软件学报 ISSN 1000-9825, CODEN RUXUEW
[doi: 10.13328/j.cnki.jos.007646] [CSTR: 32375.14.jos.007646]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

具有最优坍塌安全性的双分组长度哈希函数*

张绍煊[1,2], 郭 淳[1,2,3]

[1](山东大学 网络空间安全学院, 山东 青岛 266237)

[2](密码技术与信息安全教育部重点实验室 (山东大学), 山东 青岛 266237)

[3](山东省工业技术研究院, 山东 济南 250102)

通信作者: 张绍煊, E-mail: shaoxuanzhang@mail.sdu.edu.cn

摘 要: 双分组长度哈希函数是提高哈希函数具体安全性的一种经典方法, 该结构已被证明在一定条件下能达到最优的量子抗碰撞性. 然而, 针对坍塌性这一适用性更强的量子安全模型, 双分组长度哈希函数能否达到最优具体安全性还是一个开放性问题. 为了进一步研究此问题, 考虑在量子条件下抗碰撞性的扩展属性坍塌性, 并研究基于随机谕言机的 Nandi 之双分组哈希结构的坍塌性. 提出当结构内的置换 π 完全是由若干个 c-循环 (c-cycle) 置换 (即对于任意 $x\in\{0,1\}^m$, $\pi^a(x)=x$ 当且仅当 $a=c$) 组成时, 该结构的坍塌性达到最优, 而构造满足由若干个 c-循环置换组成的置换 π 是简单的. 最优的坍塌性意味着当随机谕言机输出大小为 n 比特时, 敌手至少进行 $O(2^{2n/3})$ 次查询, 才能有效区分测量量子叠加信息的哈希值与测量量子叠加信息本身两个状态. 该最优结构也可由 Merkle-Damgård 结构进行扩展, 扩展后的哈希函数仍具有坍塌性, 这为今后坍塌哈希函数的设计提供了理论基础.

关键词: 后量子安全性; 哈希函数; 双分组长度; 压缩函数; 坍塌性

中图法分类号: TP311

中文引用格式: 张绍煊, 郭淳. 具有最优坍塌安全性的双分组长度哈希函数. 软件学报. http://www.jos.org.cn/1000-9825/7646.htm

英文引用格式: Zhang SX, Guo C. Double-block-length Hash Function with Optimal Collapsing Security. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7646.htm

Double-block-length Hash Function with Optimal Collapsing Security

ZHANG Shao-Xuan[1,2], GUO Chun[1,2,3]

[1](School of Cyber Science and Technology, Shandong University, Qingdao 266237, China)

[2](Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education (Shandong University), Qingdao 266237, China)

[3](Shandong Research Institute of Industrial Technology, Jinan 250102, China)

Abstract: Double-block-length hash functions are a classical approach for amplifying the concrete security of hash functions. This construction has been proven to achieve optimal quantum collision resistance under certain conditions. However, whether double-block-length constructions can still achieve optimal concrete security in the stronger and more applicable quantum security model of the collapsing property remains an open question. To conduct a further study on this issue, this study considers the collapsing property, which extends the notion of collision resistance in the quantum setting. This study focuses on the collapsing security of Nandi's double-block-length construction based on a random oracle. This study proposes that when the permutations π within the construction is composed completely of a number of c-cycle permutations (i.e., for any $x\in\{0,1\}^m$, $\pi^a(x)=x$ if and only if $a=c$), the collapsing security of this construction is optimal. Constructing a permutation π composed solely of c-cycle permutations is straightforward. Optimal collapsing security implies that when the output size of the random oracle is n bits, the adversary can effectively distinguish between the two states, measuring the hash value of a quantum superposition of messages and measuring the message superposition itself, only after making at

* 基金项目: 国家重点研发计划 (2023YFA1011200); 国家自然科学基金 (62372274)
收稿时间: 2025-06-10; 修改时间: 2025-09-18; 采用时间: 2026-01-30; jos 在线出版时间: 2026-07-22

least $O(2^{2n/3})$ queries. The proposed optimal construction can also be extended by the Merkle-Damgård construction. The extended hash function retains the collapsing property. Therefore, this study provides a theoretical foundation for the design of collapsing hash functions in the future.

Key words: post-quantum security; hash function; double-block-length; compression function; collapsing

1 引 言

哈希函数是现代密码学的核心原语之一, 几乎在所有的加密协议中都有使用. 构造哈希函数常用方法之一是首先设计一个压缩函数 $CF_n^{n+k}\colon \{0,1\}^{n+k}\to\{0,1\}^n$, 然后使用 Merkle-Damgård 结构[1,2]将压缩函数 CF_n^{n+k} 扩展为可变输入长度的哈希函数. 压缩函数 CF_n^{n+k} 通常基于分组密码 $E_n^{n+k}\colon \{0,1\}^k\times\{0,1\}^n\to\{0,1\}^n$ 构造, 例如 Davies-Meyer 结构[3]. 很多经典的哈希函数, 如 MD 系列[4−6]、SHA-1[7]和 SHA-2[8]等, 都使用了这种构造方法.

抗碰撞性作为哈希函数的核心安全属性之一, 是密码学领域的研究热点. 哈希函数的抗碰撞性与其压缩函数的长度密切相关. 具体而言, 对于任何输出为 n 比特的压缩函数 $CF_n^{n+k}\colon \{0,1\}^{n+k}\to\{0,1\}^n$, 都可在 $O(2^{n/2})$ 时间内找到该函数的一个碰撞 $CF_n^{n+k}(x)=CF_n^{n+k}(x')$. 这意味着当 n 过小, 如 $n=128$ 时, 函数将不再具有抗碰撞安全性. 为此, 学界引入了双分组长度哈希的概念 (请参阅文献 [9] 以了解早期讨论). 此类结构利用高超的设计技巧, 使用 n 比特压缩函数或分组密码构造 $2n$ 比特的压缩函数, 以求超过 $n/2$ 比特的抗碰撞性. 按照这条路线, 学界提出了许多具有更高安全性[10−12]或效率[13−18]的双分组哈希结构, 其中具有代表性的一个就是 Nandi 之双分组哈希结构[18].

本文重点关注 Nandi 之双分组哈希结构[18] $F^{\pi}\colon \{0,1\}^m\to\{0,1\}^{2n}$, 其结构如图 1 所示, 即:

$$F^{\pi}(x)=(CF_n^m(x),CF_n^m(\pi(x))),$$

其中, CF_n^m 是从 $\{0,1\}^m$ 到 $\{0,1\}^n$ 的压缩函数, π 是在 $\{0,1\}^m$ 上的非密码学的置换 (non-cryptographic permutation). Nandi[18]指出, 如果置换 π 存在大量不动点 (即当 $x\in\{0,1\}^m$ 时, 有 $\pi(x)=x$), 该结构会受到生日攻击, 进而发现碰撞. 由于没有不动点的置换很常见 (如第 2.2 节所示), 因此构建此结构时应选择没有不动点的置换 π. Nandi[18]随后证明, 如果 CF_n^m 是一个随机谕言机且 π 没有不动点, 则该结构具有最优的 $\Omega(2^n)$ 的抗碰撞性.

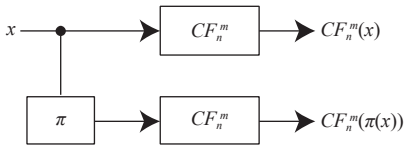

图 1 基于随机谕言机 CF_n^m 的 Nandi 之双分组哈希结构

如同 Nandi[18]的工作, 许多工作[9,11,13,14,17,19−26]在随机谕言机模型或者理想密码模型中证明了对应结构能够实现超 $n/2$ 比特的抗碰撞性. 总之, 已有多个双分组压缩函数被证明可以达到最优的抗碰撞性, 而 Merkle-Damgård 结构[1,2]能将哈希函数的抗碰撞性归约到压缩函数的抗碰撞性, 因此使用 Merkle-Damgård 结构[1,2]将这些压缩函数扩展后, 可以构造出具有最佳抗碰撞性的双分组哈希函数.

近几十年来, 量子计算取得了显著进展. 经典的哈希结构的具体安全边界在量子条件下因为 Grover 算法[27]与 BHT 算法[28]而显著降低. 具体而言, 对于 n 比特的压缩函数 $CF_n^m\colon \{0,1\}^m\to\{0,1\}^n$, BHT 算法[28]可以在 $O(2^{n/3})$ 量子步骤内发现碰撞 $CF_n^m(x)=CF_n^m(x')$, 这远低于经典条件下的复杂度 $O(2^{n/2})$. 此外, Simon 算法[29]的提出也使许多结构复杂的对称密钥密码系统[30,31]被破解. 因此, 需要重新评估原有结构在量子环境下的安全性.

Hirose 等人[32]针对 Nandi 之双分组哈希结构的工作填补了这一空白. 他们证明, 当置换 π 没有固定点且满足一定条件时, 该结构具有最优的 $\Omega(2^{2n/3})$ 量子抗碰撞安全性. 此外, 当置换 π 是对合时, 他们提出了对该结构 $O(2^{n/2})$ 量子步骤的碰撞攻击.

然而, 抗碰撞性在量子条件下对于许多应用并不足够[33,34]. 为了解决这一问题, Unruh[34]提出了哈希函数的坍塌性 (具体定义见第 2.4 节), 作为抗碰撞性的后量子替代品. 简言之, 坍塌性意味着在量子计算上无法区分测量量

子叠加的信息的哈希值与测量量子叠加的信息本身后的两个状态. 哈希函数的坍塌性已被公认为后量子安全的首要属性, 适用于存在回滚 (rewinding) 情况[35−38]与不存在回滚情况[39]. 坍塌性不仅是哈希函数的自然属性, 还是后量子承诺[34,40]、后量子签名底层的识别协议[41,42]和一般参数系统[38]的属性之一.

因此, 一个关键问题是, Nandi 之双分组哈希结构是否具有坍塌性? 特别地, 它是否具备最优的 $O(2^3/2^{2n})$ 坍塌性?

本文针对 Nandi 之双分组哈希结构 F^π 的坍塌性进行研究, 给出当 π 满足一定条件时, F^π 结构具有最优坍塌性的证明. 为此, 引入“仅包含 c-循环”的置换概念: 称 π 为“仅包含 c-循环”的, 若对于任意 $\{0,1\}^m$, $\pi^a(x)=x$ 当且仅当 $a=c$. 本文证明: 若使用这样的“仅包含 c-循环”的置换 π 且 $2<c\leqslant 2^{2n}$, 则 $F^\pi(x)=(CF(x),CF(\pi(x)))$ 具有 $O(2^3/2^{2n})$ 坍塌性. 此类仅包含 c-循环的置换 π 可通过简单的函数构造 (如第 2.2 节所示). 根据 Unruh 的工作[34]可知, 如果一个结构具有坍塌性, 该结构至少具有相同的抗碰撞性的安全界, 这意味着由仅包含 c-循环的 π 构建的 F^π 至少具有 $2n/3$ 比特的量子抗碰撞性, 这与前面提到的 Hirose 等人[32]的结论相匹配, 因而是紧致界. 本文的证明是对 Zhang 等人[43]的工作推广, 本文改进了原有的构造方法, 避免证明过程中压缩函数掩盖置换 π 的信息, 使得原有的证明过程可以推广到本文针对的结构.

结合本文结论与 Unruh 的工作[44], 进一步得到如果使用 Merkle-Damgård 结构对由仅包含 c-循环的 π 构建的 F^π 进行扩展, 且使用可以在多项式时间内计算的后缀码作为其填充函数时, 扩展后的哈希函数具有坍塌性.

结合本文结构与现有密码标准, 可以快速给出有较高坍塌性的新型哈希算法, 其可靠性与现有密码标准相当. 例如, 国密标准 SM3 的坍塌性约为 85.3 比特, 若将 SM3 的压缩函数代入本文结构, 则可构造摘要长度为 512 比特、坍塌性约为 170 比特的双分组哈希算法 (假设 SM3 压缩函数近似随机谕言机), 满足部分机要单位对量子安全性的要求.

本文第 2 节介绍符号和基本概念. 第 3 节给出由仅包含 c-循环的 π 构建的 F^π 结构的坍塌性证明. 最后, 在第 4 节进行总结.

2 基础知识

2.1 符号说明

对于非负整数 $n\in\mathbb{N}$, 用 $\{0,1\}^n$ 表示所有长度为 n 的由 0,1 组成的字符串构成的集合, 用 $[n]$ 表示集合 $\{0,1,\ldots,n-1\}$, 用 $(\{0,1\}^n)^*$ 表示所有长度是 n 的倍数的由 0,1 组成的字符串构成的集合. 对任意集合 $\mathcal{X}$ 和 $\mathcal{Y}$, 用 $Func(\mathcal{X},\mathcal{Y})$ 表示所有从 $\mathcal{X}$ 到 $\mathcal{Y}$ 的函数构成的集合. 对于两个比特字符串 x,y, 用 $x\|y$ 表示 x 和 y 的级联, 用 $x\oplus y$ 表示 x 和 y 按位的异或值. 如果 $x=x_1\|x_2$, 其中 $x\in\{0,1\}^{2n}, x_1,x_2\in\{0,1\}^n$, 令 $x_{\text{left}}=x_1$, $x_{\text{right}}=x_2$. 用 $x\leftarrow A$ 表示 x 被算法 A 输出的结果赋值. 对任意集合 $\mathcal{X}$, 用 $x\xleftarrow{\$}\mathcal{X}$ 表示从 $\mathcal{X}$ 中均匀随机选取成员, 并令 x 等于选出的成员. 对任意分布 D, 用 $f\leftarrow D$ 表示根据分布 D 采样 (sample), 并令 f 等于采样结果. 用 $domf$ 表示函数 f 的定义域. 用 $ranf$ 表示函数 f 的值域.

2.2 基于随机谕言机的 Nandi 之双分组哈希结构

基于随机谕言机的 Nandi 之双分组哈希结构如图 1 所示, 用 CF_n^m 表示从 $\{0,1\}^m$ 到 $\{0,1\}^n$ 的随机函数, 用 π 表示在 $\{0,1\}^m$ 上的非密码学的置换. 根据 Nandi[18]定义, 此类双分组哈希结构函数 $F^\pi(x)$ 定义为 $CF_n^m(x)\|CF_n^m(\pi(x))$. 因此, $F^\pi(x)_{\text{right}}=CF_n^m(\pi(x))=F^\pi(\pi(x))_{\text{left}}$. 本文聚焦于一类特殊结构, 即由仅包含 c-循环的 π 构建的双分组哈希结构. 事实上, 构建仅包含 c-循环的置换 π 可通过简单的函数实现, 例如:

$$\pi(x)=\begin{cases}x+1, & \text{如果}(x+1)\text{不是}c\text{的倍数}\\ x+1-c, & \text{如果}(x+1)\text{是}c\text{的倍数}\end{cases}.$$

因此, 在构造此类置换 π 时, 只需先将定义域中的元素按 c 个一组进行分组, 再定义每个分组内的映射关系即可. 显然, 当双分组哈希构由仅包含 c-循环的 π 构建时, 其定义域的元素个数等于 c 的倍数, 为了简化证明且不失一般性, 下文假设 $c=2^i$ ($i\in\mathbb{N}$, $i\geqslant 2$), 且置换 π 按照本节所述的方式定义.

2.3 量子计算

为了引入坍塌哈希函数的概念, 本节将介绍一些量子计算的背景知识. 我们假设读者对量子计算的基础符号有所了解 (参见文献 [45]). 一个量子系统 Q 由经典条件下有限集合 B 定义, 为便于理解, 本节将考虑特定的集合 $B=\{0,1\}^{n_B}$. 量子系统 Q 上的纯态是 $\mathbb{N}^{|B|}$ 空间中的一个单位向量, 其向量上的每个元素代表集合 B 中相应元素的系数值. 即, 令 $|\phi\rangle$ 为 Q 上的一个纯态, 则 $|\phi\rangle$ 可表示为:

$$|\phi\rangle=\sum_{x\in B}\alpha_x|x\rangle,$$

其中, $\sum_{x\in B}|\alpha_x|^2=1$. 集合 $\{|x\rangle\}_{x\in B}$ 构成 $\mathbb{C}^{|B|}$ 空间的一组计算基. 同时也是 $\mathbb{C}^{|B|}$ 空间的标准正交基. 对于两个状态 $|\phi_1\rangle$ 和 $|\phi_2\rangle$, 用 $|\phi_1\rangle\otimes|\phi_2\rangle$ 表示它们的张量积. 为简单起见, 在上下文明确时, 该符号简写为 $|\phi_1\rangle$, $|\phi_2\rangle$. 纯态 $|\phi\rangle\in Q$ 经由酉算子 U 变换后的新状态表示为 $|\phi'\rangle=U|\phi\rangle$. 本文假设量子计算机能够实现任意酉算子变换.

通过测量操作可以从状态 $|\phi\rangle$ 中提取信息. 测量操作需要指定一个标准正交基, 这通常是计算基. 测量结果 x 出现的概率为 $|\langle x|\phi\rangle|^2$. 一旦获得测量结果 x, 原状态 $|\phi\rangle$ 将“坍塌”到状态 $|x\rangle$.

2.4 坍塌哈希函数

本节讨论哈希函数 $H_m\colon(\{0,1\}^m)^*\to\{0,1\}^n$. 不失一般性, 本节假设函数 H_m 为压缩函数, 即 $|(\{0,1\}^m)^*|>|\{0,1\}^n|$. 令 $Eval(x)$ 表示计算哈希函数 $H_m(x)$ 并返回哈希值 $y=H_m(x)$ 的算法. 坍塌哈希函数定义如下.

定义 1. 坍塌哈希函数[34,35]. 对于一个哈希函数 $H_m\colon(\{0,1\}^m)^*\to\{0,1\}^n$, 如果存在一对有效的量子算法 $Eval$, 在以下实验 $Exp_H(A)$ 中能抵抗任何有效的量子敌手 A 的攻击, 那么这个哈希函数是可量子计算的坍缩哈希函数, 即该哈希函数具有坍塌性.

(1) 将敌手 A 在这个实验中分成两个阶段 A_0 和 A_1.

(2) 令 η 表示安全参数, A_0 在 η 的多项式时间内生成状态:

$$|\phi\rangle\colon=\sum_{x,y}\alpha_{x,y,z}|x,y,z\rangle,$$

其中, $x\in(\{0,1\}^m)^*$ 和 $y\in\{0,1\}^n$ 分别表示哈希函数 $H_m(x)$ 的输入和输出值, z 为辅助字符串. 然后, A_0 将包含哈希函数 $H_m(x)$ 输入输出值的寄存器发送给挑战者.

(3) 挑战者随机选择值 $b\leftarrow\{0,1\}$. 若 $b=0$, 挑战者在计算基上测量其接收状态的输出寄存器; 若 $b=1$, 则测量输入寄存器.

(4) 挑战者将寄存器 $|\phi\rangle$ 测量后的状态返回给敌手 A_1.

(5) 第 2 阶段敌手 A_1 从挑战者接收测量后的状态并从 A_0 继承信息之后, 经过量子多项式时间的计算, 输出它的决策 $b'\to\{0,1\}$. 当且仅当 $b'=b$ 时, 敌手赢得游戏.

敌手获胜时, 实验结果记作 $Exp_H(A)=1$, 否则记作 $Exp_H(A)=0$. 若 H_m 是坍塌哈希函数, 即具有坍塌性时, 应满足:

$$|\Pr[Exp_H(A)=1]-\frac{1}{2}|\leqslant negl(\eta).$$

上式对任何高效的量子敌手 A 都成立. 此处 $negl(\eta)$ 表示有关安全参数 η 的一个可忽略函数.

根据文献 [46], 挑战者在实验中可以通过再次调用 H_m 来验证 $|\phi\rangle$ 的有效性. 不失一般性, 假设 A_0 始终返回有效的状态, 即输出寄存器正确存储了对应输入的正确哈希值. 这使得本文无需再讨论如 Unruh[34]提出的关于能否总是存储正确哈希值的问题. 对于单射函数, 其定义域中的每个元素经映射后各不相同. 因此, 无论挑战者测量哪个寄存器, 输入输出寄存器都会坍塌至仅存储观测值及其对应的函数值的状态, 这表明单射函数具有坍塌性. 进一步地, 置换同样具有坍塌性.

Zhandry[47]设计了以下游戏以直观地解释坍塌性的概念.

敌手向挑战者发送一个哈希值 y, 挑战者随后随机选择一个比特 b, 如果敌手能生成一个 y 的原像 x, 使得 x 的首位为 b, 则敌手赢得此游戏. 显然, 敌手可以先任意选取任意 x 并计算其哈希值 y, 再将 y 发送给挑战者, 此时 x 的

首位是 b 的概率为 $1/2$. 那么就有一个问题, 敌手能否提高胜率?

若该哈希函数具有抗碰撞性, 在经典条件下, 敌手无法做得更好. 否则, 假设对于给定的 y, 敌手能以 $1/2+\epsilon$ 的概率获胜, 那么无论 $b=0$ 还是 $b=1$, 敌手的获胜概率都至少为 ϵ. 具体而言, 可以在 $b=0$ 的条件下令敌手进行游戏, 然后进行回滚操作, 直到敌手刚发送 y 时, 改为在 $b=1$ 的条件下继续游戏. 因此, 在所构建的碰撞中, 得到了首位分别为 0 和 1 的 y 的原像 x_0 和 x_1, 其概率不低于 ϵ^2.

然而, 在量子条件下, 上述策略不再有效. 首次游戏中对 x_0 的测量可能破坏敌手的状态, 使敌手无法保证产生 x_1. Ambainis 等人[33]提供了一个反例, 展示了在这种情况下获得 x_1 的概率变得可忽略不计.

Unruh[34]引入了坍塌哈希函数的概念, 解决了这一问题. 基本上, 敌手的第 1 条信息 y 会导致哈希函数的输出寄存器被测量. 根据坍塌性的定义, 此操作与测量输入寄存器无法区分, 即等同于提取 x_0. 虽然这种提取可能会改变量子状态, 但无法被探测. 因此, 第 2 次运行产生 x_1 会仍然成功, 进而发现碰撞. 如 Unruh 所解释, 坍塌性隐含着抗碰撞性, 因此敌手只能以概率 $1/2+negl()$ 赢得比赛.

此外, Unruh[34]还证明了随机谕言机具有 $\mathrm{O}(q^3/2^n)$ 的坍塌性 (该证明框架在文献 [48] 得到更正). Unruh 基于 Zhandry[49]的工作证明当随机谕言机的值域与定义域均为 n 比特时, 任意敌手在对随机谕言机进行 q 次量子查询后, 区分随机谕言机和随机置换的优势为 $\mathrm{O}(q^3/2^n)$. 因为随机置换具有坍塌性, 所以此类随机谕言机具有 $\mathrm{O}(q^3/2^n)$ 的坍塌性. 针对定义域大于值域的随机谕言机, Unruh 构造了一类新的随机函数, 其定义域小于值域, 并证明其与原随机谕言机及相应随机置换之间的不可区分性, 最终证明所有的随机谕言机都具有 $\mathrm{O}(q^3/2^n)$ 坍塌性.

3 由仅包含 c-循环的 π 构建的 F^π 结构的坍塌性证明

为便于阅读, 先回顾基于随机谕言机 CF_n^m 的 Nandi 之双分组哈希结构 F^π 的定义如下. 用 CF_n^m 表示从 $\{0,1\}^m$ 到 $\{0,1\}^n$ 的随机函数, 用 π 表示在 $\{0,1\}^m$ 上的非密码学的置换. 此类双分组哈希结构函数 $F^\pi(x)$ 定义为 $CF_n^m(x)\|CF_n^m(\pi(x))$. 本节考虑由仅包含 c-循环的 π 构建的双分组哈希结构.

本文主要结论为该结构的坍塌性, 如下.

定理 1. 对于基于随机谕言机 CF_n^m 的 Nandi 之双分组哈希结构 F^π, 令 q 为敌手对 F^π 结构的量子查询次数, 当 F^π 是由仅包含 c-循环的 π 构建时, F^π 具有 $\mathrm{O}(q^3/2^{2n})$ 的坍塌性.

本节以下为定理 1 的证明 (如前文第 2.2 节所述, 本节假设 $c=2^i\ (i\in\mathbb{N}, i\geqslant 2)$).

为便于理解, 本节首先概述证明思路. 本节根据文献 [49] 提供的思路, 首先对任意能被 c 整除的参数 r, 定义一个分布 D_r, 进而定义一个基于 D_r 分布采样的函数 $G_2\circ G_1$. 随后, 证明 $G_2\circ G_1$ 和一个置换 P 不可区分, 这允许定义一个值域大于定义域的特殊函数 F^π. 根据文献 [48], 可证明特殊函数 F^π 具有坍塌性. 再结合文献 [48] 结果, 推导 $F^\pi\circ G_2\circ G_1$ 具有坍塌性. 由于 $F^\pi\circ G_2\circ G_1$ 和 $F^\pi\circ P$ 不可区分, 得出 $F^\pi\circ P$ 具有坍塌性. 最后, 由于 $F^\pi\circ P$ 和 F^π 具有相同的分布, 因此 F^π 具有坍塌性.

首先, 根据文献 [48,49], 本文定义 D_r 分布如下. 设 r 为能被 c 整除的正整数, N 为任意正整数. 定义从 $\{0,1\}^N$ 到 $\{0,1\}^N$ 的函数的 D_r 分布, 该分布根据如下步骤采样:

(1) 选择一个随机函数 $g:\{0,1\}^N\to[r]$, g 满足对任意 $x,y\in\{0,1\}^N$, 若 $y=\pi^a(x)$, 则存在一个 $k\in\{0,1,\ldots,r/c-1\}$, 使得 $g(y)$, $g(x)\in\{kc+0,kc+1,\ldots,kc+c-1\}$, 且 $(g(y)-g(x))\equiv a \bmod c$. 即当 x 通过若干次 π 置换变换为 y 时, x、y 经由 g 函数变换后的值落在相同的某个随机值 $k\in\{0,1,\ldots,r/c-1\}$ 表示的集合 $\{kc+0,kc+1,\ldots,kc+c-1\}$ 范围内, 从而保留 x、y 在原函数 π 中的关系信息.

(2) 设 $S=\{g(x)\colon x\in\{0,1\}^N\}$. 即 S 是函数 g 的值域.

(3) 选择一个随机单射函数 $h\colon S\to\{0,1\}^N$, h 满足对任意 $x,y\in\{kc+0,kc+1,\ldots,kc+c-1\}\ (k\in[r/c])$, 若 $x>y$, 则有 $h(x)=\pi^{(x-y)}(h(y))$, 即函数 h 将集合 S 中每一组保留 π 函数关系信息的值随机映射到 $\{0,1\}^N$ 上, 并保留这些值之间的对应关系.

(4) 输出函数 $f=h\circ g$.

根据文献 [48], 需证明文献 [49] 中的以下引理对于本文定义的 D_r 分布同样适用.

引理 1. 给定 k 对值 (x_i, r_i), 设 $p(r) = \Pr_{f \leftarrow D_r}[f(x_i) = r_i, \forall i \in \{1,2,\ldots,k\}]$. 那么, p 是 $1/r$ 的多项式函数, 其次数不超过 $k-1$.

证明: 本引理与文献 [49] 第 3.1 节的一个引理很类似, 但所研究的分布有差异: 文献 [49] 第 3.1 节的分布是针对随机函数, 而我们的分布是针对本文的 F^{π} 结构, 因此我们将它的证明做了针对性的修改, 呈递如下. 根据 D_r 分布的定义, 当 $k=1$ 时, 对于任意的 $(x_0, r_0) \in (\{0,1\}^N)^2$, 有 $p(r) = \Pr_{f \leftarrow D_r}[f(x_0) = r_0] = 1/2^N$. 因此, 此引理在 $k=1$ 时成立. 现假设对于所有 $k' < k$, 此引理均成立.

不失一般性, 可假设对于任意的 i, j, 都不存在一个 $a \in \{1,2,\ldots,c\}$, 使得 $\pi^a(x_i) = x_j$. 若存在这样的 a, 应有以下情况:

- 若 $x_i = x_j$ 且 $r_i = r_j$, 则可以删除多余数据对 (x_j, r_j).
- 若 $x_i = \pi^a(x_j)$ 且 $r_i = \pi^a(r_j)$ $(a \in \{1,2,\ldots,c-1\})$, 根据函数的定义, 也可以删除多余数据对 (x_j, r_j).
- 若 $x_i = x_j$ 且 $r_i \neq r_j$, 则有 $p(r) = 0$.
- 若 $x_i = \pi^a(x_j)$ 且 $r_i \neq \pi^a(r_j)$ $(a \in \{1,2,\ldots,c-1\})$, 则有 $p(r) = 0$.

用 $l = |r_i : i \leqslant k-1|$ 表示在不包括 r_k 的情况下, 满足上述假设的 r_i 的数量. 根据引理 1 与假设, 概率

$$p'(r) = \Pr_{f \leftarrow D_r}[f(x_i) = r_i, \forall i \in \{1,2,\ldots,k-1\}],$$

是关于 $1/r$ 的多项式函数, 其次数不超过 $k-2$. 考虑以下条件概率:

$$p(r) = \Pr_{f \leftarrow D_r}[f(x_k) = r_k \mid f(x_i) = r_i, \forall i \in \{1,2,\ldots,k-1\}].$$

假设对于某些 $i < k$, 存在 $r_k = r_i$. 这种情况仅当 $g(x_k) = g(x_i)$ 时发生, 其概率为 $1/r$. 假设对于某些 $i < k$, 存在 $r_k = \pi^a(r_i)$ $(a \in \{1,2,\ldots,c-1\})$, 这种情况仅当 $g(x_k) - g(x_i) \equiv a \bmod c$ 且存在对应的 $j \in \{0,1,\ldots,r/c-1\}$ 使得 $g(x_k), g(x_i) \in \{jc+0, jc+1, \ldots, jc+c-1\}$ 时发生, 其概率同样为 $1/r$. 现假设对于任何 $i < k$ 与 $a \in \{1,2,\ldots,c-1\}$, 均有 $r_k \neq r_i$ 且 $r_k \neq \pi^a(r_i)$. 即对于所有 $i < k$, 函数值 $g(x_k)$ 与 $g(x_i)$ 不会落在相同的由某个 $j \in \{0,1,\ldots,r/c-1\}$ 表示的区间 $\{jc+0, jc+1, \ldots, jc+c-1\}$ 内, 其概率为 $1-cl/r$. 这种情况下, $h(g(x_k)) = r_k$ 的概率为 $1/(2^N - cl)$. 因此, $f(x_k) = r_k$ 的概率是 $\dfrac{(1-cl/r)}{2^N - cl}$.

综上所述, 值

$$p(r) = \Pr_{f \leftarrow D_r}[f(x_k) = r_k \mid f(x_i) = r_i, \forall i \in \{1,2,\ldots,k-1\}],$$

是关于 $1/r$ 的多项式函数, 其次数为 1. 结合 $p'(r)$ 的结果, 可以得出 $p(r)$ 是关于 $1/r$ 的多项式函数, 其次数不超过 $k-1$.

注意到, 上述证明和定义的函数 f 的陪域和定义域无关, 因此在证明过程中只需关注这两个域的一致性, 而无需考虑它们的具体大小.

根据文献 [49] 第 3.1 节, 任意量子算法对分布采样的结构进行 q 次量子查询后, 只能以 $O(q^3/r)$ 的概率区分 D_r 和 D_{∞} 分布.

基于引理 1, 定义随机函数 $G_2 \circ G_1 : \{0,1\}^m \to \{0,1\}^m$, 该函数根据 $D_{2^{2n}}$ 分布采样获得 (即令 $r = 2^{2n}$, G_1 为 $D_{2^{2n}}$ 分布定义中选取的随机函数 g, G_2 为 $D_{2^{2n}}$ 分布定义中选取的随机函数 h). 另设 $P : \{0,1\}^m \to \{0,1\}^m$ 为一个随机置换, 其满足对于所有的 $x, y \in \{0,1\}^m$ 与 $a \in \{1,2,\ldots,c\}$, 若 $y = \pi^a(x)$, 则有 $P(y) = \pi^a(P(x))$. 此时, P 服从 D_{∞} 分布. 根据文献 [49] 第 3.1 节, $G_2 \circ G_1$ 和 P 是 $O(q^3/2^{2n})$ 不可区分的. 由于 P 是一个置换, 因此 P 具有坍塌性, 从而 $G_2 \circ G_1$ 具有 $O(q^3/2^{2n})$ 的坍塌性. 注意到, $G_2 \circ G_1$ 的值域小于等于 2^{2n}, 即 $|ranG_2 \circ G_1| \leqslant 2^{2n}$ (如第 2.1 节所述, $ranG_2 \circ G_1$ 表示函数 $G_2 \circ G_1$ 的值域).

基于上述证明可以定义特殊的函数 $F^{\pi}|_{ranG_2 \circ G_1} : ranG_2 \circ G_1 \to \{0,1\}^{2n}$, 其表达式为 $F^{\pi}|_{ranG_2 \circ G_1}(x) = f(x) \| f(\pi(x))$. 其与 F^{π} 的区别仅在于其定义域为函数 $G_2 \circ G_1$ 的值域. 对于任意的 G_1, G_2 有 $|domF^{\pi}|_{ranG_2 \circ G_1}| \leqslant 2^{2n}$.

根据文献 [48] 思路, 应构造一个与 F^{π} 对应的置换 $\hat{G}_3$, 并在该函数后添加一个随机函数, 以确保组合后的函数与 F^{π} 具有相同的分布. 然而, 对于结构 $F^{\pi}(x)=CF_n^m(x)\|CF_n^m(\pi(x))$, 其压缩函数 CF_n^m 掩盖了 x 与 $\pi(x)$ 之间的关系信息, 因此不能直接应用原有的构造方法. 本文选择在置换 $\hat{G}_3$ 之前构造所需的函数, 并再次利用文献 [49] 第 3.1 节提出的性质来解决这一问题.

定义随机函数 $G_3''\circ G_3'$: $ranG_2\circ G_1\to ranG_2\circ G_1$, 该函数根据 $D_{2^{2n}}$ 分布采样获得 (其中 G_3' 为 $D_{2^{2n}}$ 分布定义中选取的随机函数 g, G_3'' 为 $D_{2^{2n}}$ 分布定义中选取的随机函数 h), 定义随机置换 $\hat{G}_3'$: $ranG_2\circ G_1\to ranG_2\circ G_1$, 该置换根据 D_{∞} 分布采样获得. 根据文献 [49] 第 3.1 节, 可以得到 $G_3''\circ G_3'$ 和 $\hat{G}_3'$ 是 $O(q^3/2^{2n})$ 不可区分的. 设 $\hat{G}_3$: $ranG_2\circ G_1\to ranG_2\circ G_1$ 为一个随机单射, 并满足 $\hat{G}_3(x)_{\text{right}}=\hat{G}_3(\pi(x))_{\text{left}}$. 因此, $\hat{G}_3\circ G_3''\circ G_3'$ 和 $F^{\pi}(x)|_{ranG_2\circ G_1}$ 服从相同的分布函数, $\hat{G}_3\circ\hat{G}_3'$ 和 $\hat{G}_3$ 服从相同的分布函数. 由于 $G_3''\circ G_3'$ 和 $\hat{G}_3'$ 是 $\mathrm{O}(q^3/2^{2n})$ 不可区分的, 因此 $F^{\pi}(x)|_{ranG_2\circ G_1}$ 和 $\hat{G}_3$ 是 $\mathrm{O}(q^3/2^{2n})$ 不可区分的. 因为 $\hat{G}_3$ 是单射, 所以 $\hat{G}_3$ 具有坍塌性, 进而得出对于任意随机的 G_1,G_2, $F^{\pi}(x)|_{ranG_2\circ G_1}$ 具有 $\mathrm{O}(q^3/2^{2n})$ 的坍塌性.

根据文献 [48], 由于 $F^{\pi}(x)|_{ranG_2\circ G_1}$ 和 $G_2\circ G_1$ 都具有 $\mathrm{O}(q^3/2^{2n})$ 的坍塌性, $F^{\pi}(x)\circ G_2\circ G_1=F^{\pi}(x)|_{ranG_2\circ G_1}\circ G_2\circ G_1$ 具有 $\mathrm{O}(q^3/2^{2n})+\mathrm{O}(q^3/2^{2n})=\mathrm{O}(q^3/2^{2n})$ 的坍塌性. 因为 $G_2\circ G_1$ 和 P 是 $\mathrm{O}(q^3/2^{2n})$ 不可区分的, 所以 $F^{\pi}(x)\circ G_2\circ G_1$ 和 $F^{\pi}(x)\circ P$ 是 $\mathrm{O}(q^3/2^{2n})$ 不可区分的. 又因为 $F^{\pi}(x)\circ P$ 和 $F^{\pi}(x)$ 具有相同的分布, 所以 $F^{\pi}(x)$ 具有 $\mathrm{O}(q^3/2^{2n})$ 的坍塌性. 故定理 1 成立.

4 总结和讨论

本文针对 Nandi 之双分组哈希结构, 研究其结构在量子条件下的坍塌性. 基于文献 [48] 的思路, 本文研究了由仅包含 c-循环的 π 构造的 Nandi 之双分组哈希结构, 并给出相应的置换构造方法. 证明当 F^{π} 是由仅包含 c-循环的 π 构造且 $2^{2n}\geqslant c>2$ 时, F^{π} 是 $\mathrm{O}(q^3/2^{2n})$ 坍塌的. 这同时意味着由仅包含 c-循环的 π 构建的 F^{π} 上的 $2n/3$ 比特的量子抗碰撞性, 该结论与 Hirose 等人[32]的结论一致, 进一步说明本文所证明的安全界是紧的. 本文的结论也说明, 如果使用 Merkle-Damgård 结构对由仅包含 c-循环的 π 构建的 F^{π} 进行扩展, 且使用可以在多项式时间内计算的后缀码作为其填充函数, 则扩展后的哈希函数是坍塌的.

本文同时发现, 在 Nandi 之双分组哈希结构在没有固定点且非由仅包含 c-循环的 π 构建的情况下, 难以利用 Zhandry[49]的结论将该结构的原始输入携带置换 π 的信息压缩, 致使难以压缩该函数的定义域, 本文并未给出该情况下结构整体的坍塌性, 且同样由于置换 π 的信息过于复杂, 使用 Zhandry[50]的压缩谕言机技术来证明该情况下是否具有最优的量子抗碰撞性也是一个开放性问题. 因此值得考虑的后续工作包括对于任何置换 π 非对合且没有固定的点的 Nandi 之双分组哈希结构是否仍然具有同样的安全性, 或在理想密码模型中该结论是否仍然适用等.

References

[1] Damgård IB. A design principle for hash functions. In: Brassard G, ed. Advances in Cryptology—CRYPTO 1989. New York: Springer, 1989. 416–427. [doi: 10.1007/0-387-34805-0_39]

[2] Merkle RC. One way hash functions and DES. In: Brassard G, ed. Advances in Cryptology—CRYPTO 1989. New York: Springer, 1989. 428–446. [doi: 10.1007/0-387-34805-0_40]

[3] Davies DW, Price WL. Digital signature—An update. In: Proc. of the 7th Int'l Conf. on Computer Communications. Sydney: Elsevier, 1984.

[4] Linn J. RFC1115: Privacy enhancement for Internet electronic mail: Part III—Algorithms, modes, and identifiers. 1989. https://www.rfc-editor.org/info/rfc1115/ [doi: 10.17487/RFC1115]

[5] Rivest RL. RFC1186: MD4 message digest algorithm. 1990. https://www.rfc-editor.org/info/rfc1186/ [doi: 10.17487/RFC1186]

[6] Rivest R. RFC1321: The MD5 message-digest algorithm. 1992. https://www.rfc-editor.org/info/rfc1321/ [doi: 10.17487/RFC1321]

[7] Standard SH. FIPS Pub 180-1. National Institute of Standards and Technology, 1995, 17(180): 15.

[8] Standard SH. Federal information processing standards (FIPS) Publication FIPS-180-2. 2002. https://www.nist.gov/itl/csd/cybersecurity-%2526-privacy-publications%252C-standards-%2526-guidelines/federal-information

[9] Lai X, Massey JL. Hash functions based on block ciphers. In: Rueppel RA, ed. Advances in Cryptology—EUROCRYPT 1992. Berlin: Springer, 1992. 55–70. [doi: 10.1007/3-540-47555-9_5]

[10] Armknecht F, Fleischmann E, Krause M, Lee J, Stam M, Steinberger J. The preimage security of double-block-length compression

functions. In: Proc. of the 17th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Seoul: Springer, 2011. 233–251. [doi: 10.1007/978-3-642-25385-0_13]

[11] Lee J, Stam M, Steinberger J. The collision security of Tandem-DM in the ideal cipher model. In: Proc. of the 31st Annual Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2011. 561–577. [doi: 10.1007/978-3-642-22792-9_32]

[12] Naito Y. Optimally indifferentiable double-block-length hashing without post-processing and with support for longer key than single block. In: Proc. of the 6th Int'l Conf. on Cryptology and Information Security in Latin America on Progress in Cryptology. Santiago de Chile: Springer, 2019. 65–85. [doi: 10.1007/978-3-030-30530-7_4]

[13] Lee J, Stam M. MJH: A faster alternative to MDC-2. In: Kiayias A, ed. Topics in Cryptology—CT-RSA 2011. Berlin, Heidelberg: Springer, 2011. 213–236. [doi: 10.1007/978-3-642-19074-2_15]

[14] Mennink B. Optimal collision security in double block length hashing with single length key. In: Proc. of the 18th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Beijing: Springer, 2012. 526–543. [doi: 10.1007/978-3-642-34961-4_32]

[15] Naito Y. Indifferentiability of double-block-length hash function without feed-forward operations. In: Proc. of the 22nd Australasian Conf. on Information Security and Privacy. Auckland: Springer, 2017. 38–57. [doi: 10.1007/978-3-319-59870-3_3]

[16] Naito Y, Sasaki Y, Sugawara T. Double-block-length hash function for minimum memory size. In: Proc. of the 27th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Singapore: Springer, 2021. 376–406. [doi: 10.1007/978-3-030-92078-4_13]

[17] Özen O, Stam M. Another glance at double-length hashing. In: Proc. of the 12th IMA Int'l Conf. on Cryptography and Coding. Cirencester: Springer, 2009. 176–201. [doi: 10.1007/978-3-642-10868-6_11]

[18] Nandi M. Towards optimal double-length hash functions. In: Proc. of the 6th Int'l Conf. on Progress in Cryptology. Bangalore: Springer, 2005. 77–89. [doi: 10.1007/11596219_7]

[19] Fleischmann E, Forler C, Gorski M, Lucks S. Collision resistant double-length hashing. In: Proc. of the 4th Int'l Conf. on Provable Security. Malacca: Springer, 2010. 102–118. [doi: 10.1007/978-3-642-16280-0_7]

[20] Fleischmann E, Forler C, Lucks S, Wenzel J. Weimar-DM: A highly secure double-length compression function. In: Proc. of the 17th Australasian Conf. on Information Security and Privacy. Wollongong: Springer, 2012. 152–165. [doi: 10.1007/978-3-642-31448-3_12]

[21] Hirose S. Provably secure double-block-length hash functions in a black-box model. In: Proc. of the 7th Int'l Conf. on Information Security and Cryptology. Seoul: Springer, 2005. 330–342. [doi: 10.1007/11496618_24]

[22] Hirose S. Some plausible constructions of double-block-length hash functions. In: Proc. of the 13th Int'l Workshop on Fast Software Encryption. Graz: Springer, 2006. 210–225. [doi: 10.1007/11799313_14]

[23] Lee J, Kwon D. The security of Abreast-DM in the ideal cipher model. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94. A(1): 104–109. [doi: 10.1587/transfun.E94.A.104]

[24] Nageler M, Pallua F, Eichlseder M. Finding collisions for round-reduced romulus-H. IACR Trans. on Symmetric Cryptology, 2023, 2023(1): 67–88. [doi: 10.46586/tosc.v2023.i1.67-88]

[25] Prencel B, Bosselaers A, Govaerts R, Vandewalle J. Collision-free hashfunctions based on blockcipher algorithms. In: Proc. of the 1989 Int'l Carnahan Conf. on Security Technology. Zurich: IEEE, 1989. 203–210. [doi: 10.1109/CCST.1989.751980]

[26] Steinberger JP. The collision intractability of MDC-2 in the ideal-cipher model. In: Proc. of the 26th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Barcelona: Springer, 2007. 34–51. [doi: 10.1007/978-3-540-72540-4_3]

[27] Grover LK. A fast quantum mechanical algorithm for database search. In: Proc. of the 28th Annual ACM Symp. on Theory of Computing. Philadelphia: Association for Computing Machinery, 1996. 212–219. [doi: 10.1145/237814.237866]

[28] Brassard G, Høyer P, Tapp A. Quantum cryptanalysis of hash and claw-free functions. In: Proc. of the 3rd Latin American Symp. on Theoretical Informatics. Campinas: Springer, 1998. 163–169. [doi: 10.1007/BFb0054319]

[29] Simon DR. On the power of quantum computation. SIAM Journal on Computing, 1997, 26(5): 1474–1483. [doi: 10.1137/S0097539796298637]

[30] Kaplan M, Leurent G, Leverrier A, Naya-Plasencia M. Breaking symmetric cryptosystems using quantum period finding. In: Proc. of the 36th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2016. 207–237. [doi: 10.1007/978-3-662-53008-5_8]

[31] Xu YS, Luo YY, Dong XY, Yuan Z. Low-data quantum key-recovery attack on block cipher structures. Ruan Jian Xue Bao/Journal of Software, 2025, 36(7): 3395–3412 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/7218.htm [doi: 10.13328/j.cnki.jos.007218]

[32] Hirose S, Kuwakado H. A note on quantum collision resistance of double-block-length compression functions. In: Proc. of the 18th IMA Int'l Conf. on Cryptography and Coding. Springer, 2021. 161–175. [doi: 10.1007/978-3-030-92641-0_8]

[33] Ambainis A, Rosmanis A, Unruh D. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In: Proc. of the

55th IEEE Annual Symp. on Foundations of Computer Science. Philadelphia: IEEE, 2014. 474–483. [doi: 10.1109/FOCS.2014.57]

[34] Unruh D. Computationally binding quantum commitments. In: Proc. of the 35th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Vienna: Springer, 2016. 497–527. [doi: 10.1007/978-3-662-49896-5_18]

[35] Chia NH, Chung KM, Yamakawa T. A black-box approach to post-quantum zero-knowledge in constant rounds. In: Proc. of the 41st Annual Int'l Cryptology Conf. on Advances in Cryptology. Springer, 2021. 315–345. [doi: 10.1007/978-3-030-84242-0_12]

[36] Chiesa A, Ma F, Spooner N, Zhandry M. Post-quantum succinct arguments: Breaking the quantum rewinding barrier. In: Proc. of the 62nd IEEE Annual Symp. on Foundations of Computer Science (FOCS 2022). Denver: IEEE, 2022. 49–58. [doi: 10.1109/FOCS52979.2021.00014]

[37] Lai RWF, Malavolta G, Spooner N. Quantum rewinding for many-round protocols. In: Proc. of the 20th Int'l Conf. on Theory of Cryptography. Chicago: Springer, 2022. 80–109. [doi: 10.1007/978-3-031-22318-1_4]

[38] Lombardi A, Ma F, Spooner N. Post-quantum zero knowledge, revisited or: How to do quantum rewinding undetectably. In: Proc. of the 63rd IEEE Annual Symp. on Foundations of Computer Science (FOCS 2022). Denver: IEEE, 2022. 851–859. [doi: 10.1109/FOCS54457.2022.00086]

[39] Alagic G, Majenz C, Russell A, Song F. Quantum-access-secure message authentication via blind-unforgeability. In: Proc. of the 39th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Zagreb: Springer, 2020. 788–817. [doi: 10.1007/978-3-030-45727-3_27]

[40] Dall'Agnol M, Spooner N. On the necessity of collapsing for post-quantum and quantum commitments. In: Proc. of the 18th Conf. on the Theory of Quantum Computation, Communication and Cryptography. Aveiro: Leibniz Int'l Proc. in Informatics, 2023. 2: 1–2: 23. [doi: 10.4230/LIPIcs.TQC.2023.2]

[41] Don J, Fehr S, Majenz C, Schaffner C. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In: Proc. of the 39th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2019. 356–383. [doi: 10.1007/978-3-030-26951-7_13]

[42] Liu QP, Zhandry M. Revisiting post-quantum Fiat-Shamir. In: Proc. of the 39th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2019. 326–355. [doi: 10.1007/978-3-030-26951-7_12]

[43] Zhang SX, Guo C, Wang QM. Towards quantum security of hirose compression function and romulus-H. In: Proc. of the 30th Australasian Conf. on Information Security and Privacy. Wollongong: Springer, 2025. 3–22. [doi: 10.1007/978-981-96-9098-5_1]

[44] Unruh D. Collapse-binding quantum commitments without random oracles. In: Proc. of the 22nd Int'l Conf. on the Theory and Application of Cryptology and Information Security. Hanoi: Springer, 2016. 166–195. [doi: 10.1007/978-3-662-53890-6_6]

[45] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2010. [doi: 10.1017/CBO9780511976667]

[46] Cao SJ, Xue R. The gap is sensitive to size of preimages: Collapsing property doesn't go beyond quantum collision-resistance for preimages bounded hash functions. In: Proc. of the 42nd Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2022. 564–595. [doi: 10.1007/978-3-031-15982-4_19]

[47] Zhandry M. New constructions of collapsing hashes. In: Proc. of the 42nd Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2022. 596–624. [doi: 10.1007/978-3-031-15982-4_20]

[48] Unruh D. Computationally binding quantum commitments. Cryptology ePrint Archive, 2015. https://eprint.iacr.org/2015/361

[49] Zhandry M. A note on the quantum collision and set equality problems. Quantum Information & Computation, 2015, 15(7–8): 557–567. [doi: 10.5555/2871411.2871413]

[50] Zhandry M. How to record quantum queries, and applications to quantum indifferentiability. In: Proc. of the 39th Annual Int'l Cryptology Conf. Advances in Cryptology. Santa Barbara: Springer, 2019. 239–268. [doi: 10.1007/978-3-030-26951-7_9]

附中文参考文献

[31] 许琨松, 罗宜元, 董晓阳, 袁征. 分组密码结构的低数据量子密钥恢复攻击. 软件学报, 2025, 36(7): 3321–3338. http://www.jos.org.cn/1000-9825/7218.htm [doi: 10.13328/j.cnki.jos.007218]

作者简介

张绍煊, 博士生, 主要研究领域为后量子对称密码算法的可证明安全性.

郭淳, 博士, 教授, 博士生导师, 主要研究领域为对称密码结构可证明安全性.