第 19 卷 第 6 期 电 子 科 学 学 刊 Vol.19 No.6
1997 年 11 月 JOURNAL OF ELECTRONICS Nov. 1997

基于强单向置换杂凑算法的构造和安全性分析 [1]

朱华飞 肖国镇 王新梅
(西安电子科技大学 西安 710071)

摘 要 本文利用 $\sum^n$ 上单向置换与完善置换的复合，构造基于强单向置换的杂凑算法，并证明了该算法的安全性等价于单向置换在多项式时间内不可求逆.

关键词 单向置换，完善置换，强单向置换

中图号 TN918.1

1 引 言

强单向置换在杂凑理论中起着十分重要的作用. 文献 [1] 利用 $\sum^n$ 上 $(k+1)$ 完善和单向置换二次复合，构造强单向置换，其中 $\sum=\{0,1\}$. 通过对该强单向置换 $t$bit 的切除，得到 $(n-t)$bit 的杂凑值. 这里 $t<n-k, k$ 为现有的能穷搜索 $k$bit 的计算能力. 但是，该方案仅具有理论上的意义，缺乏实用性. 这是因为 (1) 该方案在构造过程中要求单向置换硬比特位置与 $(k+1)$ 一完善置换的独立比特的位置相一致。事实上，对于单向置换而言，要确定硬比特的位置并非易事； (2) 每次复合运算的结果，至多能切除 $t$bit, 我们认为该方案并不是最优的. 其后，文献 [1] 又利用有限域 $\mathrm{GF}(2^n)$ 上的线性置换 $ax\oplus b$ 与 $\mathrm{GF}(2^n)$ 上的单向置换 $O(n/\log n)$ 次复合，构造强单向置换，通过 $t$bit 的切除，得到 $\sum^n$ 到 $\sum^{n-t}$ 的杂凑函数. 该算法虽然克服了不足之处 (1), 但并没有注意到 (2), 并且，由原来的二次复合运算提高到 $O(n/\log n)$ 次复合运算，无疑增加了计算量. 本文利用文献 [2] 的结果： $\mathrm{DES}(K,\bullet)$(带秘密密钥 K 的美国数据加密标准) 可以近似地看 $\sum^n$ 到 $\sum^n$ 上的完善置换，构造安全性等价于文献 [1], 但杂凑值的计算速度明显快于文献 [1] 的杂凑算法.

2 基本概念和结果

众所周知：若 f 是 $\sum^n$ 到 $\sum^n$ 上的单向置换 $(\sum=\{0,1\})$, 那么给定 $f(x)$, 在多项式时间内，找到变量 $x'\in\sum^n$, 满足 $f(x')=f(x)$ 是困难的. 这是因为：如果变元 x' 的每一比特都容易从 $f(x)$ 中求得，那么， f 就不可能是单向置换. 因此，给定 $f(x)$, 满足 $f(x')=f(x)$ 的变元 x' 的部分比特是难以确定的，我们把这些难以确定的比特称为 f 的硬比特 (hard bits) .

定义 1 [1] 设 f 是 $\sum^n$ 到 $\sum^n$ 上的单向置换，如果对于任何多项式时间概率算法 M, 任何多项式 $Q(n)$ 和所有足够大的自然数 n, 有

$$\mathrm{Prob}\{M(f(x))=x_i'\}<1/2+1/Q(n), \forall x\in_r\Sigma^n, \forall x'\in\Sigma^n,$$

[1] 1996-02-05 收到， 1997-01-15 定稿
国家自然科学基金资助项目

使得 $f(x')=f(x)$, 则称第 i 位比特是 f 的硬比特. 易见, f 的硬比特是由 f 结构本身决定的.

引理 1 [1] f 的所有硬比特是相互独立的.

定义 2 [1,2] 设 V 是 $\sum^n$ 到 $\sum^n$ 的置换, 称 V 是完善置换 (complete permutation) . 如果 V 输出的每一比特都依赖于输入的每一比特. 若 V^{-1} 也是完备的, 则称 V 是双向完备置换 (two-way complete permutation) .

引理 2 [1,2] 若 V 是 $\sum^n$ 上的完备置换, 则 V 是双向完备的.

定义 3 [1,2] 称 V 是 $\sum^n$ 上的完善置换 (perfect permutation), 如果 V 是完备置换, 并且 V 输出的所有比特是两两独立的.

引理 3 [2] $\mathrm{DES}(K,\bullet)$ 是 $\sum^n$ 到 $\sum^n$ 上的完善置换 (其中 K 为密钥) .

定义 4 [1,2] 称 V 是 $\sum^n$ 上的强单向置换, 如果 V 的每一位比特都是硬比特.

定理 1 设 f 是 $\sum^n$ 上的单向置换, V 是 $\sum^n$ 上的完善置换, 那么 $f\circ V\circ f$ 是 $\sum^n$ 上的强单向置换 (其中 $\circ$ 表示置换的复合运算) .

证明 记 $m=f_2\circ V\circ f_1(f_1=f_2=f)$. 假如第 i 位不是 m 的硬比特, 则存在多项式时间概率算法 M, 多项式 $Q(n)$ 使得

$$\mathrm{Prob}\{M(m(x))=x_i\}\geq 1/2+1/Q(n).$$

此即

$$\mathrm{Prob}\{\text{估计}x_i|\text{给定}m(x)\}\geq 1/Q(n).$$

现分两种情况讨论: (1) 若第 i 位不是 f_1 的硬比特. 则

$$\mathrm{Prob}\{\text{估计}x_i|\text{给定}f_1(x)\}\geq 1/Q'(n).$$

如果完善置换 V 在多项式时间内可逆, 则

$$\mathrm{Prob}\{\text{估计}x_i|\text{给定}V\circ f_1(x)\}=\mathrm{Prob}\{\text{估计}x_i|\text{给定}f(x)\}\geq 1/Q'(n).$$

由假设第 i 位不是 m 的硬比特, 得到

$$\begin{aligned}1/Q(n)&\leq Prob\{\text{估计}x_i|\text{给定}m(x)\}\\&=\mathrm{Prob}\{\text{估计}x_i|\text{给定}V\circ f_1(x)\}\mathrm{Prob}\{\text{得到}V\circ f_1(x)|\text{给定}m(x)\},\end{aligned}$$

从而

$$\mathrm{Prob}\{\text{得到}V\circ f_1(x)|\text{给定}m(x)\}\geq\mathrm{Prob}\{\text{估计}x_i|\text{给定}m(x)\}\geq 1/Q(n).$$

由于 V 是完善置换, 因此 $V\circ f_1(x)$ 的各比特相互独立, 从而 f_2 在多项式时间内可求逆, 这与 f_2 的单向性相矛盾.

如果 V 在多项式时间内不可求逆, 则 V 是单向完善置换. 因此

$$\mathrm{Prob}\{f_1(x)|V\circ f_1(x)\}<1/Q'(n).$$

由以下的关系式:

$$\mathrm{Prob}\{\text{估计}x_i|\text{给定}m(x)\}=\mathrm{Prob}\{\text{估计}x_i|\text{得到}f_1(x)\}\times\mathrm{Prob}\{\text{得到}f_1(x)|\text{得到}V\circ f_1(x)\}$$

$$\times \text{Prob}\{\text{得到}V\circ f_1(x)|\text{给定}m(x)\}$$
$$\le \text{Prob}\{\text{得到}f_1(x)|\text{得到}V\circ f_1(x)\} < 1/Q(n).$$

由 $Q'(n)$ 的任意性，知 x_i 是 $m(x)$ 的硬比特．这与假设相矛盾．

(2) 若第 i 位是 f_1 的硬比特，则

$$\text{Prob}\{\text{估计}x_i|\text{给定}f_1(x)\} < 1/Q'(n);$$

从而 $\text{Prob}\{\text{估计}x_i|\text{给定}V\circ f_1(x)\} < 1/Q'(n)$; 因此

$$\text{Prob}\{\text{估计}x_i|\text{给定}m(x)\} = \text{Prob}\{\text{估计}x_i|\text{给定}V\circ f_1(x)\}\text{Prob}\{\text{得到}V\circ f_1(x)|\text{给定}m(x)\}$$
$$\le \text{Prob}\{\text{估计}x_i|\text{给定}V\circ f_1(x)\} < 1/Q'(n).$$

此即表明第 i 位是 m 的硬比特．这与假设相矛盾．

综合 (1),(2) 我们得到定理 1 的证明．

众所周知： $\text{DES}(K,\bullet)$, 当密钥 K 保密时可作为单向函数来使用．因此如果 f 用含秘密密钥 K 的 DES 来替代，那么我们得到以下极为有用的结论．

定理 2 $\text{DES}(K_2,\bullet)\circ\text{DES}(K_1,\bullet)\circ\text{DES}(K_2,\bullet)$ 是强单向置换．

3 强单向置换在杂凑理论中的应用

我们知道：杂凑函数就其是否带秘密密钥 K, 分为消息认证码 (MAC) 和探测处理码 (MDC) 两大类 [3] ．这一节我们利用强单向置换构造安全的杂凑方案．

设通信双方 A,B 在每次通信前，选定一秘密密钥 K, 通信一方 A 欲传输消息 M 给 B,A 对于要传输的消息 M, 经过 MD 强化后 [4], 记为 $M = M_1M_2\cdots M_m$ 其中 $|M_i| = n,(i = 1,\cdots,m)$ ．计算

$$H_1 = f\circ\text{DES}(K, f(M_1\oplus H_0)),$$
$$H_2 = f\circ\text{DES}(K, f(M_2\oplus H_1)),$$
$$\cdots$$
$$H_m = f\circ\text{DES}(K, f(M_m\oplus H_{m-1})),$$

其中 H_0 为 $n$bit 的杂凑初始值． H_m 称为消息 M 的杂凑值或认证符，记为 $H(M,H_0)$ ．

A 通过公开信道传输 $(M,H(M,H_0))$ ．当 B 接收到 $M',\hat{H}(M',H_0))$ 时，对 M' 作用同样的计算，若 $\hat{H}(M',H_0) = H(M',H_0)$, 则认为消息 M' 在传输过程中未被敌手篡改或伪造，并由预先选定的密钥 K, 可确定消息 M' 来自 A ．

由于 f 是单向置换． $\text{DES}(K,\bullet)$ 是完善置换，从而对该杂凑方案的攻击不存在优于暴力攻击的任何攻击；且由 $f\circ\text{DES}(K,\bullet)\circ f$ 是强单向置换，消息 M 的杂凑值 $H(M,H_0)$ 具有最优的混淆和扩散特征．因此该方案具有理想的计算复杂性 [4] ．特别地，若 $\text{DES}(K,\bullet)$ 中的密钥 K, 用 M_i 代替时，得到消息 M 的探测处理码，也有上述所述的安全性．因此我们不难得到以下的结论：

定理 3 基于强单向置换的消息认证码，其安全性等价于单向置换在多项式时间内不可求逆。

定理 4 基于强单向置换的探测处理码，其安全性等价于单向置换在多项式时间内不可求逆．

4 结束语

我们已经证明若 f 是 $\sum^n$ 上的单向置换，V 是 $\sum^n$ 上的完善置换，那么 $f \circ V \circ f$ 是 $\sum^n$ 上的强单向置换．特别地，如果 f 用含秘密密钥 K 的 DES 来替代，那么我们可断言 $\mathrm{DES}(K_2,\bullet)\circ\mathrm{DES}(K_1,\bullet)\circ \mathrm{DES}(K_2,\bullet)$ 是强单向置换．因此本文实际上已经证明了三重 DES 是强单向置换．这些结果对于进一步研究单向函数的密码学特性有一定的促进作用．但是如何从更弱的条件下构造强单向置换仍是我们努力的一个主题．

参 考 文 献

[1] Pieprzyk J, Sadeghiyan B. Design of Hashing Algorithm. Berlin Heidelberg: Springer–Verlag, 1993: 132–169.

[2] Webster A F, Tavares S E. On The Design of S–Boxes. Advances in Cryptology–CRYPTO'85, Santa Barbara: 1985, Berlin Heidelberg: Springer-Verlag, 1986: 523–534.

[3] Preneel B, Govaerts R, Bandewalle J. Information Authentication: Hash Functions and Digital Signatures. Computer Security and Industrial Cryptology, State of the EAST curse, Leuven 1991, Berlin Heidelberg: Springer–Verlag, 1993: 88–130.

[4] X Lai; Massey J L. Hash Function Based on Block Ciphers. Advances in Cryptology–EUROCRYPT'92. Balatonfured: 1992, Berlin Heidelberg: Springer-Verlag, 1993, 50–70.

THE CONSTRUCTION AND SECURITY ANALYSIS OF HASH ALGORITHM BASED ON STRONG ONE-WAY PERMUTATION

Zhu Huafei　Xiao Guozhen　Wang Xinmei

(Xidian University, Xi'an 710071)

Abstract This paper constructs the Hash algorithm based on strong one-way permutation by the composition of one-way permutation and perfect permutation on $\sum^n$ and proves that its security is equivalent to the one-way permutation that can not be inversed in polynomial time.

Key words One-way permutation, Perfect permutation, Strong one-way permutation

朱华飞：　男，1966 年生，博士，主要从事杂凑函数、消息认证码和代数编码理论的研究．

肖国镇：　男，1935 年生，教授，博士生导师，主要从事密码学、纠错码和信息论等方面的教学和研究．

王新梅：　男，1937 年生，教授，博士生导师，主要从事纠错码、信源编码和密码学等方面的教学和研究．