基于互信息博弈的侧信道攻击安全风险评估

姚剑波[1] 张 涛[2]
(遵义师范学院计算机科学系 遵义 563002)[1]
(中国电子科技集团公司第三十研究所卫士通公司 成都 610041)[2]

摘 要 侧信道攻击的攻防过程可以视为互信息博弈过程,博弈的双方分别为密码设备设计者(防御方)和攻击者。防御方的博弈目标是通过制定相关的防御策略,减少由侧信道泄漏所引发的局部风险和全局风险;对攻击方而言,其博弈目标正好与之相反。从制定安全策略、降低安全风险的角度出发,将互信息博弈理论引入密码芯片设计者(防御方)和攻击者的决策过程,考察攻防策略的选择对安全风险的影响,并结合互信息的量化方法,给出了Nash均衡条件下攻防双方的优化策略选择方法及Nash均衡下攻防双方的互信息收益。

关键词 互信息博弈,侧信道攻击,安全风险,风险评估
中图法分类号 TP393.08 **文献标识码** A

Side Channel Risk Evaluation Based on Mutual Information Game

YAO Jian-bo[1] ZHANG Tao[2]
(Department of Computer Science, Zunyi Normal College, Zunyi 563002, China)[1]
(Westone Corporation of No. 30 Research Institute, China Electronics Technology Group Corporation, Chengdu 610041, China)

Abstract Attack process of side channel attacks can be regarded as mutual information gambling process. Both sides of the game were cryptographic equipment designers(defense party) and the attacker. The game goal of defenders is formulated by the defense strategy to reduce local and global risk which caused by the side channels leakage; to attack side, the game target and to the contrary. From make safety strategy, reduce safety risk angle, mutual information game theory is introduced in the decision-making process of the cryptographic chips designers(defense party) and the attacker, to investigate the attack and design tactics choice to security risks, and combined with the quantitative methods of the mutual information, give the optimization tactics selection method of the both sides of attack and design on Nash equilibrium conditions, give the mutual information benefits of the both sides of attack and design on Nash equilibrium.

Keywords Mutual information game, Side-channel attack, Risk, Risk evaluation

1 引言

物理器件的信息泄露是不可避免的,任何物理设备的运算都有可能遭受到侧信道攻击。侧信道攻击的应用研究是一种交叉领域的研究,涵盖了电子器件生产与制造、密码算法设计、安全的应用等诸多领域[1,2]。

从不同的角度出发,对侧信道攻击的应用领域进行拓展,一方面有助于加深对攻击本质的认识,另一方面也为在新的应用条件下制定安全的防御策略提供研究思路。

泄漏的安全风险的评估技术是密码芯片设计的一项关键技术[3,4]。Dakshi提出的关于电磁泄露的攻击评估方法[5],其核心思想是利用信号检测理论对电磁攻击进行建模分析,并结合信息论的分析方法对电磁泄露的信息进行定量分析;文献[6]提出了基于功耗泄露的安全性能评估方法,该方法主要是通过HammingWeight模型对差分能量攻击的安全性进行分析。这些研究主要针对单一的泄漏进行分析,并且没有提出有效的防御方法及策略来降低泄漏的风险。随着泄漏和攻击技术的多元化发展,在多种泄漏和攻击并存的复杂环境下,密码芯片的安全风险评估技术成为一个开放问题。

侧信道攻击的攻防过程可以被视为互信息的博弈过程,博弈的双方分别为密码设备设计者(防御方)和攻击者。防御方的博弈目标是通过制定相关的防御策略,减少由侧信道泄漏所引发的局部风险和全局风险;对攻击方而言,其博弈目标正好与之相反。

本文把互信息博弈理论引入密码芯片设计者(防御方)和攻击者的决策过程,建立一种互信息博弈的风险量化评估模型。与已有的评估方法比较,基于信息博弈的旁路风险量化评估模型不仅能用于单一泄漏的环境,而且能用于多种泄漏和攻击并存的复杂环境。

2 侧信道攻击的安全风险计算

在安全风险分析过程中,最重要的就是对安全风险的量度指标进行评估。采用文献[7]中关于安全风险指数的方法来度量侧信道泄漏风险,风险指数R可以表示为:

$$R=f(P_s,C_s)=P_s+C_s-P_sC_s \quad (1)$$

式中,P_s和C_s分别表示风险事件发生概率函数和所产生后

本文受贵州省科学技术基金项目(黔科合J字2009(2275))资助。
姚剑波 博士,CCF高级会员,主要研究方向为网络信息安全;张 涛 博士,主要研究方向为网络信息安全。

果函数。利用模糊理论对概率 P_s 进行估算，并用互信息 $I(leak_i, Key)$ 来表示安全风险的后果 C_s 的量度。

侧信道攻击的过程可以被认为是一个信息熵减少的过程，即攻击者试图通过统计分析来减少秘密的信息熵。假设 $H(leak_i)$ 表示 $leak_i$ 的信息熵，$H(Key|leak_i)$ 表示条件 $leak_i$ 下密钥 Key 的条件熵，$I(leak_i, Key)$ 为 $leak_i$ 和 Key 的互信息，则侧信道泄漏的信息熵和互信息的相互关系如图 1 所示。

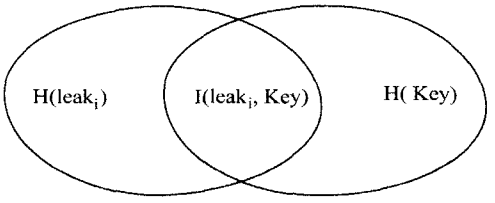

图 1　侧信道泄漏的信息熵与互信息关系图

侧信道攻击的目标是最大限度地获取泄漏信息与密钥的互信息，如式(2)所示：

$$I(Key, leak_i) = H(Key) - H(Key|leak_i) \tag{2}$$

攻击者利用不同类型的泄漏信息 $leak_i$ 对密钥 Key 进行分析，使得部分或全部的秘密信息被破解。从侧信道攻击的角度出发，对不同攻击方法的攻击性能进行量化分析，以及对防御策略的安全性进行分析，都可以借助于互信息的相关分析方法。

为了对互信息进行量化，需要对式(2)中各参数作定量。

(1)确定密钥 Key 的信息熵 $H(Key)$

假设密钥 Key 的概率密度函数为 $p_k()$，$E(x)$ 表示参数 x 的期望值，由 Shannon 信息熵可知，密钥 Key 的熵为：

$$H(Key) = -E(\log_2^{p_k()}) \tag{3}$$

(2) 确定条件信息熵 $H(Key|leak_i)$

攻击者通过对密钥 Key 的 q 次加密运算进行监测，获得侧信道泄漏信息 $leak_i$，利用该信息，攻击者建立与密钥 Key 相关的假设 P_e（e 为密钥相关的变量）。攻击者采用统计分析方法 $D(leak_i, P_e)$ 可以得到目标密钥集 KS：

$$KS = \{e | e = \text{argmax} D(leak_i, P_e)\} \tag{4}$$

式中，函数 argmax() 表示在统计分析 $D(leak_i, P_e)$ 结果最大条件下所有可能的密钥 e 的集合。

假设 $p(KS|leak_i)$ 表示在侧信道信息 $leak_i$ 条件下目标密钥集为 KS 的条件概率，则 q 次加密运算后，目标密钥集 KS 的条件信息熵为：

$$H_{KS}^q = -E(\log_2^{P(KS|leak_i)}) \tag{5}$$

由式(5)可以进一步确定密钥 Key 在条件 $leak_i$ 下的条件信息熵为：

$$H(Key|leak_i) = H_{Key}^q = -E(\log_2^{p(Key|leak_i)}) \tag{6}$$

由步骤(1)，(2)可以确定互信息 $I(leak_i, Key)$ 的数值。

3　侧信道攻击的互信息模型

把密码芯片的防御方和攻击者作为决策的对立双方，侧信道攻击的模型符合两人非合作不完全信息静态博弈[8]。在攻防决策过程中，密码芯片的防御方受到系统资源有限的限制，比如系统防御能力的增加是以牺牲一定的系统资源为代价；同样，攻击方也会受到攻击环境、实验条件等因素的约束。因此，攻防过程可以认为是在满足约束条件下的互信息博弈，即防御方试图减少侧信道泄漏与密钥的互信息值，而攻击方则试图增加其值。

侧信道攻击的互信息博弈模型由式(7)给出：

$$GAME = \langle N, A, U, ST \rangle \tag{7}$$

式中，N 为一个非空有限集合，其元素表示参与博弈的对立方，即防御方和攻击方。A 为局中人的行动策略空间，令：$A = \prod\limits_{1 \leqslant i \leqslant p, j \in N} A_i^j$，其中 $A_i^j = \{a_{i1}, \cdots, a_{ik}, \cdots, a_{iq}\}$ 表示局中人 j 对泄漏信息 $leak_i$ 采取的策略集合。U 表示局中人的收益函数。令：$U = \prod\limits_{1 \leqslant i \leqslant p, j \in N, 1 \leqslant k \leqslant q} u_{ik}^j$，其中 $u_{ik}^j = I_{a_{ik}}(leak_i, key)$ 表示侧信道信息 $leak_i$ 时，局中人 j 采用策略 a_{ik} 的互信息收益函数。ST 表示局中人的约束条件，其中 $ST = \prod\limits_{1 \leqslant i \leqslant p, j \in N, 1 \leqslant k \leqslant q} st_{ik}^j$，$st_{ik}^j$ 表示参与者 j 选择策略 a_{ik} 的约束条件。

对于博弈模型中的行动策略集合 A，其策略分布为 ΔA，假设 $C_i^j = \{\sigma_{i1}^j, \cdots, \sigma_{ik}^j, \cdots, \sigma_{iq}^j\}$ 表示参与者 j 对于单一泄漏 $leak_i$ 的策略分布，其中 σ_{ik}^j 表示参与者 j 选择策略 a_{ik} 的概率。当 $q=1$ 时，该策略为纯策略；当 $q>1$ 时，该策略为混合策略，即，纯策略可以看成是退化的混合策略。

在互信息博弈模型下，密码系统的安全风险主要由不同类型的侧信道泄漏及博弈双方的攻防策略而定。为便于分析，引入局部策略熵和全局策略熵的概念，对单一泄漏和多种泄漏条件下的博弈双方采取的策略进行分析，以下分别给出局部策略熵和全局策略熵的定义。

定义 1　对于博弈模型 $GAME = \langle N, A, U, ST \rangle$，$\Delta A$ 为行动集合 A 上的策略分布，对于任意的泄漏 $leak_i$，假设 $C_i^j = \{\sigma_{i1}^j, \cdots, \sigma_{ik}^j, \cdots, \sigma_{iq}^j\}$ 为参与者 j 对于泄漏 $leak_i$ 的一个混合策略分布，其中 σ_{ik}^j 表示参与者 j 选择策略 a_{ik} 的概率。在此条件下，局部策略熵定义为：

$$H_l(C_i^j) = -\sum_{k=1}^{q} \sigma_{ik}^j \ln \sigma_{ik}^j \tag{8}$$

式中，满足 $1 \leqslant i \leqslant p, j \in N, 0 \leqslant \sigma_{ik}^j \leqslant 1$，$H_l(C_i^j)$ 为参与者 j 选择混合策略 C_i^j 时的局部策略熵。

局部策略熵描述了对于单一泄漏信息的攻防策略的不确定性，为了衡量整个泄漏空间 LS 中所有的泄漏信息的攻防策略，引入全局策略熵的定义。

定义 2　假设侧信道信息泄漏空间为 $LS = \{leak_1, leak_2, \cdots, leak_i, \cdots, leak_p\}$，对于多种泄漏信息的攻防策略 $C^j = (C_1^j, \cdots, C_i^j, \cdots, C_p^j)$ 而言，其全局策略熵定义为：

$$H_g(C^j) = \frac{1}{p}\sum_{i=1}^{p} H_l(C_i^j) = -\frac{1}{p}\sum_{i=1}^{p}\sum_{k=1}^{q} \sigma_{ik}^j \ln \sigma_{ik}^j \tag{9}$$

式中，满足 $j \in N, 0 \leqslant \sigma_{ik}^j \leqslant 1$。

由博弈论的相关知识可知局部(全局)策略熵具有以下性质[8]：

(1) $0 \leqslant H_l(C_i^j) \leqslant \ln \sigma_{ik}^j$，$0 \leqslant H_g(C^j) \leqslant \ln \sigma_{ik}^j$

(2) $H_l(C_i^j) = 0$ 或 $H_g(C^j) = 0$ 当且仅当 σ_{ik}^j 退化为纯策略时；$H_l(C_i^j) = \ln q$ 或 $H_g(C^j) = \ln q$，当且仅当 $\sigma_{ik}^j = 1/q$，即参与者以相同的概率选择行动。

(3) 局部(全局)策略熵为 ΔA 分布上的连续凹函数。

侧信道攻击的互信息博弈反映出了博弈的局中人通过制定不同的策略，试图改变自身的收益(互信息)。通过对局部策略熵和全局策略熵的定义和分析，为量化单一泄漏的安全风险和多种泄漏环境下的安全性风险提供了理论支持。

4　优化的攻防策略-Nash 均衡分析

在博弈论中引入混合策略的重要意义在于使得所有的有限博弈都至少存在一个 Nash 均衡点[8]。在密码分析过程中，Nash 均衡是指这样一种状态：攻防双方参与者保持自己

的策略不变时，任何一方不可能通过单方面改变自己的策略来提高期望收益。在实际的环境中，当防御方采取安全性较高的防御方法时，攻击者可能获取的互信息收益就会比较低，所以攻击方选择攻击的可能性也较低；同理，防御方采取安全级别低的防御策略在现实中出现的可能也很小，因为该方法会让攻击者极大获利。综上，在博弈过程中，攻防双方总是试图争取自身利益最大化，因此出现一方收益较大而另一方收益很小这种"不理性"行为的可能性就会很低，最终攻防双方会达到收益的均衡状态。从风险评估的角度看，Nash 均衡条件下的侧信道泄漏风险值更符合于在实际情况下风险的度量值。显然，通过对 Nash 均衡状态的分析，有助于确定攻防双方的互信息博弈期望底线，从而为安全策略的制定提供依据。

在 p 种侧信道泄漏和 q 种攻击方法条件下，对应的策略分布为 ΔA，并且 j 和 $-j$ 分别表示博弈的对立双方，对于一个博弈局势，当且仅当满足：

$$\begin{cases} E(u_j(C_j^*, C_{-j}^*)) \geqslant E(u_j(S_j, C_{-j}^*)) \\ C_j^*, C_{-j}^*, S_j \in \Delta A \end{cases} \tag{10}$$

博弈双方采用的策略 (C_j^*, C_{-j}^*) 是一个 Nash 均衡策略，其中 $E(u_j(.))$ 表示参与者 j 的期望收益。该状态表明，博弈的双方参与者保持自己的策略不变时，任何一个参与者不可能通过单方面地改变自己的策略来提高期望收益。事实上，通过对攻防双方的博弈策略的分析，试图找到满足条件的 Nash 均衡点，就可以找到最合理的优化防御策略方案。然而，对于资源受限的嵌入式密码系统，攻防双方的博弈可以被认为是具有约束条件的互信息博弈。

下面对满足 Nash 均衡下的策略的选择进行分析。文献[9]指出最大熵提供了在约束条件下最为随机的分布，参与者总是选择不确定性最大的策略来迷惑对手。相反，如果局部(全局)策略熵是非最大熵时，则表明参与者在策略选择上具有一定的偏好，因此对手可以通过根据其策略的选择偏好调整自身的策略，以获得更大的价值收益。因此，当策略熵为最大熵时，所采取的策略为 Nash 均衡策略[10]。即，Nash 均衡条件下的全局策略熵满足：

$$H_{NE}(C_j^*) = \max\{H_g(C^j)\} \tag{11}$$

且

$$H_{NE}(C_{-j}^*) = -\frac{1}{p}\sum_{i=1}^{p}\sum_{k=1}^{q}\sigma_{ik}^{-j}\ln\sigma_{ik}^{-j} \tag{12}$$

式中，$\forall j, -j \in N$。

为了求取式(12)中最大熵的分布，该文将攻防策略的约束 ST 条件以及参与者的预期收益 U_e^j 作为最大熵的附加条件，则攻防双方的优化策略熵满足：

s. t.

i) $\sum_{i=1}^{p}\sum_{k=1}^{q}\sigma_{ik}^{j} = 1, 0 \leqslant \sigma_{ik}^{j} \leqslant 1$,

ii) $U_d^j \leqslant U_e^j = E[u_j(C_j, C_{-j}^*)] \leqslant U_u^j$

iii) $\sum_{i=1}^{p}\sum_{k=1}^{q} st_{ik}^{j} * \sigma_{ik}^{j} \leqslant ST$ (13)

式中，U_d^j, U_u^j 分别表示参与者 j 的预期收益的上下界，st_{ik}^{j} 表示策略 a_{ik}^{j} 的约束条件。根据文献[11]，上述优化问题可以转化为：

$$\max_{0 \leqslant M \leqslant ST, U_d^j \leqslant U_e^j \leqslant U_u^j} \{H_{\max}(C^j)\}$$

s. t.

i) $\sum_{i=1}^{p}\sum_{k=1}^{q}\sigma_{ik}^{j} = 1, 0 \leqslant \sigma_{ik}^{j} \leqslant 1$,

ii) $U_e^j = E[u_j(C_j, C_{-j}^*)]$

iii) $M = \sum_{i=1}^{p}\sum_{k=1}^{q} st_{ik}^{j} * \sigma_{ik}^{j}$ (14)

根据式(14)，具有约束条件下的嵌入式密码系统的最优攻防策略的查找方法如下：

首先求出满足以上附加条件的最大熵分布，然后在这些最大熵分布中找出一个最大值所对应的分布。如果它不是 Nash 均衡策略，假设存在另外一个最大熵分布为 $S' = \{\sigma_1', \sigma_2', \cdots, \sigma_{pq}'\}$，由于熵是连续有界的凹函数，因此这样的 S' 一定是存在且唯一的，所以 $S' = C^*$。由此可知，最大策略熵为 Nash 均衡的充分必要条件。此时，博弈中参与者 j 的 Nash 均衡收益为：

$$E[u_j(C_j^*, C_{-j}^*)] = \sum_{i=1}^{p}\sum_{k=1}^{q}\sigma_{ik}^{j}E[u_j(a_{ik}, C_{-j}^*)] \tag{15}$$

式中，$u_j(a_{ik}^{j}, C_{-j}^*) = I_{a_{ik}^{j}}(leak_i, key)$。由式(15)可知，当 $p=1$ 时，$E[u_j(C_j^*, C_{-j}^*)]$ 表示单一泄漏条件下，参与者 j 在 Nash 均衡下的互信息收益，即局部均衡收益；当 $p>1$ 时，其值表示在多种泄漏条件下密码系统的 Nash 均衡收益，即全局均衡收益。

结束语 随着攻击的多元化发展，在多种泄露条件下，密码芯片的安全风险评估问题以及优化的攻防策略选择问题成为目前研究的盲点。

本文从制定安全策略、降低安全风险的角度出发，将互信息博弈理论引入密码芯片设计者(防御方)和攻击者的决策过程，进一步考察了攻防策略的选择对安全风险的影响，并结合互信息的量化方法，给出了 Nash 均衡条件下攻防双方的优化策略选择方法及 Nash 均衡下攻防双方的互信息收益。与已有的评估方法比较，基于信息博弈的旁路风险量化评估方法不仅能用于单一泄漏的环境，而且能用于多种泄漏和攻击并存的复杂环境。

参 考 文 献

[1] 周永彬，徐秋亮. 侧信道攻击理论与技术[M]. 中国密码学发展报告 2008. 北京：电子工业出版社，2009：191-259

[2] 杜之波，陈运，吴震，等. 防范边信道攻击的逆伪操作实现算法[J]. 计算机工程，2010，36(3)：131-133

[3] 李鹤田，刘云，何德全. 信息系统安全风险评估研究综述[J]. 中国安全科学学报，2006，16(1)：108-115

[4] 王伟，李春平，李建彬. 信息系统风险评估方法的研究[J]. 计算机工程与设计，2007，28(14)：3473-3475

[5] Agrawal D, Archabeault B, Rao J R. The EM side-channel: attacks and assessment methodlogies[C]// Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems(CHES). 2002, 2523: 29-45

[6] Mangard S. Hardware countermeasures against DPA-a statistical analysis of their effectiveness[C]// Proceeding of CT-RSA 2004. 2004, 2964: 222-235

[7] 钱钢. 信息系统安全管理[M]. 南京：东南大学出版社，2004

[8] Fudenberg D. Game Theory[M]. Beijing: China Renmin University Press, 2002

[9] Van Campenhout J M, Cover T M. Maximum entropy and conditional probability[J]. IEEE Transactions on information theory, 1981, IT-27(4): 483-490

[10] He Da-yi, Qiu Wan-hua. Nash equilibria based on strategic entropy[EB/OL]. http://www.paper.edu.cn/paper.php?serial_number=200312-23

[11] Qiu Wan-hua. Management Strategy and Application Entropy [M]. Beijing: China Machine Press, 2002