doi:10.11959/j.issn.1000-436x.2016154

对联接杂凑函数的“特洛伊”消息攻击

陈士伟[1,2]，金晨辉[1]

(1. 解放军信息工程大学三院，河南 郑州 450002；2. 信息保障技术重点实验室，北京 100072)

摘 要：“特洛伊”消息攻击是 Andreeva 等针对 MD 结构杂凑函数提出的一种攻击方法，首次将其应用于不同于 MD 结构的一类杂凑函数，即联接杂凑。结合联接杂凑的特点，综合利用 Joux 的多碰撞和深度为 $n-l$ 的“钻石树”结构多碰撞，构造出了 $2n$-bit 联接杂凑函数的长度为 $n\cdot 2^k$ 块的“特洛伊”消息，并据此首次提出了对其的固定前缀“特洛伊”消息攻击，其存储复杂性为 $2l+2^{n-l+1}+n\cdot 2^{k+1}$ 块消息，时间复杂性为 $O(n\cdot 2^{n+k}+l\cdot 2^l)$ 次压缩函数运算，远低于理想的时间复杂性 $O(n\cdot 2^{2n+k})$。

关键词：杂凑函数；联接杂凑；“特洛伊”消息攻击；多碰撞；复杂性

中图分类号：TP918 **文献标识码**：A

Trojan message attack on the concatenated hash functions

CHEN Shi-Wei[1,2], JIN Chen-Hui[1]

(1. The Third College, PLA Information Engineering University, Zhengzhou 450002, China;
2. Science and Technology on Information Assurance Laboratory, Beijing 100072, China)

Abstract: The Trojan message attack was proposed by Andreeva, et al. aiming at the hash functions with MD structure. First it was applied on the hash function beyond MD structure, that was, concatenated hash. Utilizing the property of the concatenated hash, and combining the Joux's multicollision and the “diamond” structure with the depth of $n-l$, a Trojan message of the length $n\cdot 2^k$ blocks for the $2n$-bit concatenated hash was constructed, based on which a chosen-prefix Trojan message attack was first proposed. And the memory complexity of proposed attack is about $2l+2^{n-l+1}+n\cdot 2^{k+1}$ blocks and the time complexity is about $O(n\cdot 2^{n+k}+l\cdot 2^l)$ computations of the compression function, much less than the ideal value $O(n\cdot 2^{2n+k})$.

Key words: hash functions, concatenated hash, Trojan message attack, multicollsion, complexity

1 引言

杂凑函数是密码学领域中一类重要的密码算法。它是将任意长度的消息转化成固定长度的二元字符串的一类函数，杂凑的结果称为杂凑值或摘要。若杂凑值的规模为 n bit，则称其为 n-bit 杂凑函数。一个杂凑函数 $H(M)$需要满足以下 3 条基本的安全性原则。

1) 抗碰撞性：找到满足 $H(M_1)=H(M_2)$ 的一对碰撞消息 (M_1,M_2) 在计算上是不可行的。

2) 抗原像性：对于给定的杂凑值 h，找到满足 $H(M)=h$ 的消息 M 在计算上是不可行的。

3) 抗第二原像性：对于给定的消息 M_1 和对应的杂凑值 $h=H(M_1)$，找到另一个消息 $M_2\neq M_1$，使 $H(M_2)=h$ 在计算上是不可行的。

杂凑函数的安全强度取决于杂凑值的规模，对于一个 n-bit 杂凑函数，如果找到产生相同杂凑值的一对碰撞消息的时间复杂性低于 $2^{\frac{n}{2}}$，或找到给定杂凑值的原像（或第二原像）的时间复杂性低于 2^n，则称该杂凑函数是可破的。

杂凑函数主要包括 2 部分，即压缩函数和迭代结构，其中，迭代结构是迭代压缩函数的一种变换

收稿日期：2015-09-08；**修回日期**：2016-05-31
基金项目：国家自然科学基金资助项目（No.61272041）
Foundation Item: The National Natural Science Foundation of China(No.61272041)

方式，比如杂凑函数 MD5、SHA-0 等所用的迭代结构是强化的 Merkle-Damgard[1,2]（简称 MD）结构。通常情况下，密码学者们在压缩函数是随机函数或满足某些性质的条件下，分析迭代结构的安全性，这类分析方法称为对杂凑函数的一般攻击。Merkle[1]和 Damgard[2]在压缩函数满足抗碰撞的条件下，证明了强化 MD 结构也是抗碰撞的，因此它在最初的杂凑函数设计中是最常用的一种迭代结构。然而，在假定压缩函数是随机函数的条件下，Joux[3]构造出了 MD 结构杂凑函数的 2^k-碰撞，即 2^k 个不同的消息产生相同的杂凑值，其时间复杂性约为 $O(k\cdot 2^{\frac{n}{2}})$，低于理想值 $O\left(2^{\frac{(k-1)n}{k}}\right)$。之后，Kelsey 和 Schneier 利用可扩展消息提出了对具有 MD 结构的杂凑函数的长消息第二原像攻击[4]，又利用“钻石树”结构提出了对其的选择目标强制前缀攻击（即“牧群”攻击）[5]。2011 年，陈士伟等[6]提出了对强化 MD 结构的改进“牧群”攻击。在这些对 MD 结构杂凑函数的有效攻击被提出的同时,密码学者们也开始尝试着分析并设计一些不同于 MD 结构的迭代结构。2009 年，Andreeva 等[7]基于 Joux 的 $l\cdot 2^{\frac{n}{2}}$ – 多碰撞构造出了深度为 l 的“钻石树”结构的方法，其时间复杂性约为 $O\left(2^{\frac{n+l}{2}}\right)$，并利用该方法将“牧群”攻击应用于联接杂凑、二次杂凑等与 MD 结构不同的其他迭代结构，进一步地将其转化为第二原像攻击。与此同时，他们提出了一种新的攻击方法——“特洛伊”消息攻击，但仅将其应用于 MD 结构杂凑函数。2013 年的亚密会上，Kortelainen T 等[8]提出了构造 n-bit 杂凑函数的深度为 d 的“钻石树”结构的新方法，其时间复杂性约为 $O\left(2^{\frac{n+d}{2}}\right)$，并提出了对 MD 结构杂凑函数的 2 类改进的“特洛伊”消息攻击。但是，迄今为止，没有文献提出对具有不同于 MD 结构的迭代结构的杂凑函数的“特洛伊”消息攻击。

联接杂凑是不同于 MD 结构的一种迭代结构，它利用 2 个不同的杂凑函数对输入消息进行杂凑，然后将 2 个杂凑的结果联接作为杂凑值输出，这是提高杂凑函数安全强度的一个简单又有效的设计思想。本文将综合利用“钻石树”结构、Joux 的多碰撞等多种技术，构造出 2n-bit 联接杂凑的长度为 $n\cdot 2^k$ 块的“特洛伊”消息，并据此提出对其的“特洛伊”消息攻击，其时间复杂性约为 $O(n\cdot 2^{n+k}+l\cdot 2^l)$，存储复杂性为 $2l+2^{n-l+1}+n\cdot 2^{k+1}$ 块消息。

2　基本概念

下面介绍联接杂凑函数和“特洛伊”消息攻击的相关概念。

2.1　联接杂凑函数

首先给出 MD 结构杂凑函数的概念。

设 $f:\{0,1\}^m\times\{0,1\}^n\to\{0,1\}^n$ 为压缩函数，$M=(m_0,m_1,\cdots,m_{t-1})$ 为输入的 t 块 m-bit 消息，则基于压缩函数 f 的 MD 结构杂凑函数 MD_f 的描述如下

$$MD_f(IV,M)=f(\cdots f(f(IV,m_0),m_1)\cdots m_{t-1})$$

就联接杂凑函数而言，对于任意的输入消息，它是将 2 个基于不同压缩函数的 MD 结构杂凑函数的杂凑结果联接之后作为杂凑值输出。下面给出 2n-bit 联接杂凑函数 $ConHF_{f_1,f_2}$ 的具体描述。

设 $f_1:\{0,1\}^m\times\{0,1\}^n\to\{0,1\}^n$ 和 $f_2:\{0,1\}^m\times\{0,1\}^n\to\{0,1\}^n$ 为 2 个不同的压缩函数，$M=(m_0,m_1,\cdots,m_{t-1})$ 为输入的 t 块 m-bit 消息，IV_1、IV_2 为 2 个初始链接变量，则

$$ConHF_{f_1,f_2}(IV_1,IV_2,M)=MD_{f_1}(IV_1,M)\|MD_{f_2}(IV_2,M)$$

下文中称 $MD_{f_1}(IV_1,M)$ 为第 1 条杂凑路径，$MD_{f_2}(IV_2,M)$ 为第 2 条杂凑路径。

2.2　“特洛伊”消息攻击

2009 年，Andreeva 等[7]提出了对杂凑函数的一种新的一般攻击方法，即“特洛伊”消息攻击，它本质上是一类第二原像攻击。其基本的攻击思路是首先攻击者 $\mathcal{A}$ 构造一个“特洛伊”消息 S 并提供给受害者 $\mathcal{V}$，$\mathcal{V}$ 从一个限定的集合中任意选择前缀 P 构成消息 $P\|S$ 传递给 $\mathcal{A}$。由于“特洛伊”消息 S 是由攻击者 $\mathcal{A}$ 构造的，故如果 S 能够满足一些特定的性质，则 $\mathcal{A}$ 就可以成功地给出消息 $P\|S$ 的一个第二原像。针对 MD 结构杂凑函数 H，Andreeva 等给出了以下 2 类“特洛伊”消息攻击。

1) 碰撞–“特洛伊”攻击：在 S 中引入一个限定的改变产生 S'，使 $H(P\|S)=H(P\|S')$。

2) 牧群–“特洛伊”攻击：在 S 几乎不发生改变的条件下，找到 P' 和 S'，使 $H(P\|S)=H(P'\|S')$。

2013 年，Kortelainen T 等[8]利用“钻石树”结构和可扩展消息技术提出了对 MD 结构杂凑的改进

版本的“特洛伊”消息攻击，即弱“特洛伊”攻击和强“特洛伊”攻击，其时间复杂性明显低于文献[5]中的攻击方法。

然而，迄今为止，并没有文献对联接杂凑抵抗“特洛伊”消息攻击的能力进行分析。

3 对联接杂凑函数的“特洛伊”消息攻击算法

“特洛伊”消息攻击中最关键的步骤在于“特洛伊”消息的构造。“特洛伊”消息的成功构造可以保证在攻击过程中只需改变“特洛伊”消息的小部分比特，即可给出原消息的第二原像。而由联接杂凑的描述可知，它是利用 2 个不同的 MD 结构杂凑函数对同一消息进行杂凑，并将杂凑的结果联接后输出，故构造出的“特洛伊”消息应该在 2 条杂凑路径上保持一致。下面将利用 Joux 的多碰撞技术和“钻石树”结构多碰撞技术提出对联接杂凑的固定前缀的“特洛伊”消息攻击，即对给定的单块前缀 Pre，找到 P' 和 S'，使 $ConHF_{f_1,f_2}(P\|S)=ConHF_{f_1,f_2}(Pre\|P'\|S')$，并对该攻击算法的计算复杂性进行分析。

3.1 算法描述

对联接杂凑函数的固定前缀“特洛伊”攻击分 2 个阶段，即“特洛伊”消息构造阶段和固定前缀的第二原像攻击阶段。在“特洛伊”消息构造阶段，为了保证“特洛伊”消息在 2 条杂凑路径上保持一致，首先在第 1 条路径上构造长度为 $(n-l)\frac{n}{2}$ 的多碰撞，然后以此多碰撞为基础构造出深度是 $n-l$ 的“钻石树”结构。接着，构造出长度为 n 的多碰撞，然后在 2^n 个多碰撞消息中选择出 1 个使 2 条路径上的消息一致。在固定前缀的第二原像攻击阶段，已构造的具有 2^{n-l} 个起始点的“钻石树”结构多碰撞和长度为 l 的多碰撞使能够成功找到产生相同杂凑值的第二原像。下面给出算法的具体描述（如图 1 所示）。

记 $f_i^*(i=1,2)$ 是以 f_i 为压缩函数的 MD 结构的杂凑函数，$P=\{p_i,i=0,1,2,\cdots,2^k-1\}$ 为给定的且双方已知的集合。

1) 第 1 阶段：“特洛伊”消息构造阶段

Step1 在第 1 条杂凑路径上,以 IV_1 为初始值，计算 $f_1(IV_1,Pre)\triangleq h_a$，并以 h_a 为起始点，利用文献[3]中 Joux 的方法构造长度为 $l+(n-l)\frac{n}{2}$ 块的多碰撞，产生的最终链接变量记为 h_b。

Step2 在第 2 条杂凑路径上，以 IV_2 为初始值，计算 $f_2(IV_2,Pre)\triangleq h'_a$，随机选择 2^{n-l} 个起始点，基于第 1 条杂凑路径上的长为 $(n-l)\frac{n}{2}$ 的多碰撞，构造出深度为 $n-l$ 的“钻石树”结构，产生的最终链接变量记为 h'_b。

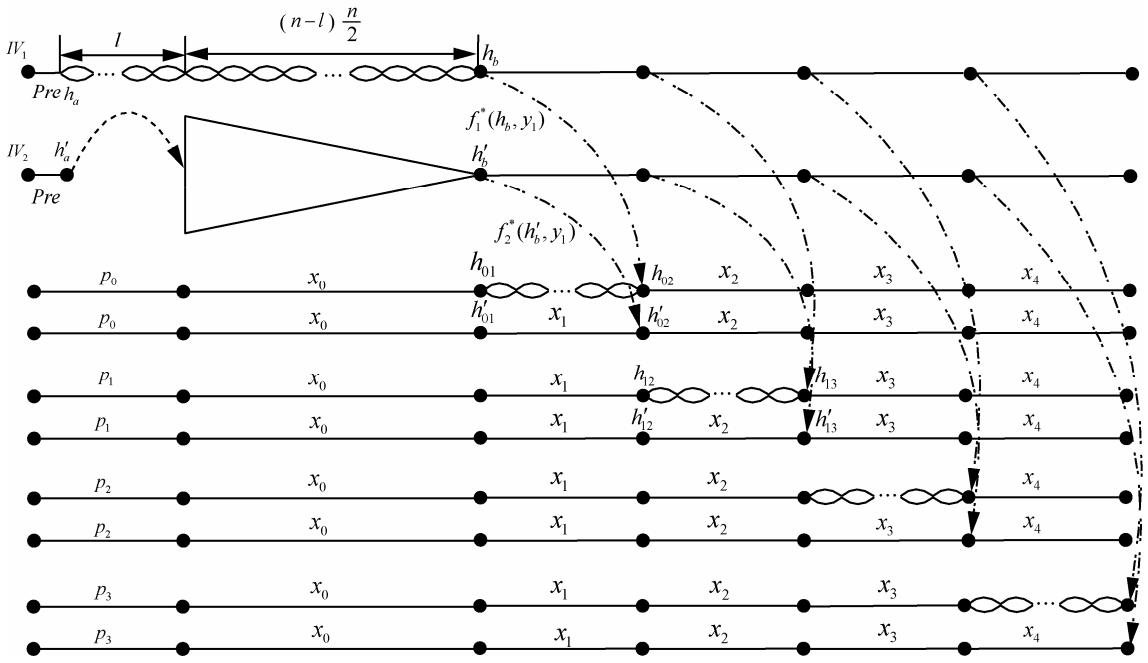


图 1 对联接杂凑函数的固定前缀“特洛伊”消息攻击

Step3　选择长度为 $(n-l)\frac{n}{2}$ 块的一个值 x_0，并计算 $f_1^*(IV_1, p_0 \| x_0) \triangleq h_{01}$，以链接变量 h_{01} 为起始点，构造一个长度为 n 块的多碰撞，产生的最终链接变量记为 h_{02}。

Step4　搜索长度为 n 块的一个值 y_1，使 $f_1^*(h_b, y_1) = h_{02}$。

Step5　记 $f_2^*(IV_2, p_0 \| x_0) = h'_{01}$，由于对任意元素 $0 \leqslant s \leqslant 2^n - 1$ 和固定的初始值 h，$P(f_i^*(h, x) = s) = \frac{1}{2^n}, i = 1,2$，故从 Step3 构造出的长度为 n 块的多碰撞中的 2^n 个消息中一定能够找到一个消息 x_1 使 $f_2^*(h'_b, y_1) = f_2^*(h'_{01}, x_1) \triangleq h'_{02}$，则有 $f_1^*(h_b, x_1) = f_1^*(h_b, y_1) = h_{02}$。

Step6　类似于 Step3~Step5，找到满足条件的第 i 个消息 x_i，即：记 $f_1^*(IV_1, p_{i-1} \| x_0 \| \cdots \| x_{i-1}) = h_{(i-1)i}$，在第 1 条杂凑路径上，以 $h_{(i-1)i}$ 为起始点，构造长度为 n 块的多碰撞，产生的最终链接变量记为 $h_{(i-1)(i+1)}$；搜索长度为 n 块的消息 y_i 使 $f_1^*(h_{(i-2)i}, y_i) = h_{(i-1)(i+1)}$；在第 2 条杂凑路径上，从第 1 条杂凑路径上产生的 n 块长多碰撞中的 2^n 个消息中找到一个消息 x_i 使 $f_2^*(h'_{(i-2)i}, y_i) = f_2^*(h'_{(i-1)i}, x_i) \triangleq h'_{(i-1)(i+1)}$，则有 $f_1^*(h_{(i-2)i}, y_i) = f_2^*(h_{(i-1)i}, x_i) = h_{(i-1)(i+1)}$。

Step7　依此类推，直至找到 2^k 个具有类似性质的消息 $x_1, x_2, x_3, x_4, \cdots, x_{2^k}$。

Step8　输出“特洛伊”消息 $x_0 x_1 x_2 \cdots x_{2^k}$。

攻击者 $\mathcal{A}$ 将构造出的“特洛伊”消息 $x_0, x_1, x_2, \cdots, x_{2^k}$ 传递给受害者 $\mathcal{V}$，受害者 $\mathcal{V}$ 从已知的前缀集合 P 中选择一个前缀值 p_i 并将消息 $p_i x_0 x_1 x_2 \cdots x_{2^k}$ 返回给 $\mathcal{A}$。下面 $\mathcal{A}$ 将给出消息 $p_i x_0 x_1 x_2 \cdots x_{2^k}$ 的一个固定前缀为 *Pre* 的第二原像。

2) 第 2 阶段：输出第二原像阶段

Step1　以 h'_a 为初始值，从第 1 阶段的 Step1 中构造的长度为 l 块的多碰撞中选择消息 $\bar{t}$，使 $f_2^*(IV_2, \bar{t})$ 等于“钻石树”的 2^{n-l} 个起始点中的一个，并在“钻石树”结构多碰撞中找到以此为起始点的消息 M_0。

Step2　输出消息 $\bar{t} \| M_0 \| x_1 \| \cdots \| x_{i-1} \| y_i \| x_{i+1} \| \cdots \| x_{2^k}$，则

$$H(\bar{t} \| M_0 \| x_1 \| \cdots \| x_{i-1} \| y_i \| x_{i+1} \| \cdots \| x_{2^k}) = H(p_i \| x_0 \| x_1 \| x_2 \| \cdots \| x_{2^k})$$

其长度为 $l + (n-l)\frac{n}{2} + n \cdot 2^k$ 块。

3.2　算法复杂性分析

下面分 2 个阶段给出联接杂凑的“特洛伊”攻击的时间复杂性和存储复杂性分析结果。

1) 第 1 阶段

在 Step1 中，构造长度为 $l + (n-l)\frac{n}{2}$ 块的多碰撞的时间复杂性为 $\left[l + (n-l)\frac{n}{2}\right]2^{\frac{n}{2}}$；由文献[6]的结果可知，Step2 中构造深度为 $n-l$ 的“钻石树”结构的时间复杂性为 $2^{n-\frac{l}{2}}$；Step3 中，由于 p_0 的长度为 l+1 块，x_0 的长度为 $(n-l)\frac{n}{2}$ 块，故计算 $f_1^*(IV_1, p_0 \| x_0) \triangleq h_{01}$ 需要 $(n-l)\frac{n}{2} + l + 1$ 次压缩函数运算，且构造 n 块长多碰撞的时间复杂性为 $n \cdot 2^{\frac{n}{2}}$；Step4 中，由于 f_1 的输出规模为 n，故随机选择 y_1 使 $f_1^*(h_b, y_1) = h_{02}$ 的时间复杂性为 $n \cdot 2^n$；Step5 从 2^n 个消息中找到满足条件的 x_1 所需的时间复杂性为 $n \cdot 2^n$；类似于 Step4 和 Step5，Step6 中找到满足条件的 x_i 所需的时间复杂性为 $n \cdot 2^{\frac{n}{2}} + 2n \cdot 2^n$，故找到“特洛伊”消息 $x_1, x_2, x_3, x_4, \cdots, x_{2^k}$ 所需的时间复杂性为 $2^k(n \cdot 2^{\frac{n}{2}} + 2n \cdot 2^n)$。因此，第 1 阶段所需的时间复杂性为

$$\left[l + (n-l)\frac{n}{2}\right]2^{\frac{n}{2}} + 2^{n-\frac{l}{2}} + (n-l)\frac{n}{2} + l + 1 + 2^k(n \cdot 2^{\frac{n}{2}} + 2n \cdot 2^n) = O(n \cdot 2^{n+k})$$

在 Step1 和 Step2 中，需存储长为 l 块的多碰撞和深度为 n–l 的“钻石树”结构，共 $2l + \sum_{i=0}^{n-l} 2^{n-l-i}$ 块消息；Step5~Step7 中，需存储 2^k 对长度为 n 的消息对 (x_i, y_i)，共 $2n \cdot 2^k$ 块消息，故第 1 阶段的存储复杂性为

$$2l + \sum_{i=0}^{n-l} 2^{n-l-i} + 2n \cdot 2^k = 2l + 2^{n-l+1} + n \cdot 2^{k+1}$$

2) 第 2 阶段

Step1 所需的时间复杂性为 $l \cdot 2^l$ 次压缩函数运算，且 Step2 的时间复杂性可忽略不计，故第 2 阶段的时间复杂性为 $l \cdot 2^l$，存储复杂性可忽略不计。

综合 2 个阶段的分析结果可知，对联接杂凑的固定前缀的“特洛伊”攻击的时间复杂性约为 $O(n\cdot 2^{n+k}+l\cdot 2^{l})$ 次压缩函数运算，存储复杂性约为 $2l+2^{n-l+1}+n\cdot 2^{k+1}$ 块消息。由于“特洛伊”攻击给出的第二原像的长度 $l+(n-l)\frac{n}{2}+n\cdot 2^{k}$ 块,故找到杂凑值规模为 $2n$ bit 的联接杂凑的相同长度的第二原像的理想计算复杂性为 $\left[l+(n-l)\frac{n}{2}+n\cdot 2^{k}\right]2^{2n}=n\cdot 2^{k+2n}$ 次压缩函数运算，约为本文给出的“特洛伊”消息攻击所需时间复杂性的 2^{n} 倍。

特别地，当 $k=l=\frac{n}{2}$ 时，本文提出的固定前缀的“特洛伊”攻击的时间复杂性为 $O(n\cdot 2^{\frac{3n}{2}})$，存储复杂性约为 $O((n+1)2^{\frac{n}{2}+1})$。

4 结束语

本文通过分析联接杂凑函数的特点，综合利用 Joux 的多碰撞和“钻石树”结构多碰撞，首次提出了对联接杂凑函数的固定前缀“特洛伊”消息攻击，其存储复杂性为 $2l+2^{n-l+1}+n\cdot 2^{k+1}$ 块消息，时间复杂性为 $O(n\cdot 2^{n+k}+l\cdot 2^{l})$ 次压缩函数运算，远低于理想的时间复杂性。这说明联接杂凑函数不能抵抗“特洛伊”消息攻击。

参考文献：

[1] MERKLE R. A certified digital signature[C]//Advances in Cryptology-CRYPTO 1989. LNCS 435, Heidelberg: Springer-Verlag, c1990: 218-238.

[2] DAMGARD I. A design principle for hash functions[C]//Advances in Cryptology-CRYPTO 1989. LNCS 435, Heidelberg: Springerr-Verlag, c1990: 416-427.

[3] JOUX A. Multicollisions in iterated hash functions application to cascaded constructions[C]//Advances in Cryptology–CRYPTO 2004. LNCS 3152, Heidelberg: Springer-Verlag, c2004: 306-316.

[4] KELSEY J, SCHNEIER B. Second preimages on *n*-bit hash functions for much less than 2^{n} work[C]//Advances in Cryptology- EUROCRYPT 2005. LNCS 3494, Heidelberg: Springer-Verlag, c2005: 474-490.

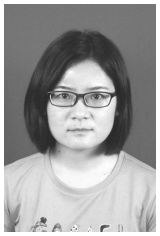
[5] KELSEY J, KOHNO T. Herding hash functions and the nostradamus attack[C]//Advances in Cryptology–EUROCRYPT 2006. LNCS 4004, Heidelberg: Springer-Verlag, c2006: 183-200.

[6] 陈士伟, 金晨辉. 对强化 MD 结构杂凑函数的一个新的“牧群”攻击[J]. 电子与信息学报, 2010, 32(8): 1953-1955.
CHEN S W, JIN C H. A new herding atlack on hash functions with strengthening Merke-Damgard(MD) construction[J]. Journal of Electronics & Information Technology, 2010, 32(8): 1953-1955.

[7] ANDREEVA E, BOUILLAGUET C, DUNKELMAN O, et al. Herding, second preimage and Trojan message attacks beyond Merkle-Damgård[C]//Selected Areas in Cryptography 2009. LNCS 5867, Heidelberg: Springer-Verlag, c2009: 393-414.

[8] KORTELAINEN T, KORTELAINEN J. On diamond structures and Trojan message attacks[C]//Advances in Cryptology–ASIACRYPT 2013, Part II, LNCS 8270. Heidelberg: Springer-Verlag, c2013: 524-539.

作者简介：



陈士伟（1983-），女，河南唐河人，解放军信息工程大学讲师，主要研究方向为对称密码算法分析。

金晨辉（1965-），男，河南扶沟人，解放军信息工程大学教授，主要研究方向为密码学与信息安全。