ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 18238.2—2024
代替 GB/T 18238.2—2002

# 网络安全技术　杂凑函数
# 第2部分:采用分组密码的杂凑函数

**Cybersecurity technology—Hash-functions—Part 2: Hash-functions using a block cipher**

**(ISO/IEC 10118-2:2010, Information technology—Security techniques—Hash-functions—Part 2: Hash-functions using an n-bit block cipher, MOD)**

2024-09-29 发布　　2025-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 18238《网络安全技术　杂凑函数》的第2部分。GB/T 18238已经发布了以下部分：

——第1部分：总则；

——第2部分：采用分组密码的杂凑函数；

——第3部分：专门设计的杂凑函数。

本文件代替GB/T 18238.2—2002《信息技术　安全技术　散列函数　第2部分：采用$n$位块密码的散列函数》，与GB/T 18238.2—2002相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了术语“分组”（见3.1）；

b) 增加了杂凑函数的概述（见6.1）；

c) 更改散列函数3为杂凑函数2，更改散列函数4为杂凑函数3，并删除散列函数2（见第7章、第8章，2002年版的第7章、第8章、第9章）。

本文件修改采用ISO/IEC 10118-2:2010《信息技术　安全技术　杂凑函数　第2部分：采用$n$位块密码的杂凑函数》。

本文件与ISO/IEC 10118-2:2010相比做了下述结构调整：

——第7章对应ISO/IEC 10118-2:2010的第8章；

——第8章对应ISO/IEC 10118-2:2010的第9章。

本文件与ISO/IEC 10118-2:2010的技术差异及其原因如下：

——增加了规范性引用文件GB/T 25069—2022（见第3章）；

——更改了术语“$n$位分组密码”为“分组密码”，删除术语“轮函数”（见第3章）；

——增加了$D$、$D_i$、$H$、$H_i$、$IV$、$L_1$、$L_2$、$L_X$、$n$、$q$、$T$、$X \| Y$、$X \oplus Y$、$:=$、$\phi$，完善了符号定义（见第4章）；

——删除了ISO/IEC 10118-2:2010规定的杂凑函数2，因该杂凑函数已被发现存在安全问题；并将ISO/IEC 10118-2:2010规定的杂凑函数3和杂凑函数4依次更改为本文件的杂凑函数2（见第7章）及杂凑函数3（见第8章），同时优化了描述逻辑（见第7章、第8章）；

——删除了规范性附录C，因为该附录给出的代码不适用于我国情况。

本文件做了下列编辑性改动：

——为与我国技术标准体系协调，标准名称更改为《网络安全技术　杂凑函数　第2部分：采用分组密码的杂凑函数》；

——纳入了ISO/IEC 10118-2:2010/Cor 1:2011；

——增加了术语“分组”的注（见3.1）；

——增加了关于杂凑函数安全性提示的注释（见7.1、8.1）；

——更改了ISO/IEC第9章轮函数中笔误，将“与该杂凑函数相关的$\beta$的具体定义见8.1”更改为“与该杂凑函数相关的$\beta$的具体定义见7.5”（见第9章）；

——更改了资料性附录A，使用SM4分组密码算法替换了AES分组密码算法，以指导SM4算法的使用，将表A.1中“子函数$i$”更改为“密钥的前3位”，将表A.2中“子函数$i$”更改为“密钥的前4位”（见附录A）；

——更改了资料性附录 B,使用 SM4 分组密码算法给出了三种杂凑函数的示例(见附录 B);

——增加了资料性引用文件 GB/T 32907—2016(见附录 B);

——调整了部分语句(见 7.5、8.5),为方便阅读,对部分数据改用表格形式,并增加了表编号(见附录 B);

——调整了参考文献。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中电科网络安全科技股份有限公司、国家密码管理局商用密码检测中心、中国电子技术标准化研究院、中国科学院软件研究所、中国电子科技集团公司第十五研究所、山东大学、西安西电捷通无线网络通信股份有限公司、中国科学院信息工程研究所、中国科学院大学、北京银联金卡科技有限公司、山东得安信息技术有限公司、华为技术有限公司、格尔软件股份有限公司、智巡密码(上海)检测技术有限公司、北京江南天安科技有限公司、北京信安世纪科技股份有限公司、北京海泰方圆科技股份有限公司。

本文件主要起草人:张立廷、罗鹏、李彦峰、眭晗、毛颖颖、李艳俊、李世敏、王薇、黄晶晶、张国强、史丹萍、王鹏、孙思维、孙晓峰、杨波、谭亦夫、王秉政、马洪富、曾光、郑强、韩玮、李雪雁、龚晓燕、潘文伦、贾世杰、熊云、张雪、刘赣秦、魏曼。

本文件及其所代替文件的历次版本发布情况为:

——2002 年首次发布为 GB/T 18238.2—2002;

——本次为第一次修订。

# 引　言

杂凑函数使用特定的算法将任意长度(通常设有上限)的位串映射到固定长度的位串。采用分组密码的杂凑函数是指:在设计过程中,以分组密码算法(如 SM4 等)为主要部件,通过一定的迭代机制形成的杂凑函数。

GB/T 18238《网络安全技术　杂凑函数》由 3 个部分组成。

——第 1 部分:总则。目的在于规定杂凑函数的要求和通用模型,用于指导 GB/T 18238 的其他部分。

——第 2 部分:采用分组密码的杂凑函数。目的在于规定采用分组密码的杂凑函数。

——第 3 部分:专门设计的杂凑函数。目的在于规定专门设计的杂凑函数。

# 网络安全技术　杂凑函数
# 第2部分：采用分组密码的杂凑函数

## 1　范围

本文件规定了三种采用($n$ 位)分组密码的杂凑函数。第一种杂凑函数提供长度不大于 $n$ 位的杂凑值，第二种杂凑函数提供 $2n$ 位的杂凑值，第三种杂凑函数提供 $3n$ 位的杂凑值。

本文件适用于采用分组密码的杂凑函数的设计、开发和检测。

## 2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18238.1—2024　网络安全技术　杂凑函数　第1部分：总则(ISO/IEC 10118-1：2016，MOD)

注：GB/T 18238.1—2024 被引用的内容与 ISO/IEC 10118-1:2000 被引用的内容没有技术上的差异。

GB/T 25069—2022　信息安全技术　术语

## 3　术语和定义

GB/T 25069—2022 和 GB/T 18238.1—2024 界定的以及下列术语和定义适用于本文件。

3.1

**分组　block**

作为一个单位记录或传输的元素序列。

注：这里的元素是字符、字或记录。

[来源：GB/T 25069—2022，3.354]

3.2

**分组密码　block cipher**

加密算法在明文分组(即界定了长度的位串)上运算，以此产生密文分组的对称加密系统。

[来源：GB/T 25069—2022，3.161]

## 4　符号

下列符号适用于本文件。

$B^L$：当 $n$ 为偶数时，$n$ 位串 $B$ 的最左边的 $n/2$ 位位串；当 $n$ 为奇数时，$n$ 位串 $B$ 的最左边 $(n+1)/2$ 位位串。

$B^R$：当 $n$ 为偶数时，$n$ 位串 $B$ 的最右边的 $n/2$ 位位串；当 $n$ 为奇数时，$n$ 位串 $B$ 的最右边 $(n-1)/2$ 位位串。

$B_i$：当 $B$ 是由多个 $m$ 位字构成的序列时，$B_i$ $(i\geqslant 0)$ 表示 $B$ 的第 $i$ 个 $m$ 位字。特别地，当 $m=8$

时，$B_i$是$B$的第$i$个字节。

$C$：变换$u$的输入。

$D$：数据。

$D_i$：数据$D$经填充后的第$i$个$n$位分组。

$D_{j,i}$：输入到轮函数$\phi$的第$j$轮第$i$个$n$位分组。

$E$：$n$位分组密码算法。

$E_K(P)$：以明文$P$和密钥$K$作为输入的$n$位分组密码算法$E$的加密运算。

$H$：杂凑值。

$H_i$：用于存储杂凑运算中间结果的位串，其长度为$L_2$。

$H_{j,i}$：轮函数$\phi$的第$j$轮第$i$个$n$位分组输出。

$IV$：初始化值。

$K$：$n$位分组密码算法$E$的密钥。

$L_X$：位串$X$的位长度。

$L_1$：输入到轮函数$\phi$的两个位串中，第一个位串的位长度。

$L_2$：输入到轮函数$\phi$的两个位串中，第二个位串的位长度，也是轮函数$\phi$输出值的位长度，以及初始值$IV$的位长度。

$n$：$n$位分组密码算法$E$的分组长度。

$q$：经过填充和分割操作后，输入数据位串$D$的分组个数。

$T$：输出变换，比如截短。

$u$或$u'$：一种变换，把一个$n$位分组转换为分组密码算法$E$的密钥。

$X \| Y$：按顺序将位串$X$和$Y$连接所构成的位串。

$X \oplus Y$：位串$X$和位串$Y$的异或（其中$L_X = L_Y$）。

：=：赋值符号，表示符号左边的值应与符号右边的值相等。

$\phi$：轮函数。

## 5 通用模型的使用

第6章、第7章及第8章中规定的杂凑函数提供长度为$L_H$的杂凑值$H$，并且符合GB/T 18238.1—2024中规定的通用模型。因此，对于第6章、第7章及第8章中规定的三个杂凑函数，只需规定：

——参数$L_1$，$L_2$，$L_H$；

——填充方法；

——初始化值$IV$；

——轮函数$\phi$；

——输出变换$T$。

## 6 杂凑函数1

### 6.1 概述

本章规定的杂凑函数提供长度为$L_H$的杂凑值，其中$L_H \leqslant n$，推荐$n$不小于128。

附录A给出了初始化值和变换$u$的定义，附录B给出了示例。

注：参考文献[3]中9.4.1介绍了杂凑函数1。

### 6.2 参数选择

杂凑函数 1 的参数$L_1$、$L_2$和$L_H$应满足$L_1=L_2=n$，并且$L_H\leqslant n$，推荐 $n$ 不小于 128。

### 6.3 填充方法

杂凑函数 1 的填充方法应输出 $q\geqslant 1$ 个分组$D_1$，$D_2$，…，$D_q$，其中每个分组$D_j$的长度为 $n$ 位，并且不同的输入应产生不同的输出。具体填充方法采用 GB/T 18238.1—2024 附录 A 中 A.2 描述的方法 1。即，在数据串右侧填充一个位“1”，然后在所得到的位串右侧填充“0”，尽可能少填充(甚至不填充)，以达到所要求的长度。

### 6.4 初始化值

杂凑函数 1 的 $IV$ 的选择不属于本文件的范围。$IV$ 应是一个长度为 $n$ 位的位串，并且 $IV$ 的值应由杂凑函数的用户协商确定。

### 6.5 轮函数

轮函数 $\phi$ 用于产生$H_j$，其输入包括填充后的数据分组$D_j$(长度为$L_1=n$ 位)与轮函数前一步的输出$H_{j-1}$(长度为$L_2=n$ 位)，输出为$H_j$(长度为$L_2=n$ 位)。

作为轮函数的一部分，变换 $u$ 将 $n$ 位分组变换成分组密码算法 $E$ 的密钥。变换 $u$ 的定义超出了本文件的范围，示例见附录 A。

轮函数定义如下，如图 1 所示。

$$\phi(D_j,H_{j-1})=E_{K_j}(D_j)\oplus D_j,\text{其中}K_j=u(H_{j-1}),1\leqslant j\leqslant q,H_0=IV。$$

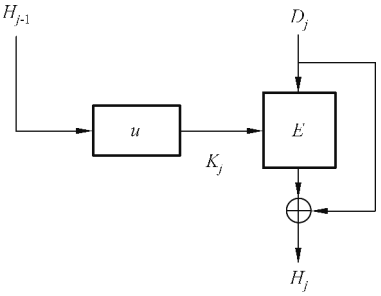


**图 1 杂凑函数 1 的轮函数**

### 6.6 输出变换

输出变换 $T$ 是简单的截短操作，即通过截取最终输出$H_q$的左边$L_H$位得到杂凑值 $H$。

## 7 杂凑函数 2

### 7.1 概述

本章规定的杂凑函数提供长度为$L_H$的杂凑值，其中$L_H=2n$，$n$ 为偶数。

B.3 给出了示例。

注 1：参考文献[4]介绍了杂凑函数 2。

注 2：参考文献[6][7][8][9]给出了针对杂凑函数 2 的轮函数的密码攻击。当 $n=128$ 时，找到杂凑函数 2 的轮函数的碰撞的复杂度为$2^{76.8}$，找到原像的复杂度为$2^{170.7}$。

### 7.2 参数选择

杂凑函数 2 的参数$L_1$、$L_2$和$L_H$应满足$L_1=4n$，$L_2=8n$，且$L_H=2n$，推荐 $n$ 不小于 128。

### 7.3 填充方法

具体填充方法应采用 GB/T 18238.1—2024 中 A.3 规定的方法 2，且 $r=n$。

### 7.4 初始化值

杂凑函数 2 的 $IV$ 的选择不属于本文件的范围。$IV$ 应是一个长度为 $8n$ 位的位串，并且 $IV$ 的值应由杂凑函数的用户协商确定。

### 7.5 轮函数

轮函数 $\phi$ 具有 8 个并行的加密过程，用于产生 8 个 $n$ 位串$H_{j,1}$，$H_{j,2}$，…，$H_{j,8}$。

在每次迭代中，轮函数 $\phi$ 的输入包括 4 个 $n$ 位数据分组$D_{j,1}$，$D_{j,2}$，$D_{j,3}$，$D_{j,4}$（总长度为$L_1=4n$ 位）与轮函数前一步的输出$H_{j-1,1}$，$H_{j-1,2}$，…，$H_{j-1,8}$（总长度为$L_2=8n$ 位），输出为$H_{j,1}$，$H_{j,2}$，…，$H_{j,8}$（总长度为$L_2=8n$ 位）。

令$H_{0,1}$，$H_{0,2}$，…，$H_{0,8}$满足$H_{0,1}\parallel H_{0,2}\parallel\cdots\parallel H_{0,8}=IV$。

对 $j=1$ 到 $q$，轮函数具有下列形式（见图 2）：

{$(X_{j,1},X_{j,2},\cdots,X_{j,8},Y_{j,1},Y_{j,2},\cdots,Y_{j,8}):=\gamma_1(H_{j-1,1},H_{j-1,2},\cdots,H_{j-1,8},D_{j,1},D_{j,2},D_{j,3},D_{j,4})$；

对 $i=1$ 到 8，执行：$H_{j,i}:=f_i(X_{j,i},Y_{j,i})$。}

轮函数基于线性映射$\gamma_1$和 8 个函数$f_i$，其中分别使用了线性映射 $\beta$ 和变换 $u$，定义如下。

a） 线性映射 $\beta$

线性映射 $\beta$ 将一个 $2n$ 位串 $X=x_0\parallel x_1\parallel x_2\parallel x_3$映射到一个 $2n$ 位串 $Y=y_0\parallel y_1\parallel y_2\parallel y_3$，具体方式如下：

$y_0:=x_0\oplus x_3$；

$y_1:=x_0\oplus x_1\oplus x_3$；

$y_2:=x_1\oplus x_2$；

$y_3:=x_2\oplus x_3$；

其中，$x_i$和$y_j$（$i,j=0,1,2,3$）均为 $n/2$ 长的位串。

b） 线性映射$\gamma_1$

$\gamma_1$的输入是 12 个 $n$ 位串$l_1$，$l_2$，…，$l_{12}$，映射$\gamma_1$需要 8 个 $2n$ 位辅助串$R_0$，$R_1$，$M_0$，$M_1$，…，$M_5$。

输出包括 8 个 $n$ 位串$X_1$，$X_2$，…，$X_8$和 8 个 $n$ 位串$Y_1$，$Y_2$，…，$Y_8$。

映射$\gamma_1$的运算过程如下（见图 3）：

1） 对 $i=0$ 到 5，执行：{

$M_i^L:=l_{2i+1}$；

$M_i^R:=l_{2i+2}$；

$M_i:=M_i^L\parallel M_i^R$}。

2） 令$R_0:=0$；$R_1:=0$；

对 $i=0$ 到 5，执行：{

$B:=R_1\oplus M_i$；

$R_1:=R_0\oplus\beta(B)$；

$R_0:=B$}。

3） 对 $i=1$ 到 8，执行：$X_i:=l_i$。

令 $Y_1:=R_0^L;Y_2:=R_0^R;Y_3:=R_1^L;Y_4:=R_1^R;$

对 $i=1$ 到 4，执行：$Y_{4+i}:=l_{8+i}$。

c) 变换 $u$

定义 8 个变换 $u_1,u_2,\cdots u_8$，它们的输入为长度为 $n$ 的位串，输出作为分组密码 $E$ 的密钥。要求对于集合{1,2,…8}中任意两个不同的 $i,j$，以及所有 $C$，变换 $u_1,u_2,\cdots u_8$ 满足 $u_i(C)\neq u_j(C)$。

上述条件可通过固定密钥的特定位而满足。例如，可将密钥中 3 个位的值分别固定为 000，001，…，111。为避免弱密钥或者分组密码互补性等问题，可对变换 $u_i$ 增加附加条件。

d) 函数 $f_i$

8 个函数 $f_i$ 定义如下：

$$f_i(X_{j,i},Y_{j,i})=E_{u_i(X_{j,i})}(Y_{j,i})\oplus Y_{j,i},1\leqslant i\leqslant 8。$$

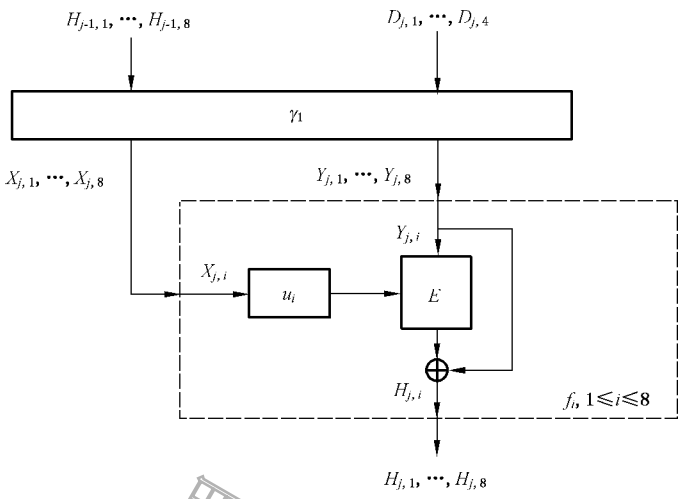


图 2 杂凑函数 2 的轮函数

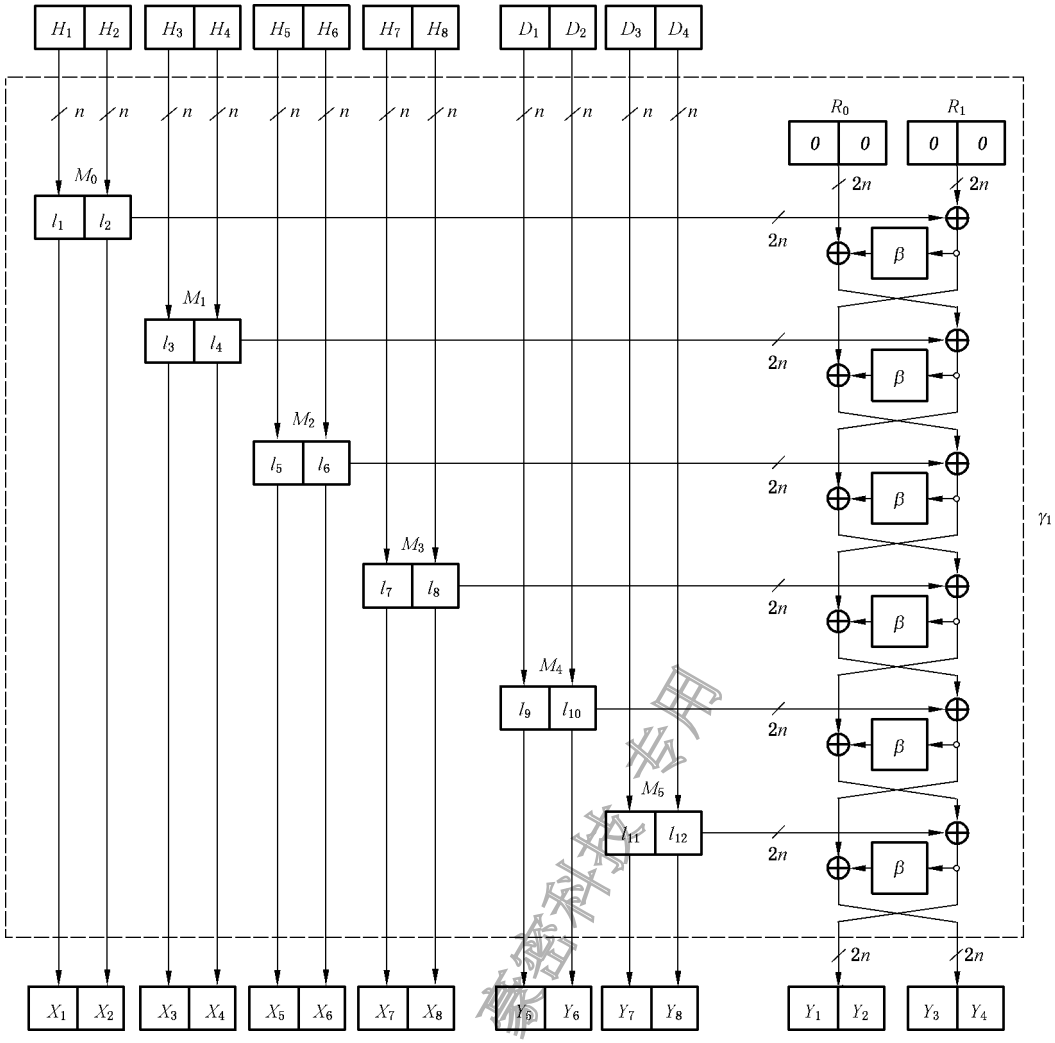


**图 3　杂凑函数 2 的线性映射 $\gamma_1$**

### 7.6　输出变换

处理完所填充的消息后，得到 $H_{q,1}$，$H_{q,2}$，…，$H_{q,8}$。然后执行 4 次附加的轮函数迭代，每次输入的 4 个 $n$ 位数据分组分别定义如下：

第 1 次，$D_{q+1,i}=H_{q,i}$，$1\leqslant i\leqslant 4$；

第 2 次，$D_{q+2,i}=H_{q,i+4}$，$1\leqslant i\leqslant 4$；

第 3 次，$D_{q+3,i}=H_{q,i}$，$1\leqslant i\leqslant 4$；

第 4 次，$D_{q+4,i}=H_{q,i+4}$，$1\leqslant i\leqslant 4$。

杂凑函数的输出 $H$ 由 $H_{q+4,1}\parallel H_{q+4,2}$ 构成。输出变换需进行 26 次加密（最后一次迭代仅需两次加密）。

## 8　杂凑函数 3

### 8.1　概述

本章规定的杂凑函数提供长度为 $L_H$ 的杂凑值，其中 $L_H=3n$，$n$ 为偶数。

B.4 给出了示例。

注 1：参考文献[5]介绍了杂凑函数 3。

注 2：参考文献[6][7][8][9]给出了针对杂凑函数 3 的轮函数的密码攻击。当 $n=128$，找到杂凑函数 3 的轮函数的碰撞复杂度为 $2^{85.3}$，找到原像复杂度为 $2^{192}$。

### 8.2 参数选择

杂凑函数 3 的参数 $L_1$、$L_2$ 和 $L_H$ 应满足 $L_1=3n$，$L_2=9n$，且 $L_H=3n$，推荐 $n$ 不小于 128。

### 8.3 填充方法

具体填充方法应采用 GB/T 18238.1—2024 中 A.3 规定的方法 2，且 $r=n$。

### 8.4 初始化值

杂凑函数 3 的 $IV$ 的选择不属于本文件的范围。$IV$ 应是一个长度为 $9n$ 位的位串，并且 $IV$ 的值应由杂凑函数的用户协商确定。

### 8.5 轮函数

轮函数 $\phi$ 具有 9 个并行的加密过程，用于产生 9 个 $n$ 位串 $H_{j,1}, H_{j,2}, \cdots, H_{j,9}$。

在每次迭代中，轮函数 $\phi$ 的输入包括 3 个 $n$ 位数据分组 $D_{j,1}, D_{j,2}, D_{j,3}$（总长度为 $L_1=3n$ 位）与轮函数前一步的输出 $H_{j-1,1}, H_{j-1,2}, \cdots, H_{j-1,9}$（总长度为 $L_2=9n$ 位），输出为 $H_{j,1}, H_{j,2}, \cdots, H_{j,9}$（总长度为 $L_2=9n$ 位）。

令 $H_{0,1}, H_{0,2}, \cdots, H_{0,9}$ 满足 $H_{0,1} \| H_{0,2} \| \cdots \| H_{0,9}=IV$。

对 $j=1$ 到 $q$，轮函数具有下列形式（见图 4）：

$\{(X_{j,1}, X_{j,2}, \cdots, X_{j,9}, Y_{j,1}, Y_{j,2}, \cdots, Y_{j,9}) := \gamma_2(H_{j-1,1}, H_{j-1,2}, \cdots, H_{j-1,9}, D_{j,1}, D_{j,2}, D_{j,3})$；

对 $i=1$ 到 9，执行：$H_{j,i} := f_i(X_{j,i}, Y_{j,i})$。$\}$

轮函数基于线性映射 $\gamma_2$ 和 9 个函数 $f_i$，其中分别使用了线性映射 $\beta$ 和变换 $u$，定义如下。

a) 线性映射 $\beta$

与该杂凑函数相关的 $\beta$ 的具体定义见 7.5。

b) 线性映射 $\gamma_2$

$\gamma_2$ 的输入是 12 个 $n$ 位串 $l_1, l_2, \cdots, l_{12}$，映射 $\gamma_2$ 需要 9 个 $2n$ 位辅助串 $R_0, R_1, R_2, M_0, M_1, \cdots, M_5$。

输出包括 9 个 $n$ 位串 $X_1, X_2, \cdots, X_9$ 与 9 个 $n$ 位串 $Y_1, Y_2, \cdots, Y_9$。

映射 $\gamma_2$ 运算过程如下（见图 5）：

1) 对 $i=0$ 到 5，执行：$\{$

$M_i^L := l_{2i+1}$；

$M_i^R := l_{2i+2}$；

$M_i := M_i^L \| M_i^R \}$。

2) 令 $R_0 := 0$；$R_1 := 0$；$R_2 := 0$；

对 $i=0$ 到 5，执行：$\{$

$B := R_2 \oplus M_i$；

$U := \beta(B)$；

$R_2 := R_1 \oplus U$；

$R_1 := R_0 \oplus U$；

$R_0 := B \}$。

3） 对 $i=1$ 到 9，执行：$X_i:=l_i$。

令 $Y_1:=R_0^L;Y_2:=R_0^R;Y_3:=R_1^L;Y_4:=R_1^R;Y_5:=R_2^L;Y_6:=R_2^R;$

对 $i=1$ 到 3，执行：$Y_{6+i}:=l_{9+i}$。

c） 变换 $u$

定义 9 个变换 $u_1,u_2,\cdots,u_9$，它们的输入为长度为 $n$ 的位串，输出作为分组密码 $E$ 的密钥。要求对于集合{1,2,…,9}中任意两个不同的 $i,j$，以及所有 $C$，变换 $u_1,u_2,\cdots,u_9$ 满足 $u_i(C)\neq u_j(C)$。

上述条件可通过固定密钥的特定位而满足。例如，可将密钥中 4 个位的值分别固定为 0000，0001，…，1000。为避免弱密钥或分组密码互补特性等问题，可对变换 $u_i$ 增加附加条件。

d） 函数 $f_i$

9 个函数 $f_i$ 定义如下：

$f_i(X_{j,i},Y_{j,i})=E_{u_i(X_{j,i})}(Y_{j,i})\oplus Y_{j,i}$，$1\leqslant i\leqslant 9$。

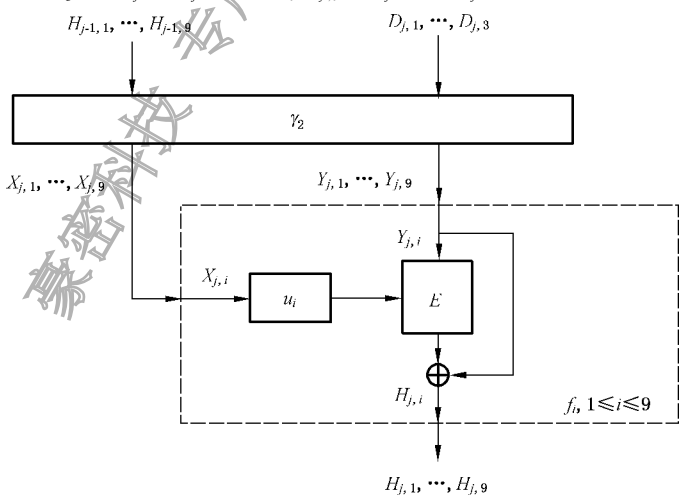


**图 4 杂凑函数 3 的轮函数**

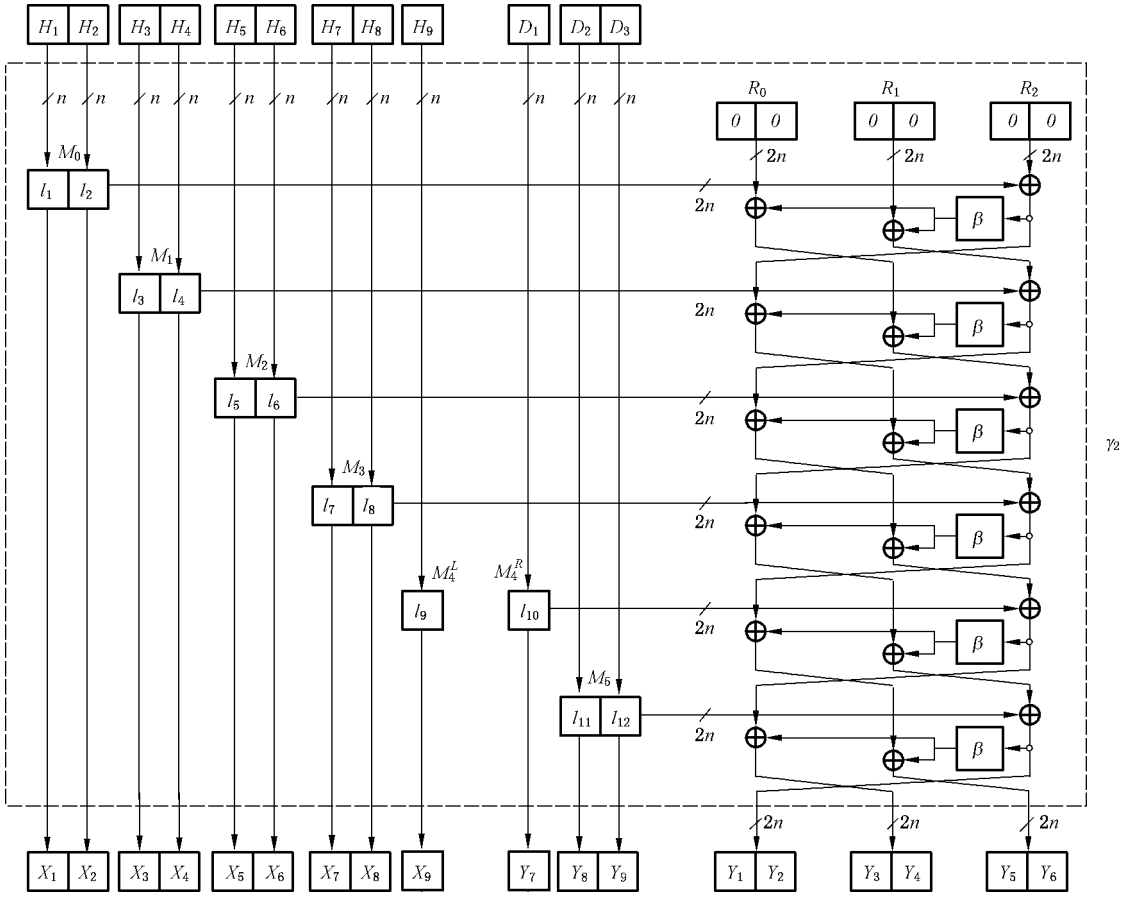


**图 5　杂凑函数 3 的线性映射 $\gamma_2$**

## 8.6　输出变换

处理完所填充的消息后，得到 $H_{q,1}$，$H_{q,2}$，…，$H_{q,9}$。然后执行 4 次附加的轮函数迭代，每次输入的 3 个 $n$ 位数据分组分别定义如下：

第 1 次，$D_{q+1,i}=H_{q,i}$，$1\leqslant i\leqslant 3$；

第 2 次，$D_{q+2,i}=H_{q,i+3}$，$1\leqslant i\leqslant 3$；

第 3 次，$D_{q+3,i}=H_{q,i+6}$，$1\leqslant i\leqslant 3$；

第 4 次，$D_{q+4,i}=H_{q,i}$，$1\leqslant i\leqslant 3$。

杂凑函数的输出由 $H_{q+4,1}\parallel H_{q+4,2}\parallel H_{q+4,3}$ 构成。输出变换需进行 30 次加密（最后一次迭代仅需要 3 次加密）。

# 附 录 A
（资料性）
初始化值和变换 $u$ 的定义

## A.1 概述

本附录提供了一种将 SM4 分组密码算法（见 GB/T 32907—2016）与本文件中规定的杂凑函数联合使用的参数实例。SM4 分组密码算法的参数 $n=128$，密钥 $K$ 的长度为 128 位。

## A.2 杂凑函数 1

$IV$ 等于“52525252525252525252525252525252”（十六进制表示）。

变换 $u$ 的定义方式如下：定义 $X=x_1x_2\cdots x_{128}$ 为一个 128 位串的二进制分解形式，则 $Y=u(X)=X$。

注：通常认为寻找轮函数和杂凑函数的碰撞需要执行 $2^{64}$ 次 SM4 加密操作。

## A.3 杂凑函数 2

$IV_1,IV_2,\cdots,IV_8$ 等于“52525252525252525252525252525252”（十六进制表示）。

变换 $u_1,u_2,\cdots,u_8$ 的定义方式如下：定义 $X=x_1x_2\cdots x_{128}$ 为一个 128 位串的二进制分解形式，$Y=u_i(X)$ 表示将 $x_1,x_2,x_3$ 置为表 A.1 中给定值所得到的位串。

表 A.1 杂凑函数 2 中 8 个子函数中密钥的第 1、2、3 位取值

| 子函数 $i$ | 密钥的前 3 位 |
|---|---|
| 1 | 000 |
| 2 | 001 |
| 3 | 010 |
| 4 | 011 |
| 5 | 100 |
| 6 | 101 |
| 7 | 110 |
| 8 | 111 |

## A.4 杂凑函数 3

$IV_1,IV_2,\cdots,IV_9$ 等于“52525252525252525252525252525252”（十六进制表示）。

变换 $u_1,u_2,\cdots,u_9$ 的定义方式如下：定义 $X=x_1x_2\cdots x_{128}$ 为一个 128 位位串的二进制分解形式，则 $Y=u_i(X)$ 表示将 $x_1,x_2,x_3,x_4$ 置为表 A.2 中给定值所得到的位串。

表 A.2　杂凑函数 3 中 9 个子函数中密钥的第 1、2、3、4 位取值

| 子函数 $i$ | 密钥的前 4 位 |
|---|---|
| 1 | 0000 |
| 2 | 0001 |
| 3 | 0010 |
| 4 | 0011 |
| 5 | 0100 |
| 6 | 0101 |
| 7 | 0110 |
| 8 | 0111 |
| 9 | 1000 |

# 附 录 B
（资料性）
示例

## B.1 概述

本附录采用 GB/T 32907—2016 规定的分组密码算法给出了使用第 6 章、第 7 章及第 8 章规定的所有杂凑函数计算杂凑值的示例，以及 GB/T 18238.1—2024 附录 A 中规定的填充方法的举例。

根据 GB/T 1988—1998 所规定的七位编码字符[1]，“Now_is_the_time_for_all_”（其中“_”表示空格）的十六进制数据串（无奇偶校验）表示如下：

“4E6F77206973207468652074696D6520666F7220616C6C20”。

## B.2 杂凑函数 1

杂凑函数 1 的 $IV$ 和变换 $u$ 见 A.2。

杂凑函数 1 的填充方法采用 GB/T 18238.1—2024 中 A.2 描述的方法 1。

表 B.1 给出了杂凑函数 1 的计算示例。

**表 B.1 杂凑函数 1 的计算示例**

| $j$ | $D_j$ | $H_{j-1}$ | $H_j$ |
|---|---|---|---|
| 1 | 4E6F772069732074<br>68652074696D6520 | 5252525252525252<br>5252525252525252 | 19962A4132D155DA<br>150D485598C6E7AA |
| 2 | 666F7220616C6C20<br>8000000000000000 | 19962A4132D155DA<br>150D485598C6E7AA | 64D32559B9166449<br>0B3255F75707B994 |

杂凑值（十六进制）：

“64D32559B91664490B3255F75707B994”。

## B.3 杂凑函数 2

杂凑函数 2 的 $IV$ 和变换 $u$ 见 A.3。

杂凑函数 2 的填充方法采用 GB/T 18238.1—2024 中 A.3 规定的方法 2，且 $r=n$。

表 B.2 给出了杂凑函数 2 的计算示例。

表 B.2　杂凑函数 2 的计算示例

| $D_{1,1}$，$D_{1,2}$，$D_{1,3}$，$D_{1,4}$ | $H_{0,1}$，$H_{0,2}$，$H_{0,3}$，$H_{0,4}$，<br>$H_{0,5}$，$H_{0,6}$，$H_{0,7}$，$H_{0,8}$ | $H_{1,1}$，$H_{1,2}$，$H_{1,3}$，$H_{1,4}$，<br>$H_{1,5}$，$H_{1,6}$，$H_{1,7}$，$H_{1,8}$ |
|---|---|---|
| 4E6F772069732074<br>68652074696D6520<br>666F7220616C6C20<br>8000000000000000<br>0000000000000000<br>0000000000000000<br>0000000000000000<br>00000000000000C0 | 5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252 | 30B6D4AAB4554969<br>87E5F12CF769F523<br>3FDBF7F7E321EA69<br>E362D9A035B05CA4<br>22CE803AD0AF18AE<br>9E5A92E2492990DB<br>20D76978ED8A2309<br>A52A600CA0C2C1E9<br>7E65EC61DD0D8CCF<br>26F6EA7E0F18CE70<br>A52E8EE709E61F49<br>B2E7E1A451EC8FC0<br>7AF1FD4E58EDF9C2<br>B4013FAA55D0286C<br>526E3CBB003BC67B<br>39C61CAD4B35A280 |
| $D_{2,1}$，$D_{2,2}$，$D_{2,3}$，$D_{2,4}$ | $H_{1,1}$，$H_{1,2}$，$H_{1,3}$，$H_{1,4}$，<br>$H_{1,5}$，$H_{1,6}$，$H_{1,7}$，$H_{1,8}$ | $H_{2,1}$，$H_{2,2}$，$H_{2,3}$，$H_{2,4}$，<br>$H_{2,5}$，$H_{2,6}$，$H_{2,7}$，$H_{2,8}$ |
| 30B6D4AAB4554969<br>87E5F12CF769F523<br>3FDBF7F7E321EA69<br>E362D9A035B05CA4<br>22CE803AD0AF18AE<br>9E5A92E2492990DB<br>20D76978ED8A2309<br>A52A600CA0C2C1E9 | 30B6D4AAB4554969<br>87E5F12CF769F523<br>3FDBF7F7E321EA69<br>E362D9A035B05CA4<br>22CE803AD0AF18AE<br>9E5A92E2492990DB<br>20D76978ED8A2309<br>A52A600CA0C2C1E9<br>7E65EC61DD0D8CCF<br>26F6EA7E0F18CE70<br>A52E8EE709E61F49<br>B2E7E1A451EC8FC0<br>7AF1FD4E58EDF9C2<br>B4013FAA55D0286C<br>526E3CBB003BC67B<br>39C61CAD4B35A280 | D025255C0A481635<br>20AF0388099E7DA0<br>CDC1BE650099E632<br>A63C83A0E72797A2<br>47B805D736D69995<br>3529A333C1042D5C<br>EA85BD9D380FA87C<br>97C8810FC788F90B<br>2B82AA57031E9EB3<br>37412B93DAC4B1B5<br>D83895AB41545471<br>B0330AB03DE0D24D<br>236BFFA0A5032F9B<br>026FD58722F4CBC0<br>86A9A73F93DFEDFF<br>7681630BBA6F90FD |

表 B.2　杂凑函数 2 的计算示例（续）

| $D_{3,1}$，$D_{3,2}$，$D_{3,3}$，$D_{3,4}$ | $H_{2,1}$，$H_{2,2}$，$H_{2,3}$，$H_{2,4}$，<br>$H_{2,5}$，$H_{2,6}$，$H_{2,7}$，$H_{2,8}$ | $H_{3,1}$，$H_{3,2}$，$H_{3,3}$，$H_{3,4}$，<br>$H_{3,5}$，$H_{3,6}$，$H_{3,7}$，$H_{3,8}$ |
|---|---|---|
| 7E65EC61DD0D8CCF<br>26F6EA7E0F18CE70<br>A52E8EE709E61F49<br>B2E7E1A451EC8FC0<br>7AF1FD4E58EDF9C2<br>B4013FAA55D0286C<br>526E3CBB003BC67B<br>39C61CAD4B35A280 | D025255C0A481635<br>20AF0388099E7DA0<br>CDC1BE650099E632<br>A63C83A0E72797A2<br>47B805D736D69995<br>3529A333C1042D5C<br>EA85BD9D380FA87C<br>97C8810FC788F90B<br>2B82AA57031E9EB3<br>37412B93DAC4B1B5<br>D83895AB41545471<br>B0330AB03DE0D24D<br>236BFFA0A5032F9B<br>026FD58722F4CBC0<br>86A9A73F93DFEDFF<br>7681630BBA6F90FD | 9FA15EB2B3046E98<br>E512D833E6EF28A5<br>A99E9BDFA6B6712B<br>327AB301AAFEC690<br>1B901DD4375EC5B9<br>9635DCEA9FF53442<br>D0C8D4F3613064E7<br>728ED1C306CB9E1F<br>68EC1A727A0648FD<br>BA56D6EFDC1B4127<br>E9F66BD310B6D073<br>5C7C3B95D52CB10D<br>34EAE9628C9A860D<br>23A3C089A1BCC263<br>FBB06E6943303A3D<br>C55A571D5D11923F |
| $D_{4,1}$，$D_{4,2}$，$D_{4,3}$，$D_{4,4}$ | $H_{3,1}$，$H_{3,2}$，$H_{3,3}$，$H_{3,4}$，<br>$H_{3,5}$，$H_{3,6}$，$H_{3,7}$，$H_{3,8}$ | $H_{4,1}$，$H_{4,2}$，$H_{4,3}$，$H_{4,4}$，<br>$H_{4,5}$，$H_{4,6}$，$H_{4,7}$，$H_{4,8}$ |
| 30B6D4AAB4554969<br>87E5F12CF769F523<br>3FDBF7F7E321EA69<br>E362D9A035B05CA4<br>22CE803AD0AF18AE<br>9E5A92E2492990DB<br>20D76978ED8A2309<br>A52A600CA0C2C1E9 | 9FA15EB2B3046E98<br>E512D833E6EF28A5<br>A99E9BDFA6B6712B<br>327AB301AAFEC690<br>1B901DD4375EC5B9<br>9635DCEA9FF53442<br>D0C8D4F3613064E7<br>728ED1C306CB9E1F<br>68EC1A727A0648FD<br>BA56D6EFDC1B4127<br>E9F66BD310B6D073<br>5C7C3B95D52CB10D<br>34EAE9628C9A860D<br>23A3C089A1BCC263<br>FBB06E6943303A3D<br>C55A571D5D11923F | 6294465C7D0BCCE6<br>FB24698833DACFD7<br>7AF13EDCB4E5FF5A<br>D65BC30F5409D696<br>65CE0EDE8DEB3D3A<br>D7F3DD403EC51A2F<br>5A975116A7A8B2CF<br>B78CB84C194A1A56<br>AEF6C71C90A68409<br>79BA0742ABD6202A<br>867C209558F73C01<br>A13028CA74ED7FC2<br>E23248975CC39A79<br>9A3E3E459E3A43EB<br>0E95EE60F1316985<br>8CE066207EB2A1C9 |

表 B.2　杂凑函数 2 的计算示例（续）

| $D_{5,1}$，$D_{5,2}$，$D_{5,3}$，$D_{5,4}$ | $H_{4,1}$，$H_{4,2}$，$H_{4,3}$，$H_{4,4}$，<br>$H_{4,5}$，$H_{4,6}$，$H_{4,7}$，$H_{4,8}$ | $H_{5,1}$，$H_{5,2}$，$H_{5,3}$，$H_{5,4}$，<br>$H_{5,5}$，$H_{5,6}$，$H_{5,7}$，$H_{5,8}$ |
|---|---|---|
| 7E65EC61DD0D8CCF<br>26F6EA7E0F18CE70<br>A52E8EE709E61F49<br>B2E7E1A451EC8FC0<br>7AF1FD4E58EDF9C2<br>B4013FAA55D0286C<br>526E3CBB003BC67B<br>39C61CAD4B35A280 | 6294465C7D0BCCE6<br>FB24698833DACFD7<br>7AF13EDCB4E5FF5A<br>D65BC30F5409D696<br>65CE0EDE8DEB3D3A<br>D7F3DD403EC51A2F<br>5A975116A7A8B2CF<br>B78CB84C194A1A56<br>AEF6C71C90A68409<br>79BA0742ABD6202A<br>867C209558F73C01<br>A13028CA74ED7FC2<br>E23248975CC39A79<br>9A3E3E459E3A43EB<br>0E95EE60F1316985<br>8CE066207EB2A1C9 | 47D40AFA02A78BCE<br>ACC4FD8AE5F27630<br>F3E3E2EADA85CCB0<br>9C2B6FC7C52EAFC5<br>C76952EA873747E4<br>FA8C24F36250F559<br>F991018E6989DC07<br>A9608ED223E1489D<br>4E6DBCC6CC4D1F5D<br>F4A987E25F1D2DAD<br>D2DE2E6E86A03A50<br>CA5D102F39BD0117<br>584D1D09BE68047B<br>8F9261319386B742<br>58436CDB28534000<br>60E1EC7E69DC8313 |

杂凑值(十六进制)：

“47D40AFA02A78BCEACC4FD8AE5F27630F3E3E2EADA85CCB09C2B6FC7C52EAFC5”。

## B.4　杂凑函数 3

杂凑函数 3 的 $IV$ 和变换 $u$ 见 A.4。

杂凑函数 3 的填充方法采用 GB/T 18238.1—2024 中 A.3 规定的方法 2，且 $r=n$。

表 B.3 给出了杂凑函数 3 的计算示例。

表 B.3　杂凑函数 3 的计算示例

| $D_{1,1}, D_{1,2}, D_{1,3}$ | $H_{0,1}, H_{0,2}, H_{0,3}, H_{0,4}, H_{0,5}, H_{0,6}, H_{0,7}, H_{0,8}, H_{0,9}$ | $H_{1,1}, H_{1,2}, H_{1,3}, H_{1,4}, H_{1,5}, H_{1,6}, H_{1,7}, H_{1,8}, H_{1,9}$ |
|---|---|---|
| 4E6F772069732074<br>68652074696D6520<br>666F7220616C6C20<br>8000000000000000<br>0000000000000000<br>00000000000000C0 | 5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252<br>5252525252525252 | 9A304A9FEF5D406E<br>A932C4D6DCAA3D0C<br>93F93F3626938154<br>9DBF1DB758A23E21<br>1EF73000E65E2A9D<br>929495B2E2A92ACE<br>51D11E67CAA959B5<br>5568CC730AD4346F<br>CAB5378477DBC1F3<br>5E3556A52A3BB22C<br>2B3E5E017DF74B0D<br>8F14A37ADF8D9AD1<br>151D61100664EE8F<br>48C3CF9EECD61483<br>1D5236CCF51AFD69<br>046A3E80FE13B1E1<br>4BC39D9BCE716A8A<br>E61AF9EBFE3159DE |
| $D_{2,1}, D_{2,2}, D_{2,3}$ | $H_{1,1}, H_{1,2}, H_{1,3}, H_{1,4}, H_{1,5}, H_{1,6}, H_{1,7}, H_{1,8}, H_{1,9}$ | $H_{2,1}, H_{2,2}, H_{2,3}, H_{2,4}, H_{2,5}, H_{2,6}, H_{2,7}, H_{2,8}, H_{2,9}$ |
| 9A304A9FEF5D406E<br>A932C4D6DCAA3D0C<br>93F93F3626938154<br>9DBF1DB758A23E21<br>1EF73000E65E2A9D<br>929495B2E2A92ACE | 9A304A9FEF5D406E<br>A932C4D6DCAA3D0C<br>93F93F3626938154<br>9DBF1DB758A23E21<br>1EF73000E65E2A9D<br>929495B2E2A92ACE<br>51D11E67CAA959B5<br>5568CC730AD4346F<br>CAB5378477DBC1F3<br>5E3556A52A3BB22C<br>2B3E5E017DF74B0D<br>8F14A37ADF8D9AD1<br>151D61100664EE8F<br>48C3CF9EECD61483<br>1D5236CCF51AFD69<br>046A3E80FE13B1E1<br>4BC39D9BCE716A8A<br>E61AF9EBFE3159DE | 3E01644F6ECE0205<br>E87427D25FB80C97<br>6CE2AC4EA5DE5EB7<br>E6DA9DAB83BB8391<br>D78698B09AA7D63F<br>BF1DBEA4A0902967<br>B41D779CDD4005A1<br>C502914148548B9B<br>5DFBA37C89152CD6<br>13C8FE2A68F4104D<br>25A4E0DE43FFE194<br>C5961FE557763364<br>94825DFAC3876DD3<br>7D65838C3FEC1C00<br>11DC013ED95C7340<br>69F9F41A9D5D228C<br>3D83262B6439632B<br>13DF35EFB919EEC3 |

表 B.3　杂凑函数 3 的计算示例（续）

| $D_{3,1}, D_{3,2}, D_{3,3}$ | $H_{2,1}, H_{2,2}, H_{2,3}, H_{2,4}, H_{2,5}, H_{2,6}, H_{2,7}, H_{2,8}, H_{2,9}$ | $H_{3,1}, H_{3,2}, H_{3,3}, H_{3,4}, H_{3,5}, H_{3,6}, H_{3,7}, H_{3,8}, H_{3,9}$ |
|---|---|---|
| 51D11E67CAA959B5<br>5568CC730AD4346F<br>CAB5378477DBC1F3<br>5E3556A52A3BB22C<br>2B3E5E017DF74B0D<br>8F14A37ADF8D9AD1 | 3E01644F6ECE0205<br>E87427D25FB80C97<br>6CE2AC4EA5DE5EB7<br>E6DA9DAB83BB8391<br>D78698B09AA7D63F<br>BF1DBEA4A0902967<br>B41D779CDD4005A1<br>C502914148548B9B<br>5DFBA37C89152CD6<br>13C8FE2A68F4104D<br>25A4E0DE43FFE194<br>C5961FE557763364<br>94825DFAC3876DD3<br>7D65838C3FEC1C00<br>11DC013ED95C7340<br>69F9F41A9D5D228C<br>3D83262B6439632B<br>13DF35EFB919EEC3 | 7477153B3708AAF4<br>33768C093B1394EF<br>57833395C67518AF<br>79B7F7E974611760<br>8DABDDB420397E6B<br>AF8ECF026058AB10<br>468B91C18250B7CF<br>AC9652A964267ED5<br>C6D50BAC97DDF05F<br>C642FCD9E750652A<br>F50B7B76E055AFF7<br>FD91944FFA3409A7<br>A5F307830968AEE0<br>C5F5BD23E632DD3A<br>3E0B63F8A002AF6B<br>5EB06C1442406516<br>8CA62F10882A0AB6<br>D59014A6BD91C502 |
| $D_{4,1}, D_{4,2}, D_{4,3}$ | $H_{3,1}, H_{3,2}, H_{3,3}, H_{3,4}, H_{3,5}, H_{3,6}, H_{3,7}, H_{3,8}, H_{3,9}$ | $H_{4,1}, H_{4,2}, H_{4,3}, H_{4,4}, H_{4,5}, H_{4,6}, H_{4,7}, H_{4,8}, H_{4,9}$ |
| 151D61100664EE8F<br>48C3CF9EECD61483<br>1D5236CCF51AFD69<br>046A3E80FE13B1E1<br>4BC39D9BCE716A8A<br>E61AF9EBFE3159DE | 7477153B3708AAF4<br>33768C093B1394EF<br>57833395C67518AF<br>79B7F7E974611760<br>8DABDDB420397E6B<br>AF8ECF026058AB10<br>468B91C18250B7CF<br>AC9652A964267ED5<br>C6D50BAC97DDF05F<br>C642FCD9E750652A<br>F50B7B76E055AFF7<br>FD91944FFA3409A7<br>A5F307830968AEE0<br>C5F5BD23E632DD3A<br>3E0B63F8A002AF6B<br>5EB06C1442406516<br>8CA62F10882A0AB6<br>D59014A6BD91C502 | 93D445A7A38994D3<br>C136F157C3C03430<br>2D90B7AAAA86A0AB<br>260046A3F179EEC6<br>13CF74B347A103F9<br>6B043C878916A6C1<br>2686E0F40F880139<br>647AAB613C1A95BF<br>A0A4413736983E5C<br>BA1956101043CC36<br>5FB7D4B6A4E5805A<br>00186426E667E3E4<br>7065048E87C6F917<br>3F423A018160B7B3<br>6DFD9BB611E1E48B<br>12D7434ABF4BCF01<br>C71B2FE97D37B65D<br>692ED0557E63781F |

表 B.3　杂凑函数 3 的计算示例（续）

| $D_{5,1}$，$D_{5,2}$，$D_{5,3}$ | $H_{4,1}$，$H_{4,2}$，$H_{4,3}$，$H_{4,4}$，<br>$H_{4,5}$，$H_{4,6}$，$H_{4,7}$，$H_{4,8}$，$H_{4,9}$ | $H_{5,1}$，$H_{5,2}$，$H_{5,3}$，$H_{5,4}$，<br>$H_{5,5}$，$H_{5,6}$，$H_{5,7}$，$H_{5,8}$，$H_{5,9}$ |
|---|---|---|
| 9A304A9FEF5D406E<br>A932C4D6DCAA3D0C<br>93F93F3626938154<br>9DBF1DB758A23E21<br>1EF73000E65E2A9D<br>929495B2E2A92ACE | 93D445A7A38994D3<br>C136F157C3C03430<br>2D90B7AAAA86A0AB<br>260046A3F179EEC6<br>13CF74B347A103F9<br>6B043C878916A6C1<br>2686E0F40F880139<br>647AAB613C1A95BF<br>A0A4413736983E5C<br>BA1956101043CC36<br>5FB7D4B6A4E5805A<br>00186426E667E3E4<br>7065048E87C6F917<br>3F423A018160B7B3<br>6DFD9BB611E1E48B<br>12D7434ABF4BCF01<br>C71B2FE97D37B65D<br>692ED0557E63781F | DA9A501ACD68F193<br>F5529C4ED9D0C5DA<br>50BEF92A12450BF7<br>E5BE851CE04622A6<br>0BBEC4603EBED88D<br>66E721B89D5473EB<br>1CAD1E24A08674C1<br>65105E1CB6AB811B<br>125948258B036BF4<br>295257051D3AFF17<br>F70398A361594D51<br>4AB647B6E68D7874<br>E6C8D0B35A429699<br>BDFFFE7DE7A52C10<br>AF8FCB95E9467F34<br>9D0EDFC767A45B8F<br>E2CA2FD43A271CEE<br>3D6DEF8BEDB4D28A |

杂凑值(十六进制)：

“DA9A501ACD68F193F5529C4ED9D0C5DA50BEF92A12450BF7E5BE851CE04622A60BBEC4603EBED88D66E721B89D5473EB”。

## 参 考 文 献

[1] GB/T 1988—1998 信息技术 信息交换用七位编码字符集

[2] GB/T 32907—2016 信息安全技术 SM4 分组密码算法

[3] Alfred Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press 1996, Fifth Printing (August 2001).

[4] Lars R. Knudsen, Bart Preneel. Hash Functions Based on Block Ciphers and Quaternary Codes. ASIACRYPT 1996: 77-90.

[5] Lars R. Knudsen, Bart Preneel. Fast and Secure Hashing Based on Codes. CRYPTO 1997: 485-498.

[6] Lars R. Knudsen, Bart Preneel. Construction of secure and fast hash functions using nonbinary error-correcting codes. IEEE Trans. Inf. Theory 48(9): 2524-2539 (2002).

[7] Onur Özen, Martijn Stam. Collision Attacks against the Knudsen-Preneel Compression Functions. ASIACRYPT 2010: 76-93.

[8] Onur Özen, Thomas Shrimpton, Martijn Stam. Attacking the Knudsen-Preneel Compression Functions. FSE 2010: 94-115.

[9] Jooyoung Lee. Provable Security of the Knudsen-Preneel Compression Functions. ASIACRYPT 2012: 504-525.

中 华 人 民 共 和 国
国 家 标 准
**网络安全技术 杂凑函数**
**第2部分:采用分组密码的杂凑函数**
GB/T 18238.2—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.net.cn
服务热线:400-168-0010
2024年9月第一版
*
书号:155066·1-77580