A5/1 时空折中攻击模型的参数选择研究

李 磊* 韩文报 王 政
(解放军信息工程大学信息研究系 郑州 450002)

摘 要：作为全世界使用最广泛的移动通信系统，全球移动通信系统(GSM)中使用的 A5/1 加密算法安全性研究有重要的现实意义。该文通过对 A5/1 算法状态空间缩减性质的分析，描述了基于可变可辨点的多表瘦彩虹表时空折中攻击模型，并给出此模型各个指标的计算公式及确定相关参数的方法。通过利用 FPGA 硬件平台和参数选择确定，实现了成功率是 99%的实时破译计算平均耗时为 1 s，从而增加了攻击的现实可用性。此攻击模型的相关参数确定方法对其他平台及限制条件下的攻击实现有一定的参考价值。

关键词：时空折中攻击；瘦彩虹表；可变可辨点；成功率
中图分类号：TN918.4 **文献标识码**： A **文章编号**：1009-5896(2012)08-1911-06
DOI: 10.3724/SP.J.1146.2011.01217

The Research of Parameters Selection on the Model of Time-memory-data Trade-off Attack to A5/1

Li Lei Han Wen-bao Wang Zheng
(*Department of Information Researching, PLA Information Engineering University, Zhengzhou* 450002, *China*)

Abstract: GSM is the most popular world-wide standard for mobile communication system. GSM uses A5/1 algorithms to protect the users' information. It is very important to research the attack of A5/1. In this paper, by analyzing the property of the state space' reduction, a model of Time-memory-data trade-off attack to A5/1 algorithms is described, that model based on variable distinguished point and thin rainbow tables. The formulas are derived and the parameters are determined. By using FPGA and parameters determining, the attack success rate exceeds 99% in 1 second on average that improve the practicability of the attack. Based on this model, the method to determine the parameters has reference value to other platform and constraints.

Key words: Time-memory-data trade-off attack; Thin rainbow table; Variable distinguished point; Success rate

1 引言

GSM 是目前使用最广泛的移动通信系统，用户超过了 44 亿[1]。因此语音通话、短信息以及数据通信的安全性就显得尤为重要。GSM 使用 A5 族算法来保护数据安全，其中密码算法分别是 A5/1, A5/2 和 A5/3 算法。A5/1 和 A5/2 是基于移位寄存器的序列密码算法。其中 A5/2 是 A5/1 的弱化版本，主要用于出口欧洲和北美之外的国家。A5/3 是基于分组密码算法的，目前尚未启用。

A5/1 算法一经出现就成为研究的热点。近 20 年来，比较有代表性的有基于解线性方程组的猜定攻击算法[2]和基于时空折中攻击的[2−4]方法。但是由于通信的实时性要求，上述方法还未产生实质性威胁。直至 2009 年，Nohl[5]公布了利用彩虹表的方法。Nohl 使用 4 块 GPU 加速卡一个月时间内生成 2 TB 的数据表，可以达到在 2 帧已知明文攻击条件下，使用 2 块 GPU 加速卡在 5 s 中内完成破解。这就使得 GSM 的使用受到严重的威胁。但在文献[5]中并没有对基于彩虹表的时空折中模型进行详细的描述，并且对参数的选择没有给出说明。

本文通过对 A5/1 算法中状态空间收敛性质的研究，描述了基于可变可辨点的多表瘦彩虹表模型，给出了相关指标表达式。并且通过时间与空间、数据之间折中、迭代函数中步长和状态空间缩减比例之间折中，在 FPGA 平台下，根据约束条件对参数进行了选择。在本文选择的参数下，在预计算阶段利用 32 个 FPGA 芯片一个月时间内完成 2 T 大小的数据表计算；在实时计算阶段利用 16 个芯片，实现破解 A5/1 算法平均时间只需 1 s，破解成功率为 99%以上。相对于文献[5]中的破译时效性上有了较大幅度的提高，并且使用 FPGA 平台无论是预计算阶段还是实时计算阶段功耗都大幅降低。

2011-11-22 收到，2012-04-06 改回
国家 863 计划项目(2009AA012201)和上海市科委重大科技攻关项目(08dz501600)资助课题
*通信作者：李磊 leilimoon@hotmail.com

本文其余部分的组织如下。第 2 节介绍 A5/1 算法和状态空间缩减性质。在第 3 节中描述了基于可变可辨点的多表彩虹表模型，并在此基础上给出了各个指标的表达式。第 4 节中，在 FPGA 实现平台下，根据具体的已知明文数量、预计算时间、存储空间大小和实时阶段实时性要求的限制，给出了参数的选择方法。第 5 节是结束语。

2 A5/1 算法描述及状态空间缩减性质

本节主要介绍了 GSM 中 A5/1 算法和使用方式以及进行攻击的数据条件，并通过对状态空间与运行时长之间的数据统计给出了状态空间缩减性质的统计结果。

2.1 A5/1 算法描述

A5/1 算法是基于移位寄存器的序列密码算法，用于 GSM 系统中保护手机和基站之间的通信。A5/1 算法由 3 个长度分别为 19, 22, 23 的级数较短的反馈移位寄存器组成，通过 3 个移位寄存器的控制位进行择多互控完成步进控制。结构如图 1 所示。

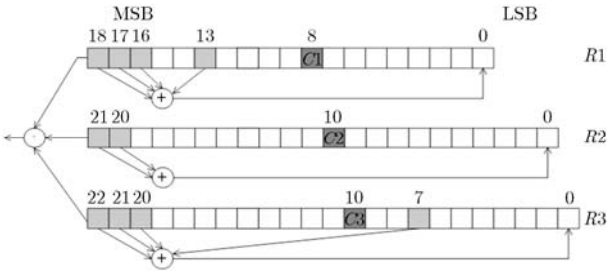

图 1 A5/1 算法结构

3 个移位寄存器分别设为 $R1$，$R2$，$R3$，控制位分别是 3 个寄存器的第 8, 10, 10 位并记为 $C1$，$C2$，$C3$。其中择多步进的定义为：设择多函数是 $maj(C1,C2,C3)=C1C2\oplus C2C3\oplus C1C3$，如果 $Cj=maj(C1,C2,C3), j=1,2,3$，则寄存器 Rj 步进。

A5/1 算法描述：其中 Kc 是 A8 算法生成的 64 bit 初始会话密钥。**IV**(Initial Value)表示由帧号生成的 22 bit 初始向量。

(1)初始化：将 3 个寄存器都置为 0。

(2)装配 Kc 和 **IV**：3 个寄存器正常步进，同时将 Kc 与 3 个寄存器的最低位进行异或操作，如此进行 64 步。然后以同样的方式对 22 bit 初始向量 **IV** 进行操作。

(3)预热阶段：按控制位的择多步进方式运行 100 步。在这一阶段不输出乱数流。

(4)密钥流生成：按控制位的择多步进方式运行 228 步，产生 228 bit 乱数，其中前 114 bit 用于下行数据，后 114 bit 用于上行数据。

在实际攻击环境中，能够得到的数据是唯密文数据。但是由于在通信过程中，尤其是在控制信道中，移动设备和基站交互的过程中会出现已知传输的内容的情况，因此可以得到已知明文的数据条件。并且在实际攻击的过程中利用的数据越少，所形成的实时性越高，攻击的效果和造成的威胁就越大，但同时对攻击方的要求也就越高。本文设定的数据条件是 2 组 228 bit 对应上下行的已知明文数据。

2.2 状态空间缩减性质

在考虑 A5/1 算法的鲁棒性时，要求状态空间的大小与时间无关，亦即各时刻的状态空间大致相同。但是文献[2]在计算一步状态转移时发现 $t=1$ 时刻的状态空间大小是 $t=0$ 时刻的 5/8。进而在文献[6]和文献[7]中，使用数据统计的手段发现状态空间和时间增长之间的关系，结果如表 1 所示。其中 t 表示 A5/1 运行时刻，表中的值是在 t 时刻状态空间相对于 $t=0$ 时刻缩减去掉部分的比例，定义为 $\mathrm{Ed}(t)$。

从表 1 中可以看出，随着时间的增长，状态空间缩减情况越发严重。

在对 A5/1 算法进行攻击时，如文献[2]中指出的，只要能根据密钥流数据得到某一时刻的寄存器状态，那么就容易利用文献[2]中的方法根据已知 **IV** 向量值递推得到初始会话密钥 Kc。因此在 $t>0$ 时刻，状态空间的缩减带来了攻击时搜索空间的减小，降低了攻击的复杂度。设状态空间函数为：$N(t)=N(0)\cdot(1-\mathrm{Ed}(t)), t>0$，其中 $N(0)=2^{64}$。由于 $N(t)$ 随着 t 的增长而减小，但是在后续章节中看出 t 值的增加又会带来预计算时间和实时阶段计算时间的增加，因此本文建立了 $N(t)$ 和 t 的折中，对于 t 的选择将在第 3 节中给出。为此，本文通过对 2^{26} 个初始状态的统计得出详细的 $\mathrm{Ed}(t)$ 与 t 之间的关系，如表 2 所示。

3 多个使用可辨点的瘦彩虹表模型及其参数公式

时空折中攻击是用于攻击密码算法中的单向函数的有效方法。通过对存储空间和运算时间的折中，有效地降低了攻击的时间复杂度。自 1980 年 Hellman[8]首次提出时空折中的方法，至今又做出了很多改进，比如在单表中应用多个不同迭代函数的彩虹表方法，利用可辨点降低查表次数的方法等。本文在此基础上提出了应用可变可辨点方法有效降低查表次数和存储空间，并由此提出了基于此的多表瘦彩虹表时空折中攻击模型。

表 1 参考文献中状态空间缩减性质表

t	1	5	10	20	30	50	100	150
文献[6]中 Ed(t)	0.375	0.47	0.52	0.61	N/A	0.73	0.81	0.84
t	16	32	48	64	80	96	100	150
文献[7]中 Ed(t)	0.57	0.68	0.74	0.78	0.82	0.84	0.86	0.89

表 2 状态空间缩减性质统计表

t	10	20	30	40	50	64	70	80	90	100
Ed(t)	0.513	0.609	0.67	0.715	0.748	0.782	0.794	0.81	0.824	0.835
t	110	120	130	140	150	160	170	180	190	200
Ed(t)	0.845	0.854	0.861	0.868	0.874	0.879	0.884	0.889	0.892	0.896

3.1 时空折中模型的建立

时空折中攻击模型一般包括两个部分：预计算阶段和实时计算阶段。在预计算阶段需要构造数据表，表中要尽量覆盖搜索空间，这一部分类似于穷尽攻击，但是预计算只需一次并且只需存储预计算阶段的一部分数据来代表整个搜索空间。实时计算阶段是在已知明文条件下，通过查找数据表中相对应的数据和少量的计算来恢复初始密钥。下面建立基于可变可辨点的 r 个表瘦彩虹表时空折中攻击模型。

预计算阶段　设 $x_{k,j,h}$ 为第 k 个表中第 j 条链的第 h 个点，其中点表示一个 64 bit 向量，并且 $x_{k,j,0}$ 为这条链的起点其高 d bit 为固定串。f_i 表示对数据表中点进行 t 步 A5/1 算法推排，其中 $i=1,\cdots,S$，S 是在一条链中使用不同迭代函数的个数。$R_k(f_i)$ 表示第 k 个表中 f_i 的结果进行的第 k 种密钥流到寄存器状态的变换函数。则第 k 个表中第 j 条数据链表示如下：

$$\begin{aligned} &x_{k,j,0} \xrightarrow{R_k(f_1)} x_{k,j,1} \xrightarrow{R_k(f_2)} \cdots \xrightarrow{R_k(f_S)} \\ &x_{k,j,S} \xrightarrow{R_k(f_1)} \cdots \xrightarrow{R_k(f_S)} x_{k,j,l_{k,j}S} \end{aligned} \tag{1}$$

其中 $x_{k,j,l_{k,j}S}$ 为终点，结束条件为其高 d bit 与起点相同的固定串，定义 $l_{k,j}$ 为其链长。由于存在某个起点通过迭代不能到达可辨点的情况和链长过短的情况，因此设定 $(l_{\min},l_{\max})$ 为最短链长和最大链长作为限定条件。定义起点和终点中使用相同的固定比特串作为可辨点的方法称为可变可辨点，这样做的好处是可以减少存储空间。

设在每个表中的初始点个数是 m，则 r 个瘦彩虹表时空折中模型如图 2 所示。

不同的起点可能会有相同的终点，因此根据终点的非固定低比特进行排序，然后按照链长去掉终点相同而长度较小的链构成完美表，最后存储起点、终点和链长作为数据表中元素。

实时计算阶段　实时计算阶段的作用是要恢复给定的密钥流数据所对应某时刻的寄存器状态。设给定一个 64 bit 密钥流数据为 c_0。首先计算其对应的 $r\times S$ 个 $R_k(f_i)$ 值。然后对这 $r\times S$ 个进行类似于预计算阶段的迭代，如果链长在 $(l_{\min},l_{\max})$ 范围内达到可辨点则进行查表。如果可以在数据表中找到相对应的终点，再根据查表得到对应的起点得到 $R_k(f_i)$ 的上一个输入，即可根据第 k 个表的状态排列方式

$$\begin{cases} m\text{行} \begin{cases} x_{1,1,0} \xrightarrow{R_1(f_1)} x_{1,1,1} \xrightarrow{R_1(f_2)} \cdots \xrightarrow{R_1(f_S)} x_{1,1,S} \xrightarrow{R_1(f_1)} \cdots \xrightarrow{R_1(f_S)} x_{1,1,l_{1,1}S} \\ \vdots \\ x_{1,m,0} \xrightarrow{R_1(f_1)} x_{1,m,1} \xrightarrow{R_1(f_2)} \cdots \xrightarrow{R_1(f_S)} x_{1,m,S} \xrightarrow{R_1(f_1)} \cdots \xrightarrow{R_1(f_S)} x_{1,m,l_{1,m}S} \end{cases} \\ \vdots \\ m\text{行} \begin{cases} x_{r,1,0} \xrightarrow{R_r(f_1)} x_{r,1,1} \xrightarrow{R_r(f_2)} \cdots \xrightarrow{R_r(f_S)} x_{r,1,S} \xrightarrow{R_r(f_1)} \cdots \xrightarrow{R_r(f_S)} x_{r,1,l_{1,1}S} \\ \vdots \\ x_{r,m,0} \xrightarrow{R_r(f_1)} x_{r,m,1} \xrightarrow{R_r(f_2)} \cdots \xrightarrow{R_r(f_S)} x_{r,m,S} \xrightarrow{R_r(f_1)} \cdots \xrightarrow{R_r(f_S)} x_{r,m,l_{1,m}S} \end{cases} \end{cases}$$

图 2 r 个瘦彩虹表时空折衷模型

得到对应的寄存器状态。利用文献[2]中递归状态推排方法，即可得到初始的 64 bit 会话密钥。如果有多个 64 bit 密钥流数据，则重复上述过程，直至找到对应的正确会话密钥。

3.2 时空折中模型的指标

下面详细说明时空折中模型成功率等公式及相关参数选择依据、存储空间大小和预计算时间、实时阶段计算时间和查表次数、迭代函数推拍步数 t 的选择。

3.2.1 成功率及相关参数 设 $P_{\mathrm{DP}}(l)$ 为在不超过 l 次迭代内能够达到可辨点的概率，根据文献[9]中的结果，若 d 为可辨点中固定串长度则有 $P_{\mathrm{DP}}(l)\approx 1-e^{-l/2^d}$。如果 $l_{\max}=2^{d+4}$，那么有 $P_{\mathrm{DP}}(l_{\max})\approx 1$，因此本文确定 $l_{\max}=2^{d+4}$ 作为链长上限。

由于 r 个彩虹表中每个表的起点个数是 m，设每个表链长范围在 $(l_{\min},l_{\max})$ 内的个数是 m'，则有

$$m'=\sum_{i=1}^{m}\Pr(x_{k,i,0}\mapsto \mathrm{DP})=\sum_{i=1}^{m}(P_{\mathrm{DP}}(l_{\max})-P_{\mathrm{DP}}(l_{\min}))\approx m\left(e^{-\frac{l_{\min}}{2^d}}-e^{-\frac{l_{\max}}{2^d}}\right)$$

设 $l_{\mathrm{av}}^{'}$ 为这 m' 个点的平均长度，因此可以得到

$$\begin{aligned}l_{\mathrm{av}}^{'}&=\frac{1}{m'}\sum_{l=l_{\min}}^{l_{\max}}m(P_{\mathrm{DP}}(l)-P_{\mathrm{DP}}(l-1))l\\&\approx\frac{\sum_{l=l_{\min}}^{l_{\max}}(e^{-\frac{l-1}{2^d}}-e^{-\frac{l}{2^d}})l}{e^{-\frac{l_{\min}-1}{2^d}}-e^{-\frac{l_{\max}}{2^d}}}\\&=2^d+(l_{\min}-1)-\frac{l_{\max}-l_{\min}+1}{e^{\frac{l_{\max}-l_{\min}+1}{2^d}}}\approx 2^d+l_{\min}\end{aligned}\quad(2)$$

若有 $l_{\min}\ll 2^d$，从式(2)可以看出 $l_{\mathrm{av}}^{'}\approx 2^d$，在本文中取 $l_{\min}=2^{d-5}$。

从时空折中模型的预计算阶段可以看出，在存储时需要按照链长去掉终点相同而长度较小的链构成完美表，因此设 l_{av} 是完美表的平均链长。设完美表中最终保留的链数平均为 $\widehat{m}$，则由第 2 节中状态空间缩减性质可知 $\widehat{m}\le(1-\mathrm{ED}(t))m$，亦即平均有 $1/(1-\mathrm{ED}(t))$ 条链有相同的终点。由于 64 bit 密钥流数据条件要求，因此本文中默认取 $t\ge 64$。而这 $1/(1-\mathrm{ED}(t))$ 条链的链长都小于 2^d 的概率是 $(P_{\mathrm{DP}}(l<2^d))^{1/(1-\mathrm{ED}(t))}\ll 1$ (运用第 2 节中 $\mathrm{ED}(t)$ 与 t 的关系)。因此进行类似 $l_{\mathrm{av}}^{'}$ 的计算，并在此时取 $l_{\min}=2^d$，则有结果 $l_{\mathrm{av}}=2^{d+1}$。

由上述可以得出，单个利用可变可辨点的瘦彩虹表成功率是 $P_{\mathrm{succ}}^{'}=\widehat{m}l_{\mathrm{av}}S/N(t)=2^{d+1}\widehat{m}S/N(t)$。则 r 个彩虹表的成功率可表示为 $P_{\mathrm{succ}}=1-(1-P_{\mathrm{succ}}^{'})^r$。用 D 表示可以利用的 64 bit 密钥流数据个数，则使用 D 个密钥流数据的时空折中模型成功率可以表示成 $P_D=1-(1-P_{\mathrm{succ}})^D$。对于给定的 2 组 228 bit 密钥流数据，每组可以利用 165 个 64 bit，因此总的密钥流数据是 330 个，亦即 D=330。

下面对 $\widehat{m}$ 的大小进行详细的分析。每个彩虹表的起点个数是 m 个，而链长范围在 $(l_{\min},l_{\max})$ 内的个数是 m'，设 m_i 表示为瘦彩虹表第 i 列中新出现的点的个数，其中此处的“新出现的点”表示前第 $i-S$，$i-2S,\cdots,i-\lfloor i/S\rfloor S$ 列中并未出现过的点。因此有 $m_0=m'$，而根据第 2 节中状态空间缩减性质有 $m_1=(1-\mathrm{ED}(t))m'$。根据文献[4]中的链数公式可得

$$\widehat{m}=\left(N(t)-\sum_{k=1}^{\lfloor l_{\mathrm{av}}/S\rfloor}m_{l_{\mathrm{av}}-kS}\right)\left(1-e^{-\frac{m_{l_{\mathrm{av}}-1}}{N(t)}}\right)$$

由 $\sum_{k=1}^{\lfloor \frac{l_{\mathrm{av}}}{S}\rfloor}m_{l_{\mathrm{av}}-kS}\le\lfloor l_{\mathrm{av}}/S\rfloor m_1$ 得 $N(t)-\sum_{k=1}^{\lfloor \frac{l_{\mathrm{av}}}{S}\rfloor}m_{l_{\mathrm{av}}-kS}\ge N(t)-\lfloor l_{\mathrm{av}}/S\rfloor m_1$。又由文献[10]中的近似公式，有 $N(t)\left(1-e^{-\frac{m_{l_{\mathrm{av}}-1}}{N(t)}}\right)\approx\frac{m_1}{1+\frac{l_{\mathrm{av}}S}{N(t)}}$ 成立。故最终可得

$$\begin{aligned}\widehat{m}&\approx(1-\mathrm{ED}(t))m'(N(0)-\lfloor l_{\mathrm{av}}/S\rfloor m')\\&\cdot\left(N(0)+\frac{l_{\mathrm{av}}S}{1-\mathrm{ED}(t)}\right)^{-1}\end{aligned}\quad(3)$$

由此看到单个利用可变可辨点的瘦彩虹表成功率可以表示为

$$P_{\mathrm{succ}}^{'}\approx\frac{l_{\mathrm{av}}Sm'}{N(0)}\left(1-\lfloor l_{\mathrm{av}}/S\rfloor\frac{m'}{N(0)}\right)\left(1+\frac{l_{\mathrm{av}}S}{(1-\mathrm{ED}(t))N(0)}\right)^{-1}\quad(4)$$

3.2.2 存储空间及预计算时间 由于 r 个彩虹表中每个的起点个数是 m 个，r 个完美表中终点个数的平均值是 $\widehat{m}$。并设存储一条链所需大小为 M_0 (包括起点、终点和链长)。则数据表存储空间大小为 $M=\widehat{m}\cdot r\cdot M_0$。其中由于采用了可变可辨点，因此省略了起点和终点中固定串的存储，并且利用文件信息固定表示可以做到存储一个链只需 7 个字节，即 $M_0=7$。从式(4)可以看出，利用状态空间缩减性质大大增加了单位存储所包含的有效信息。

预计算阶段链的平均长度表示 $l_{\mathrm{av}}^{'}$，t_0 表示预计算阶段实现 A5/1 算法迭代函数推排 t 步所需时间，则预计算时间为 $T_0=m\cdot l_{\mathrm{av}}^{'}\cdot S\cdot r\cdot t_0$。

3.2.3 实时阶段运算时间及查表次数 设 t_1 表示实时计算阶段实现 A5/1 算法迭代函数推排 t 步所需时间，则实时阶段运算时间计算公式为 $T_1=D\cdot S\cdot r\cdot l_{\mathrm{av}}\cdot S\cdot t_1$。而对于 D 个 64 bit 密钥流数据，每一个需要查表 $S\cdot r$ 次，因此共需要 $D\cdot S\cdot r$ 次查表。

3.2.4 迭代函数推拍步数 t 的选择 从 3.2.2 节可以看出，状态空间函数 $N(t)$ 随着 t 的增长而减小从而增加了存储空间利用效率，但是迭代函数推排步数 t

的增加又带来了预计算时间和实时阶段运算时间的增加。因此我们选择 t 使得 $(1-\mathrm{ED}(t))\cdot t^2$ 达到最小值。但是由于密钥流数据要求 $t \geq 164$，因此从第 2 节表 2 经过计算可以得出，$t=164$ 为最佳选择。

4 时空折中模型的 FPGA 实现及相关参数确定

4.1 瘦彩虹表时空折中模型的 FPGA 实现

在文献[5]中，Nohl 使用 GPU 运算卡作为主要计算平台，相对于 GPU 来说 FPGA 具有功耗低、专门针对算法的深入优化和利用流水线实现等优点，但是逻辑编程相对困难。本文利用 Altera 公司的 Cyclone IV 系列中 EP4CGX150 芯片作为计算平台，使用 Quartus II 10.0 软件作为编译工具和 ModleSim-Altera 作为仿真工具进行实现测试。

利用流水线技术可以高效利用芯片逻辑单元资源和片内存储资源，从而实现高效的并行计算。由于一个迭代函数的推排需要 t 步，因此可以形成一个 t 级流水线的计算单元。通过 Quartus II 11.0 软件进行编译、布线、时钟分析和功耗分析，使用 ModleSim-Altera 仿真验证正确性，得出了在 EP4CGX150 芯片实现一个计算单元需要 5864 个逻辑单元(LEs，布线后)、占用的存储单元为 29733 bit、工作频率达到 200 MHz，功耗为 0.1 W。

从上看出，在一个 EP4CGX150 芯片上可以实现 23 个流水线单元，并且单个芯片的功耗为 2 W 左右。因此如果在预计算阶段使用 32 个这样的芯片，可得出基本计算时间 $t_0 = 2^{-37.1}$ s。在实时计算阶段需要 16 个这样的芯片，因此有 $t_1 = 2^{-36.1}$ s。

4.2 相关参数的确定

在现有文献中，时空折中参数的确定一般都是由实验经验得到的。在本文中，根据第 3 节中公式和在本节中所设定的条件可以经过计算来确定参数。

下面来设定各个约束条件。类似文献[5]中条件，假设需要 2 T 的存储空间并且预计算时间在 1 个月内完成。与文献[5]中不同的是，本文将实时阶段的破译计算时间缩短至 2 s，平均的实时计算时间为 1 s，设成功率限制为 99%以上，这样会大大提高实际的可用性。并且使用 FPGA 平台在 1 个月内完成预计算阶段只需要 46 kW·h，相对于文献[5]中 850 kW·h 有了大幅的提高。

下面根据预计算阶段和实时计算阶段的基本计算时间以及上面的约束条件来确定参数的选取。

(1)根据预计算时间公式和 t_0 的值可以得到 $m\cdot 2^d \cdot S\cdot r = 2^{58.4}$，其中一个月按 30 天计算。

(2)根据存储空间公式及存储空间 2 T 的约束条件，并且结合式(3)，考虑到 $\lfloor l_{\mathrm{av}}/S \rfloor m' \ll N(0)$ 和 $\dfrac{l_{\mathrm{av}}S}{1-\mathrm{ED}(t)} \ll N(0)$，因此有 $\left(N(0)-\lfloor l_{\mathrm{av}}/S\rfloor m'\right)\cdot\left(N(0)+\dfrac{l_{\mathrm{av}}S}{1-\mathrm{ED}(t)}\right)^{-1} \approx 1$，再由 $l_{\min}=2^{d-5}$ 和 $l_{\max}=2^{d+4}$，$m' \approx m\left(e^{-\frac{l_{\min}}{2^d}}-e^{-\frac{l_{\max}}{2^d}}\right)$，故有 $m' \approx 0.97m$。综合可得 $m\cdot r \approx 2^{41}$。

(3)根据成功率公式(4)，取 $D=330$ 和 $1-(1-P'_{\mathrm{succ}})^{rD} \geq 99\%$，可以得到 $r=2^5$。

(4)根据实时阶段运算时间公式和 t_1 的值及 $m\cdot r \approx 2^{41}$ 和 $m\cdot 2^d \cdot S\cdot r = 2^{58.4}$，有 $S\cdot r = 2^{10}$，因此参数 $S=2^5$。

(5)结合步骤(4)和步骤(1)，步骤(2)可得 $m=2^{36}$。并再由此确定 $d=12$。

利用查表次数公式，有实时阶段查表次数是 $D\cdot S\cdot r = 337920$ 次，在使用两块容量为 1 T 每秒随机访问次数是 23 万次的 PCI-E 接口 SSD 卡的情况下，可以达到 1 s 内完成查表，其性能完全满足 2 s 的时间限制。

至此本节得出结论，在 FPGA 平台下利用 32 个 EP4CGX150 芯片进行预计算可以在一个月时间内完成 2 T 大小的数据表，其中数据表是由 2^5 个瘦彩虹表构成，每个瘦彩虹表起点个数为 2^{36}，可辨点中固定串长度是 12 bit，瘦彩虹表中使用了 2^5 个不同的迭代函数；利用 16 个芯片实现成功率是 99%的实时破译计算时间至多 2 s，亦即平均破译时间为 1 s。

5 结束语

本文通过对 A5/1 算法中状态空间缩减性质进行研究，建立了使用可变可辨点的多表瘦彩虹表时空折中攻击模型，并推导出成功率、存储空间和预计算时间、实时破译时间和实时阶段查表次数公式，在各种约束条件限制下利用 FPGA 平台实现了使用 32 个 FPGA 芯片 1 个月内完成 2 T 数据表的运算和使用 16 个 FPGA 芯片实现成功率是 99%的实时破译计算时间至多 2 s，亦即平均破译时间为 1 s。并且使用 FPGA 平台实现本模型的功耗更低，便于实现实时阶段破译。

本时空折中模型各指标的推导和参数确定方法对于其他硬件平台和限制条件下参数的选取有参考价值。

参 考 文 献

[1] GSM Association. GSM World-Home of the GSM

Association. http://www.gsmworld.com/, June 2010.

[2] Golic J. Cryptanalysis of three mutually clock-controlled stop/go shift registers[J]. *IEEE Transactions on Information Theory*, 2000, 46(3): 1081–1090.

[3] Biryukov A, Shamir A, and Wagner D. Real time cryptanalysis of A5/1 on a PC[C]. Proccedings of Eighth Int'l Workshop Fast Software Encryption (FSE 00), New York, 2001: 1–18.

[4] Kumar S, Paar C, Pelzl J, *et al*.. Breaking ciphers with COPACOBANA —— a cost-optimized parallel code breaker [C]. Lecture Notes in Computer Science, 2006, 4249: 101–118.

[5] Nohl K. Attacking phone privacy. ftp://ftp.trinxp. com/ docz/it_tech/blackhat/BlackHat-USA-2010-Nohl-Attacking. Phone. Privacy-wp. pdf, 2010.

[6] Glendrange M, Hove K, and Hvideberg E. Decoding GSM. http://ntnu.diva-portal.org/smash/get/diva2:355716/ FULLTEXT01, June 2010.

[7] Hamdan A and Bartlett H. State space convergence in the A5/1 keystream generator. http://www.spms.ntu.du.sg /Asiacrypt 2010/Rump, Dec 7th 2010.

[8] Hellman M E. A cryptanalytic time-memory trade-off [J]. *IEEE Transactions on Information Theory*, 1980, 26(4): 401–406.

[9] Borst J. Block ciphers: design, analysis and side-channel analysis [D]. [Ph.D. dissertation], Katholieke Universiteit Leuven, 2001.

[10] Avoine G, Junod P, and Oechslin P. Time-memory trade-offs: false alarm detection using checkpoints [C]. Lecture Notes in Computer Science, 2005, 3797: 183–196.

李 磊： 男，1978 年生，博士生，研究方向为密码学与信息安全.

韩文报： 男，1963 年生，博士，教授，博士生导师，研究方向为密码学与信息安全.

王 政： 男，1975 年生，博士，副教授，研究方向为信息安全.