

基于合数剩余假设伪熵函数的优化

陈 浩¹, 靳方元¹, 朱艳琴^{1,2}

(1 苏州大学 计算机科学与技术学院, 江苏 苏州 215006;

2 苏州大学 江苏省计算机信息处理技术重点实验室, 江苏 苏州 215006)

摘 要: 2011 年 Braverman 等人在伪随机函数的概念上提出了自适应泄漏弹性的伪熵函数. 针对该方案抗泄漏量一定的问题, 文中对该方案进行改进, 基于合数剩余假设提出新的构建方案. 从证明结果可以看出, 新方案具有更高的抗泄漏量.

关键词: 自适应泄漏; 有损陷门函数; DDH 假设; 合数剩余假设

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2012)11-0157-04

An Improvement of Pseudo-Entropy Functions Based on Composite Residuosity Assumption

CHEN Hao¹, JIN Fang-yuan², ZHU Yan-qin^{1,2}

(1 School of Computer Science and Technology, Soochow University, Soochow 215006, China;

2. Computer Information Processing Technology, Soochow University, Soochow 215006, China)

Abstract: Braverman introduces pseudo-entropy functions based on pseudo-random functions in 2011. But the amount of leakage is not high enough, this paper we propose a new pseudo-entropy function based on composite residuosity assumption. From the proof, we can see that our new scheme can stand up more leakage.

Key words: adaptive leakage; lossy trapdoor function; DDH assumption; composite residuosity assumption

1 引言

传统密码系统安全依赖于密钥的完全隐私性. 然而在现实应用中, 这种假设难以得到严格的满足. 攻击者可通过时间攻击、内存攻击等方式^[1-4]获得加密系统的内部信息, 导致系统的私钥遭到泄漏. 因此, 构造在密钥存在泄漏情况下保证系统安全性的理论模型成为密码学的一个热点领域.

以往的泄漏弹性加密方案中, 设计者通常利用提取器确保种子的随机性或通过提取器隐藏私钥. 2011 年 Braverman 等人在伪随机函数的概念上提出了自适应泄漏弹性的伪熵函数^[5]. 伪熵函数不再强调种子的随机性, 种子是可以被泄漏的. 伪熵函数

构造主要利用的是 Peikert 和 Waters 提出的有损陷门函数. 从伪熵函数的构造过程中可以得出, 伪熵函数的有损度和其抗泄漏量是成正比的. Braverman 等人构建有损陷门函数利用的是 DDH 假设, 而基于该假设的有损陷门函数的有损度是一定的. 因此 Braverman 等人基于 DDH 假设的伪熵函数抗泄漏量是一定的, 无法提高伪熵函数的抗泄漏量. 针对该问题, 基于合数剩余假设, 本文提出一个抗泄漏量更高的伪熵函数.

2 基础理论

2.1 相关假设

定义 1 (DDH 假设): 对于一个有限群 G , 假

收稿日期: 2012-05-09; 修回日期: 2012-06-09

基金项目: 国家自然科学基金项目(61070170); 苏州市应用基础研究计划项目(SYJG09024); 苏州市融合通信重点实验室(SZS0805)

设其阶为 q , 生成元为 $g, a, b, c \in G$. DDH 假设是指, 给定攻击者 g^a, g^b , 攻击者区分 g^{ab}, g^c 的概率是可忽略的:

$$|Pr[A(g^a, g^b, g^{ab})=1] - Pr[A(g^a, g^b, g^c)=1]| = \text{negl}(\lambda)$$

定义 2 (合数剩余假设): 给定合数 n 及整数 z . 合数剩余假设指的是确定是否存在 y 使得 z 为 y 的 n 次剩余, 即 $z = y^n \bmod n^2$ 是困难的.

2.2 有损陷门函数

定义 3 (有损陷门函数): 对于函数族 $F = \{F_\lambda\}_{\lambda \in N}$, 若

(1) 存在两个种子生成函数 Gen_{loss} 和 Gen_{inj} , 使得

$$\textcircled{1} \{Gen_{loss}(1^\lambda)\} \approx \{Gen_{inj}(1^\lambda)\}_{\lambda \in N}$$

$\textcircled{2}$ 对于任意 $\lambda \in N$ 以及 $s \in Gen_{inj}(1^\lambda)$, 函数 $f_s: \{0, 1\}^n \rightarrow \{0, 1\}^*$ 是有损的, 假设函数的输出大小为 2^{n-w} .

(2) 存在一个概率多项式时间算法 $Eval$, 对于任意 $\lambda \in N, s \in Gen_{loss}(1^\lambda) \cup Gen_{inj}(1^\lambda)$ 及 $x \in \{0, 1\}^n$ 均有:

$$Eval(s, x) = f_s(x)$$

则称函数族 $F = \{F_\lambda\}_{\lambda \in N}$ 为有损度为 w 的有损陷门函数^[6].

2.3 伪熵函数定义及构造

伪熵函数^[5]定义有选择安全和自适应安全, 这里我们仅介绍自适应安全的伪熵函数.

定义 4 (自适应安全的伪熵函数): 对于函数族 $g = \{g_\lambda\}_{\lambda \in N}$, 具有如下性质:

(1) Gen 是以安全参数 1^λ 作为输入的概率多项式算法, 输出为 (pp, s) , 其中 pp 表示密钥的公开部分, 而 s 表示密钥秘密部分.

(2) 函数族 $g = \{g_\lambda\}_{\lambda \in N}$ 中的每个函数由密钥的公开部分 pp 和秘密部分 s 共同决定, 简记为 g_s .

(3) 存在一个概率多项式算法 Gen' , 对于每一个输入序列: $x = x(\lambda) \in \{0, 1\}^{k(\lambda)}$ 使得 $\{Gen'(1^\lambda, x)\}_{\lambda \in N} \approx \{Gen(1^\lambda)\}_{\lambda \in N}$; 攻击者向伪熵函数的 oracle 进行查询, 获得相关的信息后, 挑战者确定输入 $x, (pp, s) \leftarrow Gen'(1^\lambda, x), n = |s|$, 对于任意多项式时间的泄漏函数 L , 假设其输出为 $l(n)$ 有:

$$x = A^{g_s}(pp, L(pp, s))$$

$$\tilde{H}_\infty(g_s(x) | \dots, L(pp, s), \{g_s(x')\}_{x' \neq x}) \geq \beta(n)$$

那么称 $g = \{g_\lambda\}_{\lambda \in N}$ 是 l 泄漏 β 自适应安全伪熵函数.

本节我们给出伪熵函数的具体构造过程. 然后分别给出选择安全和自适应安全伪熵函数的参数化定义.

在伪熵函数的构造中, 约定秘密种子的长度为 n , 函数输入的长度为 k , 而输出的长度为 n , 并且 n 和 k 均依赖安全参数 λ , 其中 $k = n^\sigma, \sigma \in (0, 1)$ 远小于 n . 伪熵函数的构造利用的是有损度为 w 的有损陷门函数 $F = \{F_\lambda\}_{\lambda \in N}$. 其中的每一个有损陷门函数的输入输出长度均为 n . 设定有损度 $w = n - n^\epsilon, 0 < \epsilon < 1 - \sigma$, 对于 l 泄漏 β 自适应安全伪熵函数, 设定 $l = n - 2n^{\sigma+\epsilon}, \beta = n^{\sigma+\epsilon}$. 并且文献[3]已经证明如果有损陷门函数是 γ 计算提取器, 其中 $\gamma = n - n^{\sigma+\epsilon}$, 则构造的伪熵函数是伪随机函数. 伪熵函数的具体构造:

(1) Gen : 种子生成算法以安全参数 1^λ 作为输入, 利用 $Gen_{inj}(1^\lambda)$ 生成公共参数 pp : $2k$ 个单向函数:

$$pp = \begin{pmatrix} f_{1,0}, f_{2,0}, \dots, f_{k,0} \\ f_{1,1}, f_{2,1}, \dots, f_{k,1} \end{pmatrix}$$

以及一个秘密种子 $s \leftarrow \{0, 1\}^n$.

(2) $Eval$: $Eval$ 函数以公共参数 pp , 秘密种子 $s, x \in \{0, 1\}^k$ 作为输入, 记 $x = (x_1, \dots, x_k)$, 输出为:

$$g_s(x) = f_{1,x_1} \circ f_{2,x_2} \circ f_{3,x_3} \circ \dots \circ f_{k,x_k}(s)$$

其中 $g_s(x)$ 计算过程如下: 首先计算以种子 s 作为输入的函数值 f_{k,x_k} , 然后将 f_{k,x_k} 得输出作为 $f_{k-1,x_{k-1}}$ 的输入, 依此类推. 同时为了保证 f_{i,x_i} 的输出是 $f_{i-1,x_{i-1}}$ 的有效输入, 约定 f_{i,x_i} 的输出长度不能大于其输入的长度.

定理 1 上述定义的伪熵函数, 若其利用的有损陷门函数有损度为 w , 并且满足

$$w = n - n^\epsilon, k = n^\sigma, l = n - 2n^{\sigma+\epsilon}, \beta = n^{\sigma+\epsilon}$$

则该伪熵函数是 l 泄漏 β 选择安全的.

由定理可以看出, 若我们提高有损陷门函数的有损度将有:

$$w \uparrow \leftarrow n^\epsilon \downarrow \leftarrow \epsilon \downarrow \leftarrow n^{\sigma+\epsilon} \downarrow \leftarrow l \uparrow$$

伪熵函数的抗泄漏量也提升了, 即伪熵函数的抗泄漏量与有损陷门函数的有损度是成正比的.

3 伪熵函数的优化

Braverman 等人构建有损陷门函数利用的是 DDH 假设, 而基于 DDH 假设构造的有损陷门函数的有损度是一定的, 因此无法提高伪熵函数的抗泄漏量. 针对该问题, 我们对其进行改进, 利用合数剩余假设提出有损度更高的有损陷门函数, 从而提高伪熵函数的抗泄漏量.

3.1 基于 DDH 假设有损陷门函数的构造

本节,我们给出 Braverman 方案中基于 DDH 假设有损陷门函数的构建.

首先我们描述一个后面构造需要用的算法 $GenConceal(h, w)$, 其中 h, w 均是安全参数 λ 的概率多项式算法. 具体构造如下:

(1) 均匀随机选择 $r = (r_1, \dots, r_h) \leftarrow Z_p^h, s = (s_1, \dots, s_w) \in Z_p^w \times \{1\}$.

(2) 计算 $V = r \otimes s = r^t s \in Z_p^{h \times (w+1)}$ 为 s 与 r 的外积.

(3) 输出隐藏矩阵 $C = g^V \in G^{h \times (w+1)}$, 以及对应的陷门 s .

下面我们给出有损陷门函数基于 DDH 假设的具体构造过程:

(1) 生成单向和有损函数: 函数生成器调用群的生成元 g 生成 $G = (p, \langle G \rangle, g)$, 其中 p 是素数, $\langle G \rangle$ 表示阶为 p 的乘法循环群 G 的相关操作, g 表示 G 的生成元. 然后调用算法 $GenConceal(n, n)$ 生成隐藏矩阵 $C = g^V \in G^{n \times (n+1)}$ 以及对应的陷门 $s \in Z_p^{n+1}$. 单向函数 S_{inj} 输出函数索引 $g^Y = g^{V+I'}$, 其中 $I' \in Z_p^{n \times (n+1)}$ 为 $n \times n$ 的单位矩阵最后加上一个全零列, 单向函数的陷门为 s . 相应的, 有损函数输出函数索引 $C = g^V$.

(2) 评估算法: 有损后门函数 F_{ldf} 以 (g^Y, x) 作为输入, 其中 $g^Y \in G^{n \times (n+1)}$ 为函数索引, $x \in \{0, 1\}^n \subset Z_p^n$. 输出为 $z = g^{xY} \in G^{n+1}$.

(3) 求逆: 有损陷门逆函数 F_{ldf}^{-1} 以 (s, z) 作为输入, 其中 s 为陷门, z 表示有损陷门函数的输出. 求逆过程如下, 对于任意 $j \in [n]$, 计算 $a_j = z_j / z_{n+1}^s$, 其中 $a_j = g^{x_j}$, 从而计算出 x_j .

定理 2 在 DDH 假设下, 上述构造的有损陷门函数的有损度为 $w = n \log q - \log q$.

3.2 基于合数剩余假设有损陷门函数的构造

基于 DDH 假设有损陷门函数因为其有损度是一定的, 故不能提高伪熵函数的抗泄漏量. 因此我们基于合数剩余假设对其方案进行改进, 基于合数剩余假设构建的有损陷门函数理论上可以确保任意大小的有损度, 并且相对于 DDH 假设, 合数剩余假设构造的有损陷门函数更有效.

在我们方案的构造中, 每一个函数由函数描述符 (N, c) 所确定, 其中 N 为 n 比特的模数, $c \in Z_{N^{s+1}}$. 方案的有损陷门函数中的单向函数 c 是由 1 加密而成, 而有损函数 c 是由 0 经过随机 Damagard-Jurik^[7] 加密得到的, 其中 $s < \min\{P, Q\}$. 并且

Damagard-Jurik 加密机制可以确保单向函数和有损函数是计算不可区分的. 这里约定函数域限制在 $\{0, 1\}^{(n-1)s} \times \{0, 1\}^{n/2-1}$. 因为 N 为 n 比特的模数, 因此任何 $x \in \{0, 1\}^{(n-1)s}$ 都可以认为其为域 Z_{N^s} 中的元素. 又因为 P 和 Q 均为 $n/2$ 比特, 任意 $y \in \{0, 1\}^{n/2-1}$ 也可以认为其属于域 Z_{N^s} , 从而有 $\gcd(N, y) = 1$.

我们的方案可以由一个四元组 $F_s = (S_{loss}, S_{inj}, F, F^{-1})$ 来描述, 具体如下:

(1) 生成单向和有损函数: 算法 S_{loss} 以安全参数 1^n 作为输入, 选择 n 比特可接受的模数 $N = PQ$. 然后随机选择 $r \in Z_N^*$, 计算 $c = r^{N^s} \bmod N^{s+1}$, 对应的函数描述符为 $\sigma = (N, c)$; 算法 S_{inj} 同样以安全参数 1^n 作为输入, 选择 n 比特可接受的模数 $N = PQ$, 计算 $c = (1+N)r^{N^s} \bmod N^{s+1}$, 输出对应的函数描述符 $\sigma = (N, c)$, 该单向函数的陷门为 $\tau = (\lambda, r)$, 其中 λ 为 $P-1$ 与 $Q-1$ 的最小公倍数, 记为 $\lambda = lcm(P-1, Q-1)$.

(2) 评估: 给定函数描述符 $\sigma = (N, c)$ 以及对应的输入 $(x, y) \in \{0, 1\}^{(n-1)s} \times \{0, 1\}^{n/2-1}$, 有损陷门函数 F 将函数的输入 x, y 看作域 $Z_N^* \times Z_N^*$ 上的元素, 输出为 $c^x y^{N^s} \bmod N^{s+1}$.

(3) 求逆: 给定函数的描述符 $\sigma = (N, c)$ 以及陷门 $\tau = (\lambda, r)$, 由函数 F 的输出 $z \in Z_{N^{s+1}}$ 可以很容易的求出函数的输入.

4 安全性证明

定理 3 在合数剩余假设下, 上述构造的有损陷门函数有损度为 $(n-1)s - n/2 - 1$.

证明: 首先证明利用损陷门函数的单向函数可以很容易求逆. 由 RSA 模数 $N = PQ$, 其中 P, Q 是素数, 可以将乘法群 $Z_{N^{s+1}}^*$ 看作两个群 $G \times H$ 的作用结果. 其中群 G 是阶为 n^s 的循环群, H 与 Z_n^* 同余. 接着, 随机选择一个元素 $c \in Z_{N^{s+1}}^*$, 使得 $c = (1+n)^j \alpha \bmod n^{s+1}$, 其中 j 与 n 互素, $\alpha \in H$. 显然, 这里的 c 同时也是函数描述 (N, C) 的一部分. 因为 H 的阶与 n^s 互素, 因此若 $s < p, q$ 则 $\overline{1+n} = (1+n)H \in \bar{G}$ 为群 $\bar{G}$ 的生成元. 从而群 H 在 $Z_{N^{s+1}}^*$ 中陪集可以表示为:

$$H, (1+n)H, (1+n)^2H, \dots, (1+n)^{n^s-1}H$$

接着, 证明如何从 $(1+n)^i \bmod n^{s+1}$ 计算出 i . 首先, 定义一个函数 $L(b) = (b-1)/n$. 从而有:

$$L((1+n)^i \bmod n^{s+1}) =$$

$$\left(i + \left(\frac{i}{2}\right)n + \dots + \left(\frac{i}{s}\right)n^{s-1}\right) \bmod n^s$$

我们通过构造一个算法来计算 i , 该算法将提取出函数的值: 首先计算 $i_1 = i \bmod n$ 时的函数值, 然后计算 $i_2 = i \bmod n^2$ 的函数值, 依此类推. 显然, 计算 i_1 的值很容易计算 $i_1 = L((1+n)^i \bmod n^2) = i \bmod n$. 先假设已计算出 i_{j-1} 的值, 则 $i_j = i_{j-1} + k * n^{j-1}$, 其中 $0 \leq k < n$. 将其代入进 $L((1+n)^i \bmod n^{j+1}) = \left(i_j + \left(\frac{i_j}{2}\right)n + \dots + \left(\frac{i_j}{s}\right)n^{j-1}\right) \bmod n^j$ 则发现其中的每一个元素 $\left(\frac{i_j}{t+1}\right)n^t$ ($j > t > 0$) 满足: $\left(\frac{i_j}{t+1}\right)n^t = \left(\frac{i_{j-1}}{t+1}\right)n^t \bmod n^j$. 从而上式化简如下:

$$L((1+n)^i \bmod n^{j+1}) = \left(i_{j-1} + k * n^{j-1} + \left(\frac{i_{j-1}}{2}\right)n + \dots + \left(\frac{i_{j-1}}{s}\right)n^{j-1}\right) \bmod n^j$$

因此 i_j 可以推导如下:

$$\begin{aligned} i_j &= i_{j-1} + k * n^{j-1} = \\ i_{j-1} &+ L((1+n)^i \bmod n^{j+1}) - \\ &\left(i_{j-1} + \left(\frac{i_{j-1}}{2}\right)n + \dots + \left(\frac{i_{j-1}}{s}\right)n^{j-1}\right) \bmod n^j \\ &= L((1+n)^i \bmod n^{j+1}) - \\ &\left(\left(\frac{i_{j-1}}{2}\right)n + \dots + \left(\frac{i_{j-1}}{s}\right)n^{j-1}\right) \bmod n^j \end{aligned}$$

将其以算法形式描述如下:

```

i := 0;
for j := 1 to s do
begin
  t1 := L(a mod n^{j+1});
  t2 := i;
  for k := 2 to j do
  begin
    i := i - 1;
    t2 := t2 * i mod n^j;
    t1 := t1 - \frac{t2 * n^{k-1}}{k!} mod n^j;
  end
  i := t1;

```

给定密文 c , 计算 $\lambda = \text{lcm}(P-1, Q-1)$, 选择 d 使得 $d = 1 \bmod n^s$ 并且 $d = 0 \bmod \lambda$. 若 $z = F(x, y)$, 利用中国剩余定理, 我们有

$$\begin{aligned} z^d &= (c^x y^{n^s})^d = (((1+n)^j \alpha)^x y^{n^s})^d \\ &= (1+n)^{xjd \bmod n^s} (\alpha^x y^{n^s})^{d \bmod \lambda} \\ &= (1+n)^{xjd \bmod n^s} \end{aligned}$$

利用算法可以很容易的计算 $xjd \bmod n$, 因此利用陷门可以很容易求逆.

由于 Damagard-Jurik 加密机制确保有损陷门函数的单向函数和有损函数是计算不可区分的, 因此我们接下来只需要证明: 相对于 DDH 假设, 基于合数剩余假设的有损陷门函数能提高该函数的有损度. 在证明之前, 首先引入方案证明中所需的一个定理.

定理 4^[7] 对于任意可接受的 N 以及 $s < \min\{P, Q\}$, 定义 $Z_{N^s} \times Z_N^* \rightarrow Z_{N^{s+1}}^*$ 上的函数 $\phi_s(x, r) = (1+N)^x r^{N^s} \bmod N^{s+1}$ 在阿贝尔群上的运算是同构的. 其中:

$$\begin{aligned} \phi_s(x_1 + x_2 \bmod N^s, r_1 r_2 \bmod N) &= \\ \phi_s(x_1, r_1) \cdot \phi_s(x_2, r_2) \bmod N^{s+1} \end{aligned}$$

并且给定陷门 $\lambda(N) = \text{lcm}(P-1, Q-1)$, $\text{lcm}(P-1, Q-1)$ 表示 $P-1$ 与 $Q-1$ 的最小公倍数, 上述函数求逆可以在概率多项式时间内完成.

已知 (n, c) 为有损函数的描述符, 其中 $c = r^{N^s} \bmod N^{s+1}$, 由定理 4 的同构性可知:

$$\begin{aligned} |\text{Image}(N, c)| &\leq |\{c^x \cdot y^{N^s} \bmod N^{s+1} : x \in Z_{N^s}, y \in Z_N^*\}| \\ &= |\{(r^x \cdot y)^{N^s} \bmod N^{s+1} : x \in Z_{N^s}, y \in Z_N^*\}| \\ &= |\{\phi_s(0, r^x \cdot y \bmod N) : x \in Z_{N^s}, y \in Z_N^*\}| \\ &= |\{\phi_s(0, r^x) \cdot \phi_s(0, y) \bmod N\}| \\ &\leq N \leq 2^n \end{aligned}$$

因此该函数的有损度为 $l(n) = ((n-1)s + n/2 - 1) - n = (n-1)s - n/2 - 1$ 证明完毕. 因为 s 远大于 n , 由

$$\lim_{s \rightarrow \infty} \frac{n}{(n-1)s - n/2 - 1} = 0$$

可知基于合数剩余假设的有损陷门函数理论上可以达到我们任意想要的有损度. 又伪熵函数的抗泄漏量与有损陷门函数的有损度是成正比的, 因此基于合数剩余假设, 有损陷门函数的有损度提高了, 也就伪熵函数的抗泄漏量也就提高了.

5 结束语

本文首先介绍了自适应泄漏弹性的伪熵函数, 基于合数剩余假设, 文中对 Braverman 构造的伪熵函数进行优化, 相对于 Braverman 等人基于 DDH 假设构造的有损陷门函数, 我们采用合数剩余假设对其进行改进, 使得新方案具有更高的抗泄漏量.

的构建需要大量的训练数据.当数据数量不够大时,总有可能出现0观测值的现象,因此需要采用一些平滑算法;(3)本文的研究仅是从理论入手,尚缺少完善的实验数据.

参考文献:

- [1] 蒋宗礼,徐学可.一种基于集成学习与类指示器的文本分类方法[J].北京工业大学学报,2010,36(4):546-553.
- [2] Shao Fu bo, He Guo ping, Zhang Xin. An improved algorithm for multiclass text categorization with support vector machine[C]// International Symposium on Computational Intelligence and Design. 2008:336-339.
- [3] Rabiner L E A. Tutorial on hidden markov models and selected application in speech recognition[J]. Proceedings of The IEEE, 1989,79(2):257-286.
- [4] Freitag D, McCallum A. Information extraction with HMM structures learned by stochastic optimization [C]// Proceedings of the Eighteenth Conference on Artificial Intelligence. [s. l.]:[s. n.],2000:584-589.
- [5] Freitag D, McCallum A. Information extraction with

HMMs and shrinkages [C] // Proceedings of the AAAI'99 Workshop on Machine Learning for Information Extraction,[s. l.]:[s. n.],1999:31-36.

- [6] Frasconi P, Soda G, Vullo A. Hidden Markov models for text categorization in multi-page documents [J]. Journal of Intelligent Information Systems, 2002, 18(2):195-217.
- [7] 董云耀,钱如栏.一种改进的基于隐马尔可夫的信息检索模型[J].杭州电子科技大学学报,2009,29(4):46-49.
- [8] 杨健,汪海航.基于隐马尔可夫模型的文本分类算法[J].计算机应用,2010,30(9):2348-2350,2361.
- [9] 梁吉光,田俊华,姜杰.基于改进 HMM 的文本信息抽取模型[J].计算机工程,2011,37(20):178-179,182.
- [10] 张玉芳,彭时明,吕佳.基于文本分类 TFIDF 方法的改进与应用[J].计算机工程,2006,32(19):76-78.
- [11] 龚笔哄,彭波.对文本分类评测方法稳定性的研究[J].模式识别与人工智能,2008,21(1):12-17.

作者简介:

李开荣 男,(1963—),博士研究生,副教授.研究方向为智能信息处理、知识管理与决策支持.

(上接第 160 页)

本文仅仅探讨了具有自适应泄漏弹性的伪熵函数,下一步中我们将考虑基于伪熵函数具体的自适应泄漏弹性公钥加密方案.

参考文献:

- [1] Halderman J A, Schoen S D, Heninger N, et al. Lest we remember: Cold boot attacks on encryption keys [C]// In USENIX Security Symposium, SAN JOSE CA,2008:45-60.
- [2] Kocher P C. Timing attacks on implementations of diffie-hellman, ras, dss, and other systems[C]// CRYPTO, Springer-Verlay,1996:104-113.
- [3] Kocher P C, Jaffe J, Jun B. Differential power analysis[C]// In CRYPTO, 1999:388-397.
- [4] D A Osvik, A. Shamir, E. Tromer. Cache attacks

and countermeasures: The case of aes [C] // In CT-RSA, San Jose CA USA;IEEE,2006:1-20.

- [5] M. Braverman, A. Hassidim, Y. T. Kalai. Leaky Pseudo-Entropy Functions [C] // Computer Science Beijing, China:[s. n.] 2011.
- [6] C. Peikert and B. Waters. Lossy trapdoor functions and their applications [C] // In STOC. Victoria, British Columbia, Canada;IEEE, 2008:187-196.
- [7] J. Damgard and M. Jurik. A generalization, a simplification and some applications of Paillier's probabilistic public-key system [C] // In PKC, 2001, Che Ju Island, Korea;IEEE, 1992:119-136.

作者简介:

陈浩 男,(1987—),硕士研究生.研究方向为网络与信息安全.