信息安全中语义安全性定义及其对等性证明

胡 若 钱省三
(上海理工大学管理学院 上海 200093)

摘 要 介绍了语义安全性的定义,并且从框架的对比来分析语义的安全性,以整合语义安全性、不可区分性和不可扩展安全性的框架,这种方式有助于研究不同攻击模型之间的关系。在对照的基础上对不可区分性的定义做了部分调整。研究了在新的框架下如何证明语义安全性和不可区分性两者间的对等性。简化了语义安全性与不可区分性之间的等价性证明。

关键词 信息安全,语义框架,信息空间,加密,对等性
中图法分类号 TP393 **文献标识码** A

Definition and Equation Proof of Semantic Security in Information Security

HU Ruo QIAN Xing-san
(School of Management, University of Shanghai for Science Technology, Shanghai 200093, China)

Abstract Our definition of semantic security was introduced, and we tried to integrate the frameworks of definitions of semantic security, non-distinguishability and non-expandability by analysing semantic security in comparison based framework. This facilitates the study of relations among these goals against different attack models, and we made a slightly modified definition of classifying based on comparison and then we studied our proof of equation of semantic security and classifying in the new framework. This way makes the proof of the equation of semantic security and non-distinguishability easier and more understandable.

Keywords Information security, Semantic frame, Information space, Encryption, Equation

1 引言

公钥密码体制的安全性可通过语义安全性、不可区分性、不可扩展安全性、明文可意识性等加密效果来评估。本文主要论述语义安全性和不可区分性,其最早定义见文献[5]。不可区分性又称为多项式安全性或 Goldwasser-Micali 安全性。简言之,不可区分性即描述了敌方不可区分两份明文(其中一份明文已加密)的形式化表示。这项研究有重要的实用价值,同时还为评估环境的安全提供了一种可行之策。另一方面,如果无法找出多项式的有界信息,无法从特定密文中提取任何明文信息,则从语义上说这种加密是安全的。因此,语义安全性是保密性的直接决定因素。相对 Shannon 的绝对安全[7]理论,可将语义安全性视作计算版本的绝对安全性。不同于不可区分性,语义安全性并不涉及任何安全评估方法。

语义安全性定义中,"信息"可通过信息空间 Σ^* 中的各种函数加以构造,其中 Σ 为计算模型的字母。如果可以证明没有函数适用于这种加密系统,即可证明该加密系统具有不可区分性。不可区分性与语义安全性两者之间的等价性关系首见文献[5]。文献[5]对语义安全性的最初定义中,并未对明文信息构造函数的可计算性施加任何限制。如文献[6]所述,如果无法验证所猜测的函数是否正确,则"猜测"函数法不可行。对语义安全性进行公式化的过程中,用于构造"信息"的函数必须具有多项式可变性[8]。

文献[1]中介绍了另一种重要观点。Bellare 等建议:在研究加密对象时,应结合具体的攻击模型加以研究,而不宜做孤立的研究。在文献[1]中使用这种方式对选择明文攻击、非适应性选择密文攻击和适应性选择密文攻击的不可区分性——语义安全性的关系进行了讨论。

可在两种不同框架下对语义安全性进行形式化表示,这两种形式化分别是基于模拟器的定义和基于对照的定义。基于模拟器的定义:针对具有密文的任何敌方,存在一个称为'多项式时间算法'的模拟器。该模拟器在无需获取密文和敌方情况的前提下即可成功发动攻击(如提取重要信息等)。基于对照的定义:与只能通过随机猜测获取信息的情况相比,具有密文的敌方没有任何优势。因为随机猜测属于一种特殊模拟,基于对照的定义可能比基于模拟器的定义更加可靠。另一方面,基于模拟器的定义对敌方希望提取的部分信息的可计算性无任何限制,敌方希望提取基于对照的部分信息。操作中,通过 pol-time 算法生成和评估这部分信息。研究表明:基于模拟器的定义,其强大性优于基于对照的定义。

文献[1]中,在基于对照的框架中定义了不可扩展安全性。此前在文献[3,4]中,通过模拟器对不可扩展安全性进行了定义。除文献[1]中提出的区别外,这两种定义方式在其他方面是完全一致的。文献[8]在基于模拟器的基础上定义了

到稿日期:2010-12-14 返修日期:2011-02-23 本文受国家自然基金项目(10771039),国家科技部创新基金项目(07C26216402072)资助。
胡 若(1968-),男,博士,副教授,主要研究方向为网络信息系统,E-mail:hu68@163.com。

语义安全性。在上述某些情况下使用该定义的结论，则会使语义安全性和不可区分性的等价性证明难度增加。并且，证明该框架中语义安全性和不可区分性之间的等价性需要定义不可分割性，这种不可分割性是人为制订的安全对象，以便统一该定义框架。

本文援引了文献[1]的思想，在基于对照的框架中定义了语义安全性，并分别以适应性选择明文攻击(CPA)、非适应性选择密码攻击(CCA1)和适应性选择密文攻击(CCA2)等3种攻击为对象研究了语义安全性和不可区分性之间的关系。最后，本文提出一种更为简单易懂的方式来证明语义安全性和不可辨识性之间的对等性。

若某加密系统在适应性选择密文的攻击下不具有可扩展性，则该加密系统在遇到选择明文攻击时，从语义角度考虑是安全的。第2节介绍了部分基础性定义；第3节介绍了语义安全性的定义，并在对照的基础上对不可区分性的定义做了部分调整；第4节研究了在新的框架下如何证明语义安全性和不可区分性两者间的对等性。

2 初步定义

2.1 多项式可变函数

如果存在概率 poly-tim 算法 A 满足下列条件，则该函数 $f:M\to\Sigma^*$ 为多项式可变函数。

$\forall x\in M:A(x,f(x))=1$ 且 $y\neq f(x)\Rightarrow A(x,y)=0$

该定义中，M 为信息空间，Σ^* 代表全部明文信息。

2.2 可略去函数

如满足下列两个条件，则函数：$N\to R$ 为可略去函数。

(1) $\forall n\in N:\varepsilon(n)\geqslant 0$

(2) $\forall c\geqslant 0\ \exists k_c\ni\forall k\geqslant k_c\varepsilon(k)<k^{-c}$

公钥加密方案　公钥加密方案 $\Pi=(K,E,D)$ 涉及3种算法：

(1)密钥生成算法 K 为一种概率多项式时间算法，输入为安全参数 $k\in N$，输出为匹配的公钥和密钥对 (pk,sk)；

(2)加密算法 E 为概率多项式时间算法，输入为公钥 pk 和信息 $x\in\{0,1\}^*$，输出为密文 y；

(3)解密算法 D 为确定性多项式时间算法，输入为密钥 sk 和密文 y，输出为 $x\in\{0,1\}^*$ 信息，当无法对密文 y 进行合法解密时，则输出特殊符号 o。

2.3 敌方模型

用一对概率多项式时间算法 $A=(A_1,A_2)$ 对敌方建模，每种算法的具体用途取决于特定敌对对象。一般而言，在第一阶段通过公钥 A_1 寻找特定的敌方公钥，并输出测试实例；在第二阶段，根据具体对象采用密文 y 作为测试实例的概率函数，对敌方进行攻击。此外，A_1 还会输出部分状态信息，这些状态信息随后传至 A_2。如能突破攻击，则证明敌方算法 $A=(A_1,A_2)$ 奏效。

在选择明文攻击(CPA)时，敌方可对任何明文进行加密。在非适应选择密文攻击(CCA1)中，我们给出 A_1(公钥)，允许其访问解密 oracle，但禁止 A_2 访问解密 oracle。因此，解密 oracle 可用于产生测试实例，但在攻击前需将其消除。在适应性选择密文攻击(CCA2)中，我们继续为 A_1 提供公钥，并允许其访问解密 oracle，允许 A_2 访问相同解密 oracle，仅限制攻击密文查询。

3 对象定义

3.1 基于对照的语义安全性

将 $A=(A_1,A_2)$ 视作攻击加密方案 $\Pi=(K,E,D)$ 的敌方。在攻击的第一阶段，敌方使用公钥 pk 作为算法 A_1 的输入，输出(M,s)。其中，首元素为可在多项式时间中取样的信息空间，第二元素为需要从 A_1 传至 A_2 的任何信息。接着通过 E_{pk} 选择和加密满足 $x\in M$ 的随机信息，以生成密文 y。在攻击的第二阶段，将报文空间、状态信息和攻击密文(M,s,y)作为算法 A_2 的输入，输出(v,f)；再根据输入到 A_2 中的信息，借助随机算法选择满足 $x\in M$ 的随机数。如所选 x 满足等式 $v=f(x)$，则取样算法可行。如果敌方成功且取样算法 k 的函数、安全参数是可略去函数，则在 CSS_ATK 下，$\Pi=(K,E,D)$ 属于安全加密方案。

在正式设置中，将 $\Pi=(K,E,D)$视作加密方案，$A=(A_1,A_2)$为多项式有界的敌方。对 $atk\in\{cpa,cca1,cca2\}$和 $k\in N$，我们定义了实验 $Exp^{css-atk-1}_{\Pi,A,Sample}(k)$和 $Exp^{css-atk-0}_{\Pi,A,Sample}(k)$，两种实验具体如下：

$Exp^{css-atk-1}_{\Pi,A,Sample}(k)$

$(pk,sk)\leftarrow K(k);(M,s)\leftarrow A_1^{O_1(\cdot)}(pk);x\leftarrow M;y\leftarrow E_{pk}(x);$

$(v,f)\leftarrow A_2^{O_2(\cdot)}(M,s,y);$

if $v=f(x)$ then $d\leftarrow 1$

else $d\leftarrow 0;$

return d

$Exp^{css-atk-0}_{\Pi,A,Sample}(k)$

$(pk,sk)\leftarrow K(k);(M,s)\leftarrow A_1^{O_1(\cdot)}(pk);x\leftarrow Sample(M,s);$

$(v,f)\leftarrow A_2^{O_2(\cdot)}(M,s);$

if $v=f(x)$ then $d\leftarrow 1$

else $d\leftarrow 0;$

return d

对于任意 x，针对 $x'\in M$ 存在$|x|=|x'|$；敌方 A 中的 oracle 可访问加密 oracle，具体过程如下：

if $atk=cpa$ then $O_1(\cdot)=\varepsilon$ and $O_2(\cdot)=\varepsilon$

if $atk=cca1$ then $O_1(\cdot)=D_{sk}(\cdot)$ and $O_2(\cdot)=\varepsilon$

if $atk=cca2$ then $O_1(\cdot)=D_{sk}(\cdot)$ and $O_2(\cdot)=D_{sk}(\cdot)$

$atk=cca2$ 时，A_2 不得请求对攻击密文 y 进行解密。

敌方优势 $Adv^{css-atk}_{\Pi,A,A'}(k)$定义为：

$$Adv^{css-atk}_{\Pi,A,Sample}(k)=\Pr\left[Exp^{css-atk-1}_{\Pi,A,Sample}(k)=1\right]-\Pr\left[Exp^{css-atk-0}_{\Pi,A,Sample}(k)=1\right]$$

在 CSS_ATK 下，如果 $\forall A\ \exists S:Adv^{css-atk}_{\Pi,A,Sample}(k)$可略去，则 $\Pi=(K,E,D)$属于安全的公钥加密方案。

可以通过下列实验将上述两种实验统一化：

针对 $atk\in\{cpa,cca1,cca2\},b\in\{0,1\}$以及 $k\in N$，做如下定义：

$Exp^{css-atk-b}_{\Pi,A,Sample}(k)$

$(pk,sk)\leftarrow K(k);(M,s)\leftarrow A_1^{O_1(\cdot)}(pk);x_1\leftarrow M;y\leftarrow E_{pk}(x_1);x_0\leftarrow Sample(M,s);$

$(v,f)\leftarrow A_2^{O_2(\cdot)}(M,s,y);$

if $v=f(x_b)$ then $d\leftarrow 1;$

else $d\leftarrow 0;$

return d

3.2 不可分辨性

$\Pi=(K,E,D)$为加密方案，$A=(A_1,A_2)$为多项式有界的敌方。对于$atk\in\{cpa,cca1,cca2\}$，$b\in\{0,1\}$以及$k\in N$，定义$Exp_{\Pi,A}^{ind-atk-b}(k)$如下：

$Exp_{\Pi,A}^{ind-atk-b}(k)$

$(pk,sk)\leftarrow K(k);(x_0,x_1,s)\leftarrow A_1^{O_1(\cdot)}(pk);y\leftarrow E_{pk}(x_b);$

$d\leftarrow A_2^{O_2(\cdot)}(x_0,x_1,s,y);$

return d

式中，对于任意x，针对$x'\in M$存在$|x|=|x'|$；敌方A中的oracle可访问解密oracle，具体如下：

if $atk=cpa$ then $O_1(\cdot)=\varepsilon$ and $O_2(\cdot)=\varepsilon$

if $atk=cca1$ then $O_1(\cdot)=D_{sk}(\cdot)$ and $O_2(\cdot)=\varepsilon$

if $atk=cca2$ then $O_1(\cdot)=D_{sk}(\cdot)$ and $O_2(\cdot)=D_{sk}(\cdot)$

$atk=cca2$时，A_2不得请求对攻击密文y进行解密。敌方优势在于其正确猜测的标准，定义为输出正确I和错误I的概率差。在对敌方优势进行形式设定时，定义如下：

$$Adv_{\Pi,A}^{ind-atk}(k)=\Pr[Exp_{\Pi,A}^{ind-atk-1}(k)=1]-\Pr[Exp_{\Pi,A}^{ind-atk-0}(k)=1]$$

如满足下列要求，则在CSS_ATK下，$\Pi=(K,E,D)$公钥加密方案是安全的：

$\forall A\quad Adv_{PE,A}^{ind-atk}(k)$可忽略。

4 语义安全性和不可区分性之间的对等性

定理 1 当且仅当任何攻击$ATK\in\{CPA,CCA1,CCA2\}$从IND_ATK意义上讲是安全的，则在CSS_ATK下，$\Pi=(K,E,D)$公钥加密方案是安全的。

证明：首先证明法则的假设部分，即CSS_ATK⇒IND_ATK：假设从CSS_ATK意义上说，$\Pi=(K,E,D)$是安全的公钥加密方案，但从IND_ATK意义上说，其并非是安全的公钥加密方案。根据不可分辨性（见第3节）的定义，存在多项式时间敌方$A=(A_1,A_2)$，可以从信息空间中区分某些明文的密文。使用$A=(A_1,A_2)$作为子程序，可以构建多项式时间敌方$B=(B_1,B_2)$，该对象可以从对应的密文中提取某些重要信息。构造B很简单；每个可以区分密文$x_0,x_1\in M$的多项式时间算法将会对下列函数值进行预测：

$f:\{x_0,x_1\}\rightarrow\{0,1\}$

$$f(x)=\begin{cases}0, & \text{if } x=x_0\\ 1, & \text{if } x=x_1\end{cases}$$

敌方$B=(B_1,B_2)$可正式定义如下：

$B_1^{O_1(\cdot)}(pk)$

$(x_0,x_1,s)\leftarrow A_1^{O_1(\cdot)}(pk);M\leftarrow\{x_0,x_1\};$

return(M,s)

$B_2^{O_2(\cdot)}(M,s,y)$

$d\leftarrow A_2^{O_2(\cdot)}(x_0,x_1,s,y);v\leftarrow d$

$f:\{x_0,x_1\}\rightarrow\{0,1\}$

$$f(x)=\begin{cases}0, & \text{if } x=x_0\\ 1, & \text{if } x=x_1\end{cases}$$

return(v,f)

A_1和A_2均为多项式时间算法，因此设为B_1和B_2。

$p(b)$和$p(b')$定义如下：

$$\begin{aligned}p(b)&=\Pr[(pk,sk)\xleftarrow{R}K(k);(M,s)\leftarrow A_1^{O_1(\cdot)}(pk);x_1\leftarrow M;y\leftarrow E_{pk}(x_1);x_0\leftarrow Sample(M,s);(v,f)\leftarrow A_2^{O_2(\cdot)}(M,s,y);v=f(x_b)]\\&=\Pr[(pk,sk)\xleftarrow{R}K(k);(M,s)\leftarrow A_1^{O_1(\cdot)}(pk);x_1\leftarrow M;y\leftarrow E_{pk}(x_1);x_0\leftarrow Sample(M,s);(v,f)\leftarrow A_2^{O_2(\cdot)}(M,s,y);v=f(x_1)]\\p'(b)&=\Pr[(pk,sk)\xleftarrow{R}K(k);(x_0,x_1,s)\leftarrow A_1^{O_1(\cdot)}(pk);y\leftarrow E_{pk}(x_b);d\leftarrow A_2^{O_2(\cdot)}(x_0,x_1,s,y);d=1]\end{aligned}$$

函数f为确定性函数，$v=f(x_1)$与$d=1$的概率相等。因此，$p(b)$和$p'(b)$相等，根据敌方优势定义，得出：

$$\begin{aligned}Adv_{\Pi,A}^{css-atk}(k)&=p(1)-p(0)=p'(1)-p'(0)\\&=Adv_{\Pi,A}^{ind-atk}(k)\end{aligned}$$

所以，当$Adv_{\Pi,A}^{ind-atk}(k)$并非可省略函数时，两者都不是$Adv_{\Pi,A}^{css-atk}(k)$。

下面再证明该理论的另一部分，即IND_ATK⇒CSS_ATK：

依然采用归谬法进行证明。

假设$B=(B_1,B_2)$为攻击机密系统语义对象的敌方，则可以从其对应的密文所对应的明文中提取部分重要信息。构造敌方$A=(A_1,A_2)$，通过$B=(B_1,B_2)$子程序攻击机密系统的不可分辨性对象。敌方$A=(A_1,A_2)$定义如下：

$A_1^{O_1(\cdot)}(pk)$

$(M,s)\leftarrow B_1^{O_1(\cdot)}(pk);x_0,x_1\leftarrow M;$

return(x_0,x_1,s)

$A_2^{O_2(\cdot)}(x_0,x_1,s,y)$

$(v,f)\leftarrow B_2^{O_2(\cdot)}(M,s,y);$

if $v=f(x_0)$ then $d\leftarrow 0;$

if $v=f(x_1)$ then $d\leftarrow 1;$

else $d\xleftarrow{R}\{0,1\};$

return d

如果函数f为多项式可变函数，则在算法A_1和A_2多项式时间范围内运行。对$b\in\{0,1\}$，定义$p(b)$和$p'(b)$：

$$\begin{aligned}p(b)&=\Pr[(pk,sk)\xleftarrow{R}K(k);(x_0,x_1,s)\leftarrow A_1^{O_1(\cdot)}(pk);y\leftarrow E_{pk}(x_b);d\leftarrow A_2^{O_2(\cdot)}(x_0,x_1,s,y);d=1]\\p'(b)&=\Pr[(pk,sk)\xleftarrow{R}K(k);(M,s)\leftarrow A_1^{O_1(\cdot)}(pk);x_1\leftarrow M;y\leftarrow E_{pk}(x_1);x_0\leftarrow Sample(M,s);(v,f)\leftarrow A_2^{O_2(\cdot)}(M,s,y);v=f(x_b)]\\&=\Pr[(pk,sk)\xleftarrow{R}K(k);(M,s)\leftarrow A_1^{O_1(\cdot)}(pk);x_1\leftarrow M;y\leftarrow E_{pk}(x_1);x_0\leftarrow Sample(M,s);(v,f)\leftarrow A_2^{O_2(\cdot)}(M,s,y);v=f(x_1)]\end{aligned}$$

下列情况下算法A_1的输出值I：

如果$v=f(x_1)$且$v\neq f(x_0)$，则输出值必然为I；

如果$v\neq f(x_1)$且$v\neq f(x_0)$，则输出值为I，概率为$I/2$；

从而得出：

$$\begin{aligned}p(1)&=p'(1)(1-p'(0))+\frac{1}{2}(p'(1)p'(0)+(1-p'(1))(1-p'(0)))\\&=\frac{1}{2}+\frac{1}{2}(p'(1)-p'(0))\end{aligned}$$

因而有

$$Adv_{\Pi,A}^{ind-atk}(k)=p(1)-p(0)=2p(1)-1=p'(1)-p'(0)$$
$$=Adv_{\Pi,A}^{css-atk}(k)$$

当 $Adv_{\Pi,A}^{css-atk}(k)$ 并非可省略函数时，则有 $Adv_{\Pi,A}^{ind-atk}(k)$。

结束语 在基于对照的框架下对语义安全性进行了形式化表示。统一了语义安全性、不可分辨性的定义框架，针对选择明文攻击、非适应选择密文攻击和适应性选择密文攻击，提供了研究不可分辨性和语义安全性关系的简化表示。接着给出了在新条件下对语义安全性和不可分辨性之间对等性的简单证明。与前述证明相比，这种证明更为简洁易懂，无需定义不可分割性等任何中间对象，即可实现定义框架的统一。

参 考 文 献

[1] Bhatt M, Flahive A, Wouters C, et al. Move: a distributed framework for materialized ontology view extraction[J]. Algorithmica, 2006, 45(3): 457-481

[2] Chandrasekaran B, Josephson J R, Benjamins V R. What are ontologies, and why do we need them? [J]. IEEE Intelligent Systems, 1999, 14(1): 20-26

[3] Wouters C, Dillon T, Rahayu W, et al. Ontologies on the move [C] // Database Systems for Advanced Application. LNCS, Springer Verlag, 2004: 812-823

[4] Bhatt M, Flahive A, Wouters C, et al. A distributed approach to sub-ontology extraction [C] // Advanced Information Networking and Applications (AINA'04). IEEE Society, Japan, 2004: 636-641

[5] Flahive A, Apduhan B O, Rahayu W, et al. Simulating the distributed ontology framework in the semantic grid environment with gridSIM[C] // The 2006 International Conference on Parallel and Distributed Processing Techniques and Applications. CSREA Press, Las Vegas, Nevada, USA, 2006: 717-723

[6] De Roure D, Jennings N, Shadbolt N. The semantic grid: a future e-science infrastructure[C] // Berman F, Hey A J, Fox G, eds. Grid Computing, ch 17. Wiley, 2003: 437-470

[7] Taniar D, Rahayu W. Parallel sort-merge object-oriented collection join algorithms[J]. Computer Systems Science and Engineering, 2002, 17(3): 145-158

[8] Flahive A, Apduhan B O, Rahayu J W, et al. Validating the distributed ontology framework for deployment onto the semantic grid environment[C] // The IEEE International Conference on Parallel and Distributed Systems ICPADS. IEEE Computer Society, 2005(2): 684-688

(上接第 30 页)

[72] Barbera R, Re P L, Sava G, et al. Grid monitoring with NetSaint [R]. Italy: Università di Catania and Istituto Nazionale di Fisica Nucleare (INFN), Italy, 2002

[73] Sailer R, Valdez E, Jaeger T, et al. sHyper: Secure Hypervisor Approach to Trusted Virtualized Systems[R]. Yorktown Heights, New York: IBM Thomas J. Watson Research Center, 2005

[74] Murray D G, Milos G, Hand S. Improving Xen Security through Disaggregation[C] // The 4th ACM SIGPLAN/SIGOPS international conference on virtual execution environments. Seattle, Washington, USA, 2008: 151-160

[75] Seshadri A, Luk M, Qu Ning, et al. SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes [C] // The 21th ACM SIGOPS Symposium on Operating Systems Principles. Stevenson, WA, USA, 2007: 335-350

[76] Wang Zhi, Jiang Xuxian, Cui Weidong, et al. Countering Kernel Rootkits with Lightweight Hook Protection [C] // The 16th ACM Conference Computer and Communications Security. Chicago, USA, 2009: 545-554

[77] Payne B D, Carbone M, Sharif M, et al. Lares: An Architecture for Secure Active Monitoring Using Virtualization [C] // The IEEE Symposium on Security and Privacy. Oakland, California, USA, 2008: 233-247

[78] Sharif M, Lee Wenke, Cui Weidong, et al. Secure In-VM Monitoring Using Hardware Virtualizaiton[C] // The 16th ACM Conference on Computer and Communications Security. Chicago, IL, USA, 2009: 477-487

[79] Liu Qian, Weng Chu-liang, Li Ming-lu, et al. An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds[J]. IEEE Security & Privacy, 2010, 8(6): 56-62

[80] Reimer D, Thomas A, Ammous G, et al. Opening black boxes: Using semantic information to combat virtual machine image sprawl[C] // The 2008 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments. Seattle, Washington, USA, March 2008: 111-120

[81] Pfaff B, Garfinkel T, Rosenblum M. Virtualization Aware File Systems: Getting Beyond the Limitations of Virtual Disks[C] // The 3rd Symposium on Networked Systems Design & Implementation. San Jose, California, USA, 2006: 353-366

[82] Sailer R, Zhang Xiaolan, Jaeger T, et al. Design and implementation of a TCG-based integrity measurement architecture[C] // The 13th conference on USENIX Security Symposium. San Diego, CA, USA, 2004: 16-32

[83] Trusted Computing Group. PC client specific TPM interface specification (TIS) [R]. Version 1.2, Trusted Computing Group, July 2005

[84] Shi E, Perrig A, Doorn L V, et al. BIND: Fine-grained Attestation Service for Secure Distributed Systems [C] // The 2005 IEEE Symposium on Security and Privacy. Oakland, California, USA, 2005: 154-168

[85] Jaeger T, Sailer R, Shankar U. PRIMA: Policy-Reduced Integrity Measurement Architecture[C] // The 11th ACM symposium on access control models and technologies. Tahoe City, CA, USA, 2006: 19-28

[86] Korthaus R, Sadeqhi A R, Stüble C. A Practical Property-based Bootstrap Architecture[C] // The 2009 ACM workshop on Scalable trusted computing. Hyatt Regency Chicago, IL, USA, 2009: 29-38

[87] McCune J M, Parno B J, Perrig A. Flicker: An Execution Infrastructure for TCB Minimization[C] // The 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems. Glasgow, Scotland, UK, 2008: 315-328

[88] Berger S, Cáceres R, Goldman K A, et al. vTPM: virtualizing the trusted platform module[C] // The 15th Conference on USENIX Security Symposium. Vancouver, B. C., Canada, 2006: 305-320

[89] Kong Jinzhu. A Practical Approach to Improve the Data Privacy of Virtual Machines[C] // the 10th International Conference on Computer and Information Technology. Bradford, UK, 2010: 936-941