可证明安全性自动化证明方法研究

顾纯祥　祝跃飞　光 焱
(解放军信息工程大学信息工程学院　郑州　450002)

摘　要：可证明安全性是密码协议安全性评估的重要依据，但手写安全性证明容易出错且正确性难以判定。该文论述了基于游戏(Game based)转换的安全性证明及其自动化实现方法，重点论述了基于进程演算的自动化证明方法，并以该方法研究 OAEP+的自动化安全性证明，首次给出了其初始游戏和相关的观察等价式。

关键词：密码协议；可证明安全；自动化证明；进程演算
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)12-3001-05

Researches on Automatic Approach of Provable Security

Gu Chun-xiang　Zhu Yue-fei　Guang Yan
(*Information Engineering College*, *Information Engineering University*, *PLA*, *Zhengzhou* 450002, *China*)

Abstract: Probable security is an important criteria for analyzing the security of cryptographic protocols. However, writing and verifying proofs with hand are prone to errors. This paper introduces the game-based approach of writing security proofs and its automatic technique. It advocates the automatic security proof approach based on process calculus, makes researches on the automatic security proof of OAEP+, and presents it's initial game and observational equivalences for the first time.

Key words: Cryptographic protocols; Probable security; Automatic security proof; Process calculus

1　引言

密码协议安全性评估是协议设计中不可或缺的重要环节。目前，可证明安全性理论[1,2]是学术界广泛接受的密码协议安全性分析方法。可证明安全将攻击者描述为一个概率多项式时间的图林(Turing)机，其目标是赢得针对某一密码协议安全性的攻击游戏(game)；而安全性证明就是要在某些计算假设下，证明攻击者赢得攻击游戏的概率是可以忽略的。可证明安全得到了当前密码学界的广泛认同，但针对一个具体体制的手写安全性证明包括攻击算法构造、运行时间和成功概率的计算，这一过程容易出错，且即使出错也不易发现。由此，一些学者开始寻求利用计算机辅助，对密码协议的可证明安全性进行自动化证明的方法。

2004 年，Shop[3]详细描述了如何使用“游戏序列”来组织安全性证明过程。该方法的基本思想是：以攻击者和挑战者之间进行的攻击游戏形式化刻画对密码协议的攻击过程，如果证明攻击者达到其攻击目标的概率是可忽略的，则协议是安全的；安全性证明从实际攻击游戏开始，对游戏进行一系列小改动构造一个游戏序列，两个相邻游戏或者等价，或者非常接近(接近程度通过概率刻画)，由最后一个游戏可以得到攻击者达到攻击目标的概率的结论。2005 年，Halevi[4]提出利用计算机辅助构造“游戏序列”，进而实现密码协议安全性自动化证明的可行性以及实现思路。此后，基于游戏(Game based)转换的密码协议安全性自动化证明成为学术研究的热点之一。

2007年，Nowak[5]，Affeldt[6]等利用定理证明器Coq对基于游戏序列的密码协议安全性自动化证明的技术进行了一定的研究，但这些证明仍需要大量的人工干预。同年，Blanchet和Pointcheval[7]首次在计算复杂度模型中，基于进程演算提出了对密码协议安全性的自动化实现技术。该工作采用具有概率语义的进程演算形式化描述攻击游戏序列，以基于语法的转换和基于“观察等价(observational equivalence)”的转换刻画的游戏转换的关系，并开发出密码协议安全性自动化证明工具Cryptoverif，但目前该工具可处理的密码协议[7−9]还很有限。

本文介绍了基于游戏演化的密码协议安全性证明及其自动化方法，重点论述了基于进程演算的自动化证明方法，并给出了该方法下 OAEP+[10]的初始游戏和相关的观察等价式。

2008-11-14 收到，2009-09-21 改回
国家863计划项目(2007AA01Z471)和河南省基础与前沿技术研究基金(072300410260)资助课题

2 基于游戏转换的可证明安全性

2.1 可证明安全性

对密码协议及其安全性给予精确的形式化定义，建立相应安全模型，是可证明安全性理论的基础组成部分。不同的密码协议有不同的安全模型，下面以公钥加密体制为例介绍。

对公钥加密体制而言，目前学术界广泛接受的安全性定义是“适应性选择密文攻击下密文不可区分 (IND-CCA2: indistinguishability against adaptive chosen cipher-text attack)”。

定义 1(IND-CCA2) 设 $E=(KGen,Enc,Dec)$ 是一个公钥加密体制，$A=(A_1,A_2)$ 是一个2阶段攻击者(都是概率多项式时间算法)，$O(\cdot)$ 是解密谕示(oracle)，若对任意的A，

$$\mathrm{adv}_A=\left|\Pr\left[A_2^{O(\cdot)}(m_0,m_1,s,y)\right.\right.$$

$$\left.\left.=b\left|\begin{array}{c}(pk,sk)\leftarrow KGen(1^k),\\(m_0,m_1,s)\leftarrow A_1^{O(\cdot)}(pk),\\y=Enc(m_b,pk)\end{array}\right|-\frac{1}{2}\right|$$

是可忽略的，则称是E是IND-CCA2安全的，其中 $|m_0|=|m_1|$ 且 A_2 不能利用解密谕示 $O(\cdot)$ 获取y的明文，s 是攻击者想要保留的信息。

2.2 基于游戏转换的安全性证明

在安全性的定义中，可以把攻击过程形式化为一个攻击游戏。一个典型的游戏是一个攻击者和密码协议提供的一些接口(包括挑战者和可访问的各种谕示)的并发交互系统，通常包含一个或多个循环，循环体称为攻击者例程，由攻击者各种可能的行为组成的。因为攻击者的资源是有限的，因此可以设定游戏的循环次数有上限(达到上限意味着攻击者资源耗尽)。一旦游戏结束，攻击者以游戏的输出作为自己的输出。

随机谕示模型下公钥加密协议的IND-CCA2安全性定义的攻击过程如下：

$(pk,sk)\leftarrow KGen(1^k);(m_0,m_1,s)\leftarrow A_1^{O(\cdot),H(\cdot)}(pk);$

$y\leftarrow Enc(m_b,pk);b'\leftarrow A_2^{O(\cdot),H(\cdot)}(m_0,m_1,s,y);$

若$|\Pr[b=b']-1/2|$是可忽略的，则体制是安全的。

安全性证明通常是一个图林约化过程，通常采用对攻击游戏进行一系列小改动，进而获得一个“游戏序列”$G_0,G_1,\cdots,G_n$来给出证明。G_0是初始的安全性定义中的攻击游戏。令S_i表示G_i中攻击者攻击成功的事件($i=0,1,\cdots,n$)，P 是安全性定义预期的概率(通常是 0 或 1/2)。安全性证明的“游戏序列”构造要满足$|\Pr[S_i]-\Pr[S_{i+1}]|$和$|\Pr[S_n]-P|$都是可以忽略的，从而证明G_0中攻击者攻击成功的概率和预期概率 P 的差距是可以忽略的。

3 基于进程演算的密码协议安全性自动化证明方法

攻击游戏是一个分布式并发系统，使用进程演算可以描述攻击者和密码协议提供的一些接口的并发交互，而概率语义为相邻游戏的攻击者的成功概率变化提供了量化依据。文献[8,9]定义一种进程演算以形式化刻画攻击游戏，本文即以该进程演算作为系统形式化描述语言。

3.1 游戏转换

获取游戏序列的方式主要可分为两类：语法转换和依据密码原语安全性质的转换。

语法转换是利用进程演算的语法性质为依据的转换。如当 x 被定义为 $\mathrm{let}\ x[i_1,\cdots,i_m]:T=M\ \mathrm{in}\ P$，并且 x 没有在 M 中出现，则可以用 M 代替 x。在语法转换中，化简是非常重要的一种，即在游戏转换的过程中，利用特定的信息对描述游戏的进程语句进行简化。简化主要通过两种手段进行，一种是将一个表达式用与其相等的表达式替换；另一种是当一些分之语句的条件不成立时，移除相应的分支。

依据密码原语安全性质的转换是以密码原语的安全性质或安全假设为游戏转换的依据。记$\Pr[Q\rightsquigarrow a]$为进程Q执行的返回结果为a的概率，$\Pr[Q\rightsquigarrow\mathcal{R}]$为进程 Q 严格执行 $\mathcal{R}$ 中的事件序列的概率。

定义 2(观察等价) 两个进程 Q 和Q'是以概率差距 p 观察等价，记为$Q\approx_p Q'$，如果对所有上下文 $C[\ ]$，运行时间 t 和比特串 a，$|\Pr[C[Q]\rightsquigarrow a]-\Pr[C[Q']\rightsquigarrow a]|\le p(t)$，且$\sum_{\mathcal{R}}|\Pr[C[Q]\rightsquigarrow\mathcal{R}]-\Pr[C[Q']\rightsquigarrow\mathcal{R}]|\le p(t)$。

可以证明[7]，若 Q 执行事件 e 的概率上界是p'，$Q\approx_p Q'$，则 Q' 执行事件 e 的概率上界为 $p+p'$。观察等价为构建游戏序列提供了非常有用的依据，利用观察等价式$Q\approx_p Q'$，可以将含有$C[Q]$的游戏G_i转换为含有$C[Q']$的游戏G_{i+1}，同时可以建立转换前后的攻击成功的概率的量化关系。

3.2 可证明安全性的判别条件

在每次游戏转换之后，我们要判别能否给出安全性的结论。对公钥加密体制而言，需要判别的就是 IND-CCA2 游戏中 b 的秘密性。

定义 3(一次会话秘密性 one-session secrecy) 进程 Q 保持 x 的一次会话秘密性，当且$Q|Q_x$

$\approx_0 Q \mid Q'_x$，其中

$Q_x = \text{in}(c_1, (u_1 : T_1, \cdots, u_m : T_m)); \text{if defined}(x[u_1, \cdots, u_m]) \text{ then out}(c_2, x[u_1, \cdots, u_m])$

$Q'_x = \text{in}(c_1, (u_1 : T_1, \cdots, u_m : T_m)); \text{if defined}(x[u_1, \cdots, u_m]) \text{ then new } y : T; \text{out}(c_2, y)$

T_i是$[1, n_m]$类型，信道c_1, c_2不是 Q 的信道，$u_1, \cdots, u_m, y$不是Q中变量，且$x[u_1, \cdots, u_m]$的取值类型为 T。直观地说，就是攻击者不能区分进程是输出了秘密值 x，还是输出了一个随机值 y。对 IND-CCA2 的游戏而言，就是要证明 b 满足一次会话秘密性。可以证明[8]：如果 Q 和 Q'观察等价并且 Q 保持 x 的一次会话秘密性，那么 Q'也保持 x 的这一性质。

4　OAEP＋的初始游戏和相关的观察等价式

4.1 OAEP+体制[10]

设 k 为安全参数，f是作用于$\{0,1\}^k$的单向陷门置换，g是f的逆，k_0, k_1是两个参数满足$k_0 + k_1 < k$且$2^{k_0}, 2^{k_1}$是可忽略的，明文$m \in \{0,1\}^n$，其中$n = k - k_0 - k_1$。$G : \{0,1\}^{k_0} \to \{0,1\}^n$，$H' : \{0,1\}^{n+k_0} \to \{0,1\}^{k_1}$，$H : \{0,1\}^{n+k_1} \to \{0,1\}^{k_0}$为 3 个 Hash 函数。OAEP＋体制的描述如下：

(1)$KGen$：对随机种子 r 获得公钥 $pk = pkgen(r)$和私钥$sk = skgen(r)$。

(2)Enc：输入消息 m，随机选取$x \in \{0,1\}^{k_0}$，计算 $s = (G(x) \oplus m) \,||\, H'(x \,||\, m)$，$t = H(s) \oplus x$，$y = f(s \,||\, t, pk)$，输出密文为 y。

(3)Dec：输入为密文 y，计算$s \,||\, t = g(y, sk)$，$x = H(s) \oplus t$，$m = G(x) \oplus s[0 \cdots n-1]$，$c = s[n \cdots n + k_1 - 1]$。若$c = H'(x \,||\, m)$，则输出明文 m，否则输出密文无效标记$\perp$。其中$s[l_1 \cdots l_2]$表示s的第l_1比特到第l_2比特之间的比特串。

4.2 OAEP+的进程演算的形式化描述

记 T_1, T_2, T_3, T_4 分别为 $\{0,1\}^{k_0}, \{0,1\}^n, \{0,1\}^{k_1}, \{0,1\}^k$ 上随机值类型，T_5为密钥种子类型，则$G : T_1 \to T_2$，$H' : T_1 \times T_2 \to T_3$，$H : T_2 \times T_3 \to T_1$。

在 OAEP＋中，用到的主要密码构件包括单向陷门置换 f，Hash 函数 G，H'和 H，异或$\oplus$运算，这些密码构件的安全性质和假设是安全性证明的主要依据。下面给出随机谕示模型下相关的观察等价式。为了描述方便，在观察等价式的描述中，以$(x_1 : T_1, \cdots, x_k : T_k) \to FP$表示由输入信道输入$(x_1 : T_1, \cdots, x_k : T_k)$并由输出信道输出 FP 运算结果的进程。

(1)单向陷门置换的观察等价式　单向陷门置换 f 是 OAEP＋的核心构件，首先定义攻击者 A 能成功求逆的概率：$\text{Succ}^{\text{OW}}(A) = \Pr\left[x = x' \middle| \begin{matrix} r \leftarrow T_1, (pk, sk) \leftarrow KGen(r), x \leftarrow T_2, \\ y = f(x, pk), x' = A(y, pk) \end{matrix}\right]$。记 $\text{Succ}^{OW}(t)$ 为时间 t 内对任意的攻击者成功求逆的最大概率。为将单向性用于安全性证明，使用下面的观察等价式：

$$
\begin{aligned}
&{}^{i_k \le n_k}\text{new } r : T_5; \\
&(() \to pkgen(r), \\
&\quad {}^{i_f \le n_f}\text{new } x : T_2; \\
&\quad (() \to f(pkgen(r), x) \mid \\
&\quad\quad {}^{i_e \le n_e}(x' : T_1) \to (x' = x) \mid \\
&\quad\quad () \to x)) \\
&\approx_{\text{prob}} \\
&{}^{i_k \le n_k}\text{new } r : T_5; \\
&(() \to pkgen(r) \mid \\
&\quad {}^{i_f \le n_f}\text{new } x : T_2; \\
&\quad (() \to f(pkgen(r), x) \mid \\
&\quad\quad {}^{i_e \le n_e}(x' : T_1) \to \text{find such that defined}(k) \text{ then} \\
&\quad\quad\quad (x' = x) \text{ else false} \mid \\
&\quad\quad () \to \text{let } k : \text{bitstring} = \text{mark in } x))
\end{aligned}
$$

其中 $\text{prob}(t) = n_k \cdot n_f \cdot \text{Succ}^{OW}(t + (n_k n_f - 1)t_f + (n_k - 1)t_{pkgen})$，$t_f$和$t_{pkgen}$分别为$f(\cdot)$和$pkgen(\cdot)$的计算时间。在观察等价式右边，如果 x 被输出过，则 k 被定义过，因此攻击者可以判别$x' = x$是否成立；否则，攻击者对$x' = x$的判别总是输出为 false。

单向函数还有其他一些代数性质可用于安全性证明，如$\forall r : T_1, \forall x : T_2, g(f(x, pkgen(r)), skgen(r)) = x$，等等，这里不再做详细讨论。

(2)Hash 函数的观察等价式　在随机谕示模型下，Hash 函数被假设为完全随机函数。Hash 函数进程对每一次访问，如果是已访问输入，则从访问列表中查找结果并作为应答返回；而对每个新的输入，产生一个随机值作为应答。这一假设以观察等价式形式描述如下：

第一个函数 $G(.)$的观察等价式

$$
\begin{aligned}
&{}^{i_G \le n_G}(x : T_1) \to G(x) \\
&\approx_0 \\
&{}^{i_G \le n_G}(x : T_1) \to \text{find } j \le n_G \text{ such that} \\
&\quad \text{defined}(x[j], r[j]) \wedge (x = x[j]) \text{ then } r[j] \\
&\quad\quad \text{else (new } r : T_1; r)
\end{aligned}
$$

类似地，可以得到函数$H'(\cdot)$和$H(\cdot)$的观察等价式

$$^{i_{H'}\le n_{H'}}(x:T_1,y:T_2)\to H'(x,y)$$
$$\approx_0$$
$$^{i_H\le n_{H'}}(x:T_1,y:T_2)\to \text{find } j\le n_{H'} \text{ such that}$$
$$\text{defined}(x[j],y[j],r[j])\wedge$$
$$((x=x[j])\wedge(y=y[j]))\text{ then } r[j]$$
$$\text{else (new } r:T_1;r)$$
$$^{i_H\le n_H}(x:T_2,y:T_3)\to H(x,y)$$
$$\approx_0$$
$$^{i_H\le n_H}(x:T_2,y:T_3)\to \text{find } j\le n_H \text{ such that}$$
$$\text{defined}(x[j],y[j],r[j])\wedge$$
$$((x=x[j])\wedge(y=y[j]))\text{ then } r[j]$$
$$\text{else (new } r:T_1;r)$$

(3)异或$\oplus$运算的观察等价式

$$^{i_X\le n_X}\text{new } a:T;(x:T)\to a\oplus x$$
$$\approx_0$$
$$^{i_X\le n_X}\text{new } a:T;(x:T)\to a$$

也就是说，对于随机数$a:T$，$a\oplus x$的概率分布和a的概率分布完全相同。

要实现安全性的自动化证明，需要进一步形式化初始攻击游戏。依据 IND-CCA2 的定义，定义以下进程：

(1)3 个 Hash 函数进程

$$\text{let process}\,G$$
$$=^{!i_G\le n_G}(\text{in}(c_1[i_G],x:T_1);\text{out}(c_2[i_G],G(x)))$$
$$\text{let process } H'$$
$$=^{!i_{H'}\le n_{H'}}(\text{in}(c_3[i_{H'}],(x:T_1,y:T_2));\text{out}(c_4[i_{H'}],H'(x,y)))$$
$$\text{let process } H$$
$$=^{!i_H\le n_H}(\text{in}(c_5[i_H],(x:T_2,y:T_3));\text{out}(c_6[i_H],H(x,y)))$$

其中$n_G,n_{H'},n_H$分别为攻击者访问随机谕示$G(\cdot)$, $H'(\cdot)$和$H(.)$的次数上限。

(2)密钥生成进程

$$\text{let process}KGen=$$
$$\text{in(start,());new } r:T_5;$$
$$\text{let } pk=pkgen(r)\text{ in let } sk=skgen(r)\text{ inout}(c_7,pk);$$

(3)解密谕示进程

$$\text{let process}Dec=$$
$$^{!i_D\le q_D}(\text{in}(c_8[i_D],a:T_4);$$
$$\text{find such that defined}(ch)\,\hat{}\,(a=ch)$$
$$\text{then Yield else}$$
$$\text{let } s\,||\,t=g(a,sk)\text{ in}$$
$$\text{let } x=H(s)\oplus t\text{ in}$$
$$m=G(x)\oplus s[0\cdots n-1]\text{ in}$$
$$\text{if } s[n,\cdots n+k_1-1]=H'(x\,||\,m)\text{ then}$$
$$\text{out}(c_9[i_D],m))$$

其中q_D是攻击者访问解密谕示次数的上限。ch在游戏中的含义是挑战密文，Yield 表示终止进程，即攻击者不可以ch作为该进程的输入。

(4)挑战密文生成进程

$$\text{let process}\,T$$
$$=\ \text{in}(c_{10},(m_0:T_2,m_1:T_2));$$
$$\text{new } b:\text{bool};$$
$$\text{let menc}=\text{test}(b,m_0,m_1)\text{ in}$$
$$\text{new } x:T_1;$$
$$\text{let } s_1:T_1=G(x)\oplus\text{menc in}$$
$$\text{let } s_2:T_1=H'(x,\text{menc})\text{ in}$$
$$\text{let } t:T=H(s_1,s_2)\oplus x\text{ in}$$
$$\text{let ch}:T_4=f(s_1\,||\,s_2\,||\,t,pk)\text{ in}$$
$$\text{out}(c_{11},ch);$$

其中，函数$\text{test}(b:\text{bool},x:T_2,y:T_2)$定义为对任意的$x:T_2,y:T_2$，$\text{test}(\text{true},x,y)=x$；$\text{test}(\text{false},x,y)=y$；

依据 2.2 节对 IND-CCA2 的定义，首先系统启动密钥生成进程 process$KGen$，该进程和后续processDec和process$T$是串行关系。在后续攻击中，攻击者最多访问q_D次解密谕示，并在某个时间上运行一次挑战密文生成进程，因此 processDec 和process$T$是并行关系。在随机谕示模型下，攻击者在任何时间都可以访问随机谕示。因此，将上述进程合成，可以得到随机谕示模型下 OAEP+的初始游戏：

(5)初始游戏

$$\text{process } G_0$$
$$=\text{process}\,G\mid\text{process}H'\mid\text{process}H\mid$$
$$(\text{process}KGen;(\text{process}Dec\mid\text{process}\,T))$$

5 结论

本文介绍基于游戏(Game based)转换的安全性证明及其自动化实现方法，重点论述了基于进程演算的自动化证明方法。目前该领域还是个较新的研究方向，可处理的密码算法和安全协议的范围还很有限，其进程的重写规则(观察等价式)和转换策略也有待深入研究。

参 考 文 献

[1] Bellare M. Practice-oriented provable security. Lecture Notes in Computer Science, 1997, 1396: 221–231.

[2] 冯登国. 可证明安全性理论与方法研究, 软件学报, 2005, 16(10): 1743−1756.
Deng-Guo F. Research on theory and approach of provable security. *Journal of Software*, 2005, 16(10): 1743−1756.

[3] Shoup V. Sequences of games: a tool for taming complexity in security proofs, Cryptology ePrint Archive 2004/332. http://eprint.iacr.org/2004/332. May 2004.

[4] Halevi S. A plausible approach to computer-aided cryptographic proofs. Cryptology ePrint Archive, Report 2005/181, http://eprint.iacr.org/2005/181. June 2005.

[5] Nowak D. A framework for game-based security proofs. Lecture Notes in Computer Science, 2007, 4861: 319−333.

[6] Affeldt R, Tanaka M, and Marti N. Formal proof of provable security by game-playing in a proof assistant. Lecture Notes in Computer Science, 2007, 4784: 151−168.

[7] Blanchet B and Pointcheval D. Automated security proofs with sequences of games. Lecture Notes in Computer Science, 2006, 4117: 537−554.

[8] Blanchet B. A computationally sound mechanized prover for security protocols. *IEEE Transactions on Dependable and Secure Computing*, 2008, 5(4): 193−207.

[9] Blanchet B and Chaudhuri A. Automated formal analysis of a protocol for secure file sharing on untrusted storage. IEEE Symposium on Security and Privacy, Oakland, CA, May 2008: 417−431.

[10] Shoup V. OAEP reconsidered. Lecture Notes in Computer Science, 2002, 2139: 239−259.

顾纯祥： 男，1976年生，博士，研究方向为密码学与信息安全.

祝跃飞： 男，1962 年生，教授，博士生导师，研究领域为密码学、网络与信息安全.

光 焱： 男，1981年生，博士生，研究方向为密码学与信息安全.