度（包含唯一值与密文）至多为 σ_v 个分块的攻击者 $\mathcal{A}$，有以下结果成立：

$$\boldsymbol{Adv}^{\text{int-ctxt}}_{DPAE_f}(t, q, \sigma) \leq \boldsymbol{Adv}^{\mathrm{prf}}_f(t+t_v, 2\sigma+2\sigma_v+4q+4q_v+1) + \frac{(\sigma+\sigma_v+q+q_v)^2}{2^{2b-1}} + \frac{\sigma+\sigma_v+q+2q_v}{2^b}.$$

证明. 令 G_1, G_2, G_3 的加密部分定义如前，添加解密部分定义如下. 在 G_1 中，f 是压缩函数，在 G_2 和 G_3 中，f 是一个随机函数.

算法 6. Game G_1，G_2，$\boxed{\text{Game } G_3}$ 的解密.

输入：(N, M)
输出：C

When $\mathcal{A}$ asks query (N, C, T)

41. $N_1 \| \cdots \| N_n \leftarrow Partition(Pad_1(N))$
42. $C_1 \| \cdots \| C_c \leftarrow Partition(Pad_2(C))$
43. $A \leftarrow 0^a; B \leftarrow 1^b$
44. $X \leftarrow A \| B$
45. $A \leftarrow f(X); B \leftarrow f(\overline{X})$
46. FOR $i \leftarrow 1$ TO n DO
47. $X \leftarrow (A \| B) \oplus N_i$
48. IF $(X \in Dom) \cup (\overline{X} \in Dom) \cup (X|^b = X|_b)$
49. THEN $bad \leftarrow$ true

$$\boxed{X \twoheadleftarrow \{0,1\}^{2b} / (Dom \cup \overline{Dom} \cup Twofold)}$$

50. $Dom \leftarrow Dom \cup \{X, \overline{X}\}$
51. $A \leftarrow f(X); B \leftarrow f(\overline{X})$
52. FOR $i \leftarrow 1$ TO $m-1$ DO
53. $M_i \leftarrow A \oplus C_i|_b$
54. $X \leftarrow C_i|_b \| (B \oplus C_i|^a)$
55. IF $(X \in Dom) \cup (\overline{X} \in Dom) \cup (X|^b = X|_b)$
56. THEN $bad \leftarrow$ true

$$\boxed{X \twoheadleftarrow \{0,1\}^{2b} / (Dom \cup \overline{Dom} \cup Twofold)}$$

57. $Dom \leftarrow Dom \cup \{X, \overline{X}\}$
58. $A \leftarrow f(X); B \leftarrow f(\overline{X})$
59. $M_c \leftarrow (A \oplus C_c|_b)|_{|C_c|}$
60. $X \leftarrow A \| (B \oplus C_c|^a)$
61. IF $(X \in Dom) \cup (\overline{X} \in Dom) \cup (X|^b = X|_b)$

62. THEN $bad \leftarrow$ true

$\boxed{X \xleftarrow{} \{0,1\}^{2b}/(Dom \cup \overline{Dom} \cup Twofold)}$

63. $Dom \leftarrow Dom \cup \{X, \overline{X}\}$

64. $A \leftarrow f_1(X)$; $B \leftarrow f_2(\overline{X})$

65. $X \leftarrow A \| B$

66. IF $(X \in Dom) \cup (\overline{X} \in Dom) \cup (X|^b = X|_b)$

67. THEN $bad \leftarrow$ true

$\boxed{X \xleftarrow{} \{0,1\}^{2b}/(Dom \cup \overline{Dom} \cup Twofold)}$

68. $Dom \leftarrow Dom \cup \{X, \overline{X}\}$

69. $T' \leftarrow A$

70. IF $T = T'$ THEN $bad \leftarrow$ true

在解密操作中，需要额外处理 $\sigma_v + q_v$ 个分块. 这将导致计算 $\mathcal{A}$ 在 G_1 中的输出与 G_2 的输出概率产生一点儿变化.

$$|\Pr[\mathcal{A}^{G_1} \Rightarrow 1] - \Pr[\mathcal{A}^{G_2} \Rightarrow 1]| \leq \boldsymbol{Adv}_f^{\mathrm{prf}}(t + t_v, 2\sigma + 2\sigma_v + q + q_v + 2).$$

显然，G_2 与 G_3 仍然是“直到 *bad* 发生前相同”. 在 G_3 中，对 $\mathcal{O}$ 和 $\mathcal{O}^{-1}$ 询问时，在 18、24、30、37、49、56、62、67 行中 *bad* 被设为真的概率计算与机密性证明中的相类似. 除了 *bad* 在 70 行获得一个有效的伪造使得 *bad* 被设为真以外，在 G_3 中 *bad* 被设为真的概率上界为

$$\frac{(\sigma + \sigma_v + q + q_v)^2}{2^{2b-1}} + \frac{\sigma + \sigma_v + q + q_v}{2^b}.$$

接下来我们计算 *bad* 在 70 行被设为真的概率. 如果到 69 行 *bad* 仍为否，则 $\mathcal{A}$ 构造出一个有效伪造的概率由 f 的性质决定. 从而，

$$\Pr[\mathcal{A}^{G_3} \text{中 } bad \text{ 设为真}] \leq \frac{(\sigma + \sigma_v + q + q_v)^2}{2^{2b-1}} + \frac{\sigma + \sigma_v + q + q_v}{2^b} + \frac{q_v}{2^b}.$$

将上述结果进行加和，可以得到

$$\Pr[\mathcal{A}^{G_1} \Rightarrow 1] \leq \boldsymbol{Adv}_f^{\mathrm{prf}}(t + t_v, \sigma + \sigma_v + q + q_v + 2) + \frac{(\sigma + \sigma_v + q + q_v)^2}{2^{2b-1}} + \frac{\sigma + \sigma_v + q + 2q_v}{2^b}.$$

证毕.

6 讨　论

本节针对底层模块的选择进行讨论，说明我们选择压缩函数作为底层模块的原因，并将 DPE-族方案与同类方案进行比较和分析.

6.1 底层模块的选择

在认证加密方案的构造中，常用的底层模块包括分组密码、压缩函数以及固定置换. 我们选择采用压缩函数构造新方案的主要原因包括以下几点：

(1) 杂凑函数，与分组密码相同，都是应用广泛的密码原件，具备较为完善的分析研究基础，提供了大量关于压缩函数安全性与效率的研究成果；

(2) 利用具有长杂凑值的杂凑函数中的压缩函数，可以构造出高安全性的方案(例如，用 SHA-512 可获得的安全性等级约为 2^{256}，而使用 AES-128 可获得的安全性等级约为 2^{64})；

(3) 在安全性证明中，基于压缩函数构建的方案可以用经典的伪随机函数假设进行证明，而基于置换(包含分组密码)构建的方案则需要依赖于理想模型假设.

此外，基于 SHA-1 与 SHA-256 的压缩函数构建的方案，还可得益于 Intel 处理器对 SHA 系列算法扩展的支持(Intel SHA Extensions)[35]，达到高效快速的实现.

6.2 与同类方案的比较

目前公开提出的利用杂凑函数或压缩函数构建的加密方案与认证加密方案包括 HCBC[1]、HCTR[36]、CWC[37]、CHM[38]、BTM[39]、HBS[6]、FWPAE[9] 和 OMD[7-8] 等. 其中，大部分方案均以分组密码为主要底层模块，结合压缩函数进行构建，只有 OAE1 方案 FWPAE 和 OMD 仅使用压缩函数作为底层模块. 我们将 DPE-族方案中的 OAE1 方案 DPAE 与这两个方案进行比较，结果如表 1 所示.

表 1　DPE 与同类方案的比较

	FWPAE	OMD	DPAE
可用的压缩函数	Fast-Wide Pipe	SHA-256，SHA-512	满足条件的任意压缩函数
压缩函数平均调用次数	5/9	1	2
基本运算	拆分，异或	乘法，异或	异或
是否使用掩码	否	是	否
链值泄露是否会导致整个消息的链值泄露	是	否	否
机密性	$\frac{\sigma(\sigma+1)^2}{2^{n/4-1}}$	$\frac{3\sigma^2}{2^n}$	$\frac{(\sigma+q)^2}{2^{2n-1}} + \frac{\sigma+q}{2^n}$
完整性	$\frac{(\sigma+\sigma_v)^2+q+q_v}{2^{n/4-1}}$	$\frac{3(\sigma+\sigma_v)^2}{2^n} + \frac{\sigma_v+q_v}{2^n}$	$\frac{(\sigma+\sigma_v+q+q_v)^2}{2^{2n-1}} + \frac{\sigma+\sigma_v+q+2q_v}{2^n}$

由表 1 可以看出，DPAE 方案对于压缩函数的适应性最高，可以支持 ISO/IEC 10118-3:2003 中推荐的 SHA-256、SHA-512、Whirlpool 以及国密算法 SM3 等杂凑函数的压缩函数. 当使用杂凑函数作为

底层压缩函数时,DPAE 方案还可支持几乎所有满足条件(输入长度相同,并且输出长度之和等于输入长度)的杂凑函数或杂凑函数的组合. 在实现上,DPAE 方案仅需要底层压缩函数和异或运算即可实现,而无需引入其他运算. 由于 DPAE 每次需要调用两次压缩函数,在实现代价上略高于 FWPAE 和 OMD 方案;然而借助并行实现两次压缩函数的调用,DPAE 方案在运行速度上并不输于 FWPAE 和 OMD 方案. 在安全性上,我们取压缩函数输出的比特长度为 n 时的安全性证明结果进行比较,可以看到,DPAE 的机密性与完整性都显著高于 FWPAE 方案,并且略高于 OMD 方案. DPE-族中的 DPE 方案以及 DPAE-I 也同样具有类似的性质. 此外,DPAE-I 方案是目前唯一满足 OAE2-安全的基于压缩函数构建的认证加密方案.

7 总 结

本文基于压缩函数与双管道结构构造了一族加密方案,适用于使用压缩函数或使用基于压缩函数构建的杂凑函数的应用环境.

(1) DPE 方案是在线加密方案,利用底层压缩函数的迭代更新状态链值,并截取部分状态链值作为密钥流进行加密和解密操作,可以提供在线加密和在线解密的功能;

(2) DPAE 方案是在线认证加密方案(OAE1 方案),在 DPE 方案的基础上添加了认证操作,使得消息的接收方可以利用标签验证消息的完整性;

(3) DPAE-I 方案是在线的分块认证加密方案(OAE2 方案),利用 DPAE 方案支持使用中间标签的性质,将长消息划分为若干个短消息调用 DPAE 进行加密,其中前一个消息加密得到的状态将作为下一个消息的初始状态,将每一个短消息视为一个分块,当工作存储足够大时,DPAE-I 方案可以在加密和解密方向同时具有在线性.

通过简单的修改,可以实现该族方案的相互转化. 通过选取不同的压缩函数,可以灵活地在实现效率与安全性之间进行调节,在实用中具有较好的灵活性与适应性. 选取输出长度是输入长度一半的压缩函数,可以仅利用一个压缩函数和一个密钥实现 DPE-族方案,从而降低方案的实现代价.

借助于杂凑函数较为完善的分析研究基础以及对生成较大规模杂凑值的支持,使用标准中推荐的杂凑函数中的压缩函数时,DPE-族方案可以达到的安全性上界远高于基于分组密码构造的方案可以达到的安全性上界. 利用 Intel 处理器等设备对标准推荐杂凑函数的支持,DPE-族方案可以达到高效快速的实现. 与同类基于压缩函数构建的方案相比,DPE-族方案在对压缩函数的实用性与安全性上具有一定优势.

参 考 文 献

[1] Bellare M, Boldyreva A, Knudsen L, Namprempre C. Online ciphers and the hash-CBC construction//Proceedings of the 21st Annual International Cryptology Conference. Santa Barbara, USA, 2001: 292-309

[2] Fleischmann E, Forler C, Lucks S. McOE: A family of almost foolproof on-line authenticated encryption schemes//Proceedings of the 19th International Workshop on Fast Software Encryption. Washington, USA, 2012: 196-215

[3] Andreeva E, Bogdanov A, Luykx A, et al. Parallelizable and authenticated online ciphers//Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security. Bengaluru, India, 2013: 424-443

[4] Andreeva E, Luykx A, Mennink B, Yasuda K. COBRA: A parallelizable authenticated online cipher without block cipher inverse//Proceedings of the 21st International Workshop on Fast Software Encryption. London, UK, 2014: 187-204

[5] Hoang V T, Reyhanitabar R, Rogaway P, Vizár D. Online authenticated-encryption and its nonce-reuse misuse-resistance//Proceedings of the 35th Annual Cryptology Conference. Santa Barbara, USA, 2015: 493-517

[6] Iwata T, Yasuda K. HBS: A single-key mode of operation for deterministic authenticated encryption//Proceedings of the 16th International Workshop on Fast Software Encryption. Leuven, Belgium, 2009: 394-415

[7] Cogliani S, Maimuţ D, Naccache D, et al. Offset merkle-damgård (OMD) version 1.0 a CAESAR proposal//Bernstein D J. CAESAR First Round Submission. 2014

[8] Cogliani S, Maimuţ D, Naccache D, et al. OMD: A compression function mode of operation for authenticated encryption//Proceedings of the 21st International Conference on Selected Areas in Cryptography. Montreal, Canada, 2014: 112-128

[9] Manjunath R S, Sanadhya S K. Provably Secure Authenticated Encryption Modes[M. S. dissertation]. Indraprastha Institute of Information Technology, India, 2013

[10] Chakraborti A, Chattopadhyay A, Hassan M, Nandi M. TriviA: A fast and secure authenticated encryption scheme//Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Saint-Malo, France, 2015: 330-353

[11] Bertoni G, Daemen J, Peeters M, Van Assche G. Duplexing the sponge: Single-pass authenticated encryption and other applications//Proceedings of the International Workshop on Selected Areas in Cryptography. Toronto, Canada, 2011: 320-337

[12] Andreeva E, Bilgin B, Bogdanov A, et al. APE: Authenticated permutation-based encryption for lightweight cryptography//Proceedings of the 21st International Workshop on Fast Software Encryption. London, UK, 2014: 168-186

[13] Wu Hongjun, Huang Tao. JAMBU lightweight authenticated encryption mode and AES-JAMBU//Bernstein D J. CAESAR First Round Submission. 2014

[14] Alizadeh J, Aref M R, Bagheri N. Artemia: A family of provably secure authenticated encryption schemes. The ISeCure International Journal of Information Security, 2014, 6(2): 125-139

[15] Alizadeh J, Aref M R, Bagheri N. Artemia v1//Bernstein D J. CAESAR First Round Submission. 2014

[16] Dobraunig C, Eichlseder M, Mendel F, Schläffer M. ASCON v1//Bernstein D J. CAESAR First Round Submission. 2014

[17] Saarinen M J O. The CBEAMr1 authenticated encryption algorithm//Bernstein D J. CAESAR First Round Submission. 2014

[18] Morawiecki P, Gaj K, Homsirikamol E, et al. ICEPOLE v1//Bernstein D J. CAESAR First Round Submission. 2014

[19] Bertoni G, Daemen J, Peeters M, et al. Caesar submission: Ketje v1//Bernstein D J. CAESAR First Round Submission. 2014

[20] Bertoni G, Daemen J, Peeters M, et al. Keyak v1//Bernstein D J. CAESAR First Round Submission. 2014

[21] Aumasson J-P, Jovanovic P, Neves S. NORX v1//Bernstein D J. CAESAR First Round Submission. 2014

[22] Gligoroski D, Mihajloska H, Samardjiska S, et al. π-Cipher v1//Bernstein D J. CAESAR First Round Submission. 2014

[23] Saarinen M J O. The STRIBOB1 authenticated encryption algorithm//Bernstein D J. CAESAR First Round Submission, 2014

[24] Saarinen M J O, Brumley B B. WHIRLBOB, the Whirlpool based variant of STRIBOB//Proceedings of the 20th Nordic Conference on Secure IT Systems. Stockholm, Sweden, 2015: 106-122

[25] Datta N, Nandi M. ELmD v1//Bernstein D J. CAESAR First Round Submission. 2014

[26] Zhang Liting, Wu Wenling, Sui Han, Wang Peng. iFeed[AES] v1. CAESAR First Round Submission. 2014

[27] Lucks S. A failure-friendly design principle for hash functions//Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security. Chennai, India, 2005: 474-494

[28] Yasuda K. A double-piped mode of operation for MACs, PRFs and PROs: Security beyond the birthday barrier//Proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cologne, Germany, 2009: 242-259

[29] Yasuda K. On the full MAC security of a double-piped mode of operation. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, 94(1): 84-91

[30] Lee J, Steinberger J. Multiproperty-preserving domain extension using polynomial-based modes of operation. IEEE Transactions on Information Theory, 2012, 58(9): 6165-6182

[31] Stam M. Beyond uniformity: Better security/efficiency tradeoffs for compression functions//Proceedings of the 28th Annual International Cryptology Conference. Santa Barbara, USA, 2008: 397-412

[32] Stam M. Blockcipher-based hashing revisited//Proceedings of the 16th International Workshop on Fast Software Encryption. Leuven, Belgium, 2009: 67-83

[33] Rogaway P, Zhang H. Online ciphers from tweakable blockciphers//Proceedings of the Cryptographers Track at the RSA Conference. San Francisco, USA, 2011: 237-249

[34] Rogaway P, Shrimpton T. Deterministic authenticated encryption: A provable-security treatment of the key-wrap problem//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. St. Petersburg, Russia, 2006: 373-390

[35] Gulley S, Gopal V, Yap K, et al. Intel SHA Extensions: New Instructions Supporting the Secure Hash Algorithm on Intel Architecture Processors. USA: Intel Corporation, 2013

[36] Wang Peng, Feng Dengguo, Wu Wenling. HCTR: A variable-input-length enciphering mode//Proceedings of the International Conference on Information Security and Cryptology. Beijing, China, 2005: 175-188

[37] Tadayoshi Kohno, John Viega, Doug Whiting. CWC: A high-performance conventional authenticated encryption mode//Proceedings of the 11th International Workshop on Fast Software Encryption. Delhi, India, 2004: 408-426

[38] Iwata T. New blockcipher modes of operation with beyond the birthday bound security//Proceedings of the 13th International Workshop on Fast Software Encryption. Graz, Austria, 2006: 310-327

[39] Iwata T, Yasuda K. BTM: A single-key, inverse-cipher-free mode for deterministic authenticated encryption//Proceedings of the 16th Annual International Workshop on Selected Areas in Cryptography. Calgary, Canada, 2009: 313-330

SUI Han, born in 1986, Ph. D. candidate. Her research interests include the theory of provable security, design and analysis of authenticated encryption.

WU Wen-Ling, born in 1966, Ph. D., researcher, Ph. D. supervisor. Her research interests include design and cryptanalysis of block ciphers, modes of operation for block ciphers, and the theory of provable security.

ZHANG Li-Ting, born in 1982, Ph. D., associate professor, M. S. supervisor. His research interests include the theory of provable security, design of message authentication codes and authenticated encryption.

Background

This paper focuses on the design of online cipher and online authenticated encryption. In recent years, authenticated encryption schemes with online property have become a focus, and many schemes based on block ciphers and permutations have been proposed. The conception of authenticated encryption schemes with online encryption and online decryption is proposed recently, and few scheme has been designed. On the other hand, compression functions and hash functions are implemented widely, while few of schemes is built with them.

We propose the family of encryption schemes, called DPE, this paper, which is built with compression functions and double-pipe construction. The DPE family is dedicated to convenient facilitating in environments which already have components such as compression function based hash functions or compression functions. A scheme of the DPE family has online property, and provides privacy and integrity for data. Users can adjust between the efficiency and the security of a DPE/DPAE scheme flexibly by choosing different compression function.

The authors would like to thank the anonymous referees for their valuable comments. This work was supported by the National Natural Science Foundation of China (Grant Nos. 61672509 and 61572484), and the National Cryptography Development Fund (Grant No. MMJJ20170101).