doi:10.11959/j.issn.1000-436x.2015116

WSN 中基于乱序多项式对偶密钥的攻击方案

王爱文[1,2]，温涛[1,3]，张永[3]，朱奉梅[4]，吴镝[1]

（1. 东北大学 软件中心，辽宁 沈阳 110819；2. 沈阳化工大学 计算机科学与技术学院，辽宁 沈阳 110142；
3. 大连东软信息学院 计算机科学与技术系，辽宁 大连 116023；4. 辽宁金融职业学院 信息技术系，辽宁 沈阳 110122）

摘 要：针对 Guo 等的 WSN 中基于乱序对称多项式的对偶密钥方案提出一种攻击方案。通过构造黑盒的方式，对多项式进行攻击，通过整体求解多项式集合，而不是求解单个多项式的方式，使多项式的排列顺序在多项式的破解中失去作用，从而实现乱序多项式的破解。定理证明和实例分析表明 Guo 等的方案不能抵御大规模节点俘获攻击，未能突破多项式的容忍门限，是一种不安全的方案。

关键词：无线传感器网络；对偶密钥；多项式；攻击；黑盒

中图分类号：TP393 **文献标识码**：A

Attacking scheme against the permutation-based multi-polynomial scheme for pair-wise key establishment in wireless sensor networks

WANG Ai-wen[1,2], WEN Tao[1,3], ZHANG Yong[3], ZHU Feng-mei[4], WU Di[1]

(1.Software Center, Northeastern University, Shenyang 110819, China;
2.College of Computer Science and Technology, Shenyang University Chemical Technology, Shenyang 110142, China;
3. Department of Computer Science and Technology, Dalian Neusoft University of Information, Dalian 116023, China;
4. Department of Information Technology, Liaoning Finance Vocational College, Shenyang 110122, China)

Abstract: An attacking scheme was proposed against the permutation-based multi-polynomial scheme proposed by Guo, *et al* for pair-wise key establishment in wireless sensor networks. Attacks on polynomials were carried out by constructing a black-box to integrally solve the set of polynomials rather than a single polynomial. The results show that this scheme can break the symmetric polynomials and make the permutation of polynomials lose its function. The proven theorems and instance analysis indicate that the scheme proposed by Guo, *et al* can't frustrate the large-scale node capture attack and can't break the tolerance threshold of polynomials. Therefore , the scheme is insecure.

Key words: WSN; pair-wise key establishment; polynomial; attack; black-box

1 引言

随着无线传感器网络(WSN, wireless sensor networks)技术的不断发展，无线传感器网络已广泛应用到医疗、军事、环境监测等领域[1]。由于无线传感器节点通常部署在敌对环境中，容易遭受各种恶意攻击，而医疗、军事等关键性应用又要求无线传感器网络通信链路是安全的、可靠的[2]，因此解决无线传感器网络的安全问题是使其进一步推广和应用的前提和基石。

为了加强无线传感器网络的安全性，许多人提出了认证机制和密钥管理方案，特别是对偶密钥管理(PKM, pair-wise key management)技术的发展，为无线传感器网络安全技术的发展奠定了坚实基础，也逐渐成为无线传感器安全技术的核心，因而得到了广泛的关注和研究。根据节点密钥分配方法的不同，无线传感器网络对偶密钥管理方案可分为随机对偶密钥管理方案与确定对偶密钥管理方案两大类。

收稿日期：2014-04-02；**修回日期**：2015-05-18

基金项目：国家自然科学基金资助项目（61170168, 61170169）；辽宁省教育厅科学技术基金资助项目（L2013517）；大连市科技计划基金资助项目（2013A16GX115）

Foundation Items: The National Natural Science Foundation of China(61170168, 61170169); The Science Foundation of Liaoning Education Ministry (L20130517); The Foundation of Dalian Scientific and Technical Planning Project(L2013A16GX115)

Eschenauer 等[3]于 2002 年首次提出了基于随机密钥池的随机对偶密钥管理方案（E-G 方案），随后 Chan 等[4]在 E-G 方案的基础上提出了 Q-Composite 方案，在 E-G 方案和 Q-Composite 方案的启发下，此后出现了大量的随机对偶密管理方案[5~7]。这些都是随机对偶密钥管理方案，在这些方案中，节点的密钥链（key ring）通过随机方式获取，如从一个大密钥池里随机选取一部分密钥，或从多个密钥空间里随机选取若干个密钥空间。

1984 年，Blom[8]提出的密钥预分配协议可以使无线传感器网络中任意 2 个传感节点建立对偶密钥（Blom 方案）。1993 年，Blundo 等[9]在 Blom 方案的基础上提出一种基于对称多项式的密钥预分配方案，当选取的多项式为二元对称多项式（BSP，bivariate symmetric polynomial）时可用于无线传感器网络对偶密钥的建立。此后，Yu 等[10]提出了基于扰动矩阵的密钥管理方案，Zhang 等[11]提出了基于扰动的(RPB, random perturbation-based)多项式密钥管理方案，Guo 等[12]提出了基于乱序多项式多项式(PMP, permutation-based multi-polynomial)密钥管理方案。这些都是确定对偶密钥管理方案，在这些方案中，密钥链是以确定方式获取的，如使用地理信息或使用对称多项式等。

从连通概率的角度，随机对偶密钥管理的密钥连通概率介于 0 和 1 之间，而确定对偶密钥管理的连通概率总为 1。随机对偶密钥管理方案的优点是密钥分配简便，节点的部署方式不受限制；缺点是密钥的分配具有盲目性，节点可能存储一些无用的密钥而浪费存储空间。确定对偶密钥管理方案的优点是密钥的分配具有较强的针对性，节点的存储空间利用较好，任意 2 个节点可以直接建立通信密钥；缺点是特殊的部署方式会降低灵活性，或密钥协商的计算和通信开销较大。

在上述确定对偶密钥管理方案中，基于对称多项式的管理方案具有较好的性能，但其存在容忍门限，不能应对大规模节点俘获攻击，Zhang 等[11]提出了基于扰动的多项式密钥管理方案，在突破容忍门限做出了尝试。遗憾的是，Albrecht 等[13]对文献[11]引入扰动的方案进行攻击，证明了其并不能打破容忍门限，所以不能解决大规模节点共谋攻击问题。而 Guo 等[12]提出了基于乱序多项式的多项式密钥管理方案，通过增加多项式重构的难度来应对多项式的攻击，再一次证明了突破多项式容忍门限是可能的，该方案再一次声称能够应对大规模节点俘获攻击。不幸的是，本文通过构造黑盒的方式对 Guo 等提出的基于乱序多项式密钥管理方案进行攻击，并取得成功，证明其并没有突破多项式的容忍门限，也不能应对大规模节点俘获攻击。

2　系统模型

本文方案基于无线传感器网络模型，由大规模的低能耗、低成本的传感器节点组成。节点具有有限的能量供给、存储空间和计算能力。各节点资源相当，功能对等，通过相互协作、自组织地完成网络功能。各节点存在唯一的 *ID* 号且不被篡改，各节点没有防损硬件，一旦节点被敌手俘获，敌手就可以读取节点上存储的所有信息。在这种网络模型中，没有基站式的中心控制设施，并且各节点是可移动的。假定存在一个离线的数据中心(OLDC, off-line data center)。该 OLDC 负责建立网络、配置节点启动信息和收集数据等操作，是网络所属实体(或单位)的抽象，不参与网络运行过程，不会导致单点失败。

定义 1　在无线传感器网络中，存在节点 u、v 以及它们之间通过无线通信信道建立起来的链路 (u,v)，若 u、v 之间存在共享对偶密钥 $K_{u,v}$，则链路 (u,v) 是安全的。

定义 2　设 A 为一种针对基于多项式的对偶密钥建立方案的攻击方法，$N=\{N_1,\cdots,N_n\}$ 为由 n 个节点组成的无线传感器网络，$F=\{F_1,\cdots,F_k\}\subset N$ 为俘获的节点集合，$P(N_i)$ 表示节点 N_i 上预置的一元多项式或一元多项式集合，如果在 A 的作用下，$\forall n\in N-F$，能够求得 $P(n)$，那么，称 A 攻破了整个无线传感器网络的密钥建立方案。

定义 3　在基于对称多项式的密钥管理方案中，t 多项式自身能够容忍的可被俘获的最大节点数是 t，称 t 为多项式容忍门限。

3　基于对称多项式的对偶密钥方案

3.1　二元对称多项式

1984 年，Blom[8]提出了基于对称矩阵的对偶密钥协商算法。之后，Blundo 等[9]基于这种思想提出了基于二元对称多项式的对偶密钥协商算法(BSP 方案)。基本过程如下。

OLDC 从有限域 GF(p)中(其中 p 为大质数)随机选取一组数 $\{a_{i,j}\mid 0<i<t,\ 0<j<t\}$，构成对称二元

多项式，如式(1)所示，并使等式 $f(x,y)=f(y,x)$ 成立(通常取 $a_{ij}=a_{ji}$)。

$$f(x,y)=\sum_{i=0}^{t}\sum_{j=0}^{t}a_{i,j}x^i y^j \tag{1}$$

ID 为 u 的节点在部署前需要预置一元多项式，如式(2)所示。

$$g_u(y)=f(u,y)=\sum_{i=0}^{t}\sum_{j=0}^{t}a_{i,j}u^i y^j=\sum_{j=0}^{t}c_j^u y^j \tag{2}$$

其中，$c_j^u=\sum_{i=0}^{t}a_{i,j}u^i$。保存在节点 u 内存上的一元 t 阶多项式就是由 $\{c_j^u \mid 0\leqslant j\leqslant t\}$ 表示的 $t+1$ 个系数。

节点 u、v 的共享密钥 $K_{u,v}$ 的协商过程由式(3)保证。

$$g_u(v)=f(u,v)=f(v,u)=g_v(u) \tag{3}$$

文献[9]证明上述基于多项式的密钥协商算法是无条件抵御 t 个节点共谋攻击的，或者说，只要敌手俘获的节点数不超过 t，那么，敌手不可能得到关于共享密钥的任何信息，即被俘节点的数量只要不超过多项式的容忍门限，网络是安全的。

3.2 BSP 方案攻击方法

定义 4 对某个多项式函数 $L(x)$，已知有给定的 $k+1$ 个取值点 $(x_0,y_0),\cdots,(x_k,y_k)$，其中，$x_j$ 对应自变量的位置，y_j 对应着函数在这个位置的取值，假设任意 2 个不同的 x_j 都互不相同，那么应用拉格朗日插值公式所得到的 $L(x)$ 为拉格朗日插值多项式，其表达式为[14]

$$L(x)=\sum_{j=0}^{k}y_j\ell_j(x) \tag{4}$$

其中，$\ell_j(x)$ 为拉格朗日基本多项式（或称插值基函数），其表达式为

$$\ell_j(x)=\prod_{i=0,i\neq j}^{k}\frac{x-x_i}{x_j-x_i} \tag{5}$$

当 $\partial^0 L(x)\leqslant k$ 时，由式(4)和式(5)求得的拉格朗日插值多项式 $L(x)$ 是唯一存在的[14]。

当 BSP 方案俘获节点达到 $t+1$ 时，即超过多项式的容忍门限时，设俘获的节点 ID 集合为 $F=\{ID_1,\cdots,ID_{t+1}\}$，则对于 $\forall ID\in F$ 有式(6)成立。

$$\begin{cases}C_0(x)=\sum_{i=0}^{t}a_{i,0}x^i=c_0^x\\ \cdots\\ C_t(x)=\sum_{i=0}^{t}a_{i,t}x^i=c_t^x\end{cases} \tag{6}$$

则由式(6)可分别求得 $C_0(x),\cdots,C_t(x)$，则对于 $\forall ID\notin F$ 的节点 u 中存储的一元 t 阶多项式为

$$g_u(y)=\sum_{j=0}^{t}C_j(u)y^j \tag{7}$$

即 BSP 方案获得破解。

4 基于乱序多项式对偶密钥方案

为了解决基于多项式的方案中存在的容忍门限问题，Guo 等[12]引入基于乱序的多个对称多项式的方案（PMP 方案），并声称打破了容忍门限。其基本思想是在敌手使用插值法求解多项式的过程中引入困难。下面首先简单介绍该方案，并说明其所谓的困难性，然后给出本文的攻击方法。

4.1 PMP 方案部署

为了便于理解本文的攻击方法，这一节简单介绍 PMP 方案中与多项式攻击方法有关的内容。方案的详细内容请参照文献[12]。

Guo 等的 PMP 方案可以分为 2 步：预置多项式和建立共享密钥。预置多项式包括以下 3 步。

step1 OLDC 从有限域 GF(p)中(其中 p 为大质数)随机选取一组数 $\{a_{i,j,k}\mid 1\leqslant i\leqslant m,0\leqslant j\leqslant t,0\leqslant k\leqslant t\}$，构成 m 个对称二元多项式，如式(8)所示，并使等式 $f_i(x,y)=f_i(y,x),(1\leqslant i\leqslant m)$ 成立。

$$f_i(x,y)=\sum_{j=0}^{t}\sum_{k=0}^{t}a_{i,j,k}x^j y^k,1\leqslant i\leqslant m \tag{8}$$

step2 为每一个节点分配 ID，$u\in$ GF(p)，并构造 m 个一元多项式，如式(9)所示。式(9)中的“[i]”表示多项式序号，以区别指数运算。

$$g_u^{[i]}(y)=f_i(u,y),1\leqslant i\leqslant m \tag{9}$$

step3 将 step2 中产生的 m 个一元多项式以任意顺序预置到节点 u 中，如式(10)所示。

$$g_u^{[i_1]},g_u^{[i_2]},\cdots,g_u^{[i_m]} \tag{10}$$

其中，序列 $\langle i_1,i_2,\cdots,i_m\rangle$ 是序列 $\langle 1,2,\cdots,m\rangle$ 的一个排列。

预置结束、节点部署后，节点间开始建立共享密钥。以节点 u、v 为例介绍该过程。

step1　两节点交换 ID，节点 u 得到 $ID\,v$，节点 v 得到 $ID\,u$。

step2　节点 u 将 v 代入自己的多项式序列，得式(11)。

$$g_u^{[i_1]}(v), g_u^{[i_2]}(v), \cdots, g_u^{[i_m]}(v) \tag{11}$$

step3　同理，节点 v 将 u 代入自己的多项式序列，得式(12)。

$$g_v^{[i_1]'}(u), g_v^{[i_2]'}(u), \cdots, g_v^{[i_m]'}(u) \tag{12}$$

step4　计算式(13)得共享密钥 $K_{u,v}$ 和 $K_{v,u}$

$$\begin{aligned} K_{u,v} &= g_u^{[i_1]}(v) \oplus g_u^{[i_2]}(v) \oplus \cdots \oplus g_u^{[i_m]}(v) \\ K_{v,u} &= g_v^{[i_1]'}(u) \oplus g_v^{[i_2]'}(u) \oplus \cdots \oplus g_v^{[i_m]'}(u) \end{aligned} \tag{13}$$

由于 $f_i(x,y), 1 \leqslant i \leqslant m$ 均为对称多项式，所以有 $K_{u,v} = K_{v,u}$。

4.2　PMP 方案的攻击方法

Guo 等提出的 PMP 方案认为敌手只有通过 Lagrange 插值法(称为插值攻击)才能突破上述方案。破解这些方案的过程如下。

step1　俘获 $t+1$ 个节点，提取每个节点中的 m 个一元多项式并记为一组，共有 $t+1$ 个组。

step2　对 $t+1$ 个组进行重新分组，使来自同一个二元对称多项式的一元多项式组成一个新组，共有 m 个新组，每个新组含有 $t+1$ 个一元多项式。

step3　采用 Lagrange 插值法处理每个新组，可求得 m 个二元对称多项式。

4.3　PMP 方案插值攻击方法困难性分析

由 Lagrange 插值法可知，对于一个 t 阶多项式，只要求得 $t+1$ 个解，便可以成功求得该多项式。由式(10)可知，多项式在预置到节点上时，顺序已经全部打乱，即每个节点上多项式的顺序是任意的。因此，攻击方法的 step2 是不确定的，需要尝试不同的分组方法。这个重新分组的过程是一个排列组合问题，出现了组合困难，见定理 1。

定理 1　设 PMP 方案插值法攻击时，对多项式进行分组的组合数为 $C(m,t)$，则有

$$C(m,t) = (m!)^t \tag{14}$$

其中，m 为二元对称多项式的个数，t 为二元对称多项式的阶。

证明　这个问题的数学模型是点重新分组问题，即有 $t+1$ 个组，每组有 m 个点，所有的 $(t+1)m$ 个点都不同。从每一个组中取一个点组成一个新组，最终形成含有 $t+1$ 个点的 m 个新组。$C(m,t)$ 代表这种重新分组的方法个数，$t+1$ 个组代表了 $t+1$ 个被俘获的节点，点代表了俘获节点中的一个多项式，新分组代表属于同一个二元对称多项式部署在不同节点所得的一元多项式。

点重新分组问题的解法：第一步，将第一组的 m 个点分到 m 个新组中；第二步，将第二组的 m 个点做全排列 $m!$，每一种排列对应一种分组方法，与前一步合并后，每个组有 2 个点，有 $m!$ 种分组方法；第三步，任取一种全面 $m!$ 种分组方法，将第三组的点做全排列 $m!$，进行组合，此时，每个组有 3 个点，$m!\times m!$ 种分组方法。以此类推，直到最后一组。共有 $t+1$ 个组，因此有 $(m!)^t$ 种分组方法。

证毕。

由式(14)可知，组合困难对 m 和 t 的变化很大，如表 1 所示。很小的 m 和 t 就会使组合数 $C(m,t)$ 很大。由 $C(m,t)$ 可知，对多项式进行重新分组问题的计算复杂度为 $O((m!)^t)$，因此该问题是一个 NP 问题。正因为如此，Guo 等认为 PMP 方案突破了多项式的容忍门限，可以容忍大规模节点俘获攻击。

5　PMP 方案基于黑盒的攻击方法

利用 Lagrange 插值法求解式(3)所示的二元多项式 $f(x,y)$，然后就可以求得每个节点上如式(4)

表 1　　**组合困难随 *m* 和 *t* 的变化情况**

m	$t=2$	$t=3$	$t=4$	$t=5$	$t=6$	$t=7$	$t=8$
2	4	8	16	32	64	128	256
3	36	216	1 296	7 776	46 656	279 936	1.7×10^6
4	576	13 824	331 776	8.0×10^6	1.9×10^8	4.6×10^9	1.1×10^{11}
5	14 400	1.7×10^6	2.1×10^8	2.5×10^{10}	3.0×10^{12}	3.6×10^{14}	4.3×10^{16}
6	518 400	3.7×10^8	2.7×10^{11}	1.9×10^{14}	1.4×10^{17}	1.0×10^{20}	7.2×10^{22}
7	2.5×10^7	1.3×10^{11}	6.5×10^{14}	3.3×10^{18}	1.6×10^{22}	8.3×10^{25}	4.2×10^{29}
8	1.6×10^9	6.6×10^{13}	2.6×10^{18}	1.1×10^{23}	4.3×10^{27}	1.7×10^{32}	7.0×10^{36}

所示的一元多项式，从而能够攻破整个网络的密钥建立方案，这是最直接的攻击方法。由 4.3 节的分析可知，Guo 等在求二元多项式 $f(x,y)$ 的过程中引入了如式(14)所示的组合困难，成功应对了基于 Lagrange 插值法的攻击。但是，求出所有节点上的一元多项式，或者说，攻破整个网络的密钥建立方案不必一定要求出二元多项式 $f(x,y)$。由定义 2 可知，只要能够求解任意未俘获节点上的一元多项式或者一元多项式集合即为攻破了整个无线传感器网络的密钥建立方案。下面将给出不通过求解二元多项式 $f(x,y)$，而直接求解某一未被俘获节点上的一元多项式的方法。

本文的攻击方法是基于 Ar 等[15]提出的中间模型及多项式构造方法。基本过程是寻求一个多项式集合 $\{f_1,\cdots,f_m\}$ 来完全描述一个包含 m 个映射关系的黑盒 $B=(B_1(x),\cdots,B_m(x))$，即求多项式集合 $\{f_1(x),\cdots,f_m(x)\}$ 使对于任意的 x 有集合 $\{B_1(x),\cdots,B_m(x)\}$ 与集合 $\{f_1(x),\cdots,f_m(x)\}$ 相等。详细内容请参照文献[15]。

5.1 符号定义与问题描述

基于黑盒的攻击方法用到的符号如表 2 所示。

攻击问题描述。已从由 n 个节点组成的网络中俘获 $mt+1$ 个节点，被俘获节点 ID 集合为 F，并且对于 $\forall ID\in F$，能从中提取 $\boldsymbol{UP}(ID)$，对 $\forall ID_u\in N-F$，求解 $\boldsymbol{UP}(ID_u)$。

由定义 2 可知，求解 $\boldsymbol{UP}(ID_u)$ 的过程就是攻破整个无线传感器网络密钥建立方案的过程。

5.2 攻击过程

设 $G(x,ID)$ 为节点 ID 上的多项式集合，则 $G(x,ID)$ 表达式如式(15)所示，其中，$g_{ID}^{i}(x)$ 表示节点 ID 上第 i 个多项式，$1\leqslant i\leqslant m$。

$$\begin{aligned}G(x,ID)&=\boldsymbol{UP}(ID)[x^0\quad x^1\quad\cdots\quad x^m]\\&=[g_{ID}^{[i_1]}(x)\quad g_{ID}^{[i_2]}(x)\quad\cdots\quad g_{ID}^{[i_m]}(x)]'\end{aligned}\tag{15}$$

因此，对 $\forall ID_u\in N-F$，基于黑盒攻击方法求解 $\boldsymbol{UP}(ID_u)$ 的过程主要分为以下 4 个步骤。

step1 求解多项式集合实例值 $G(ID_{c_i},ID_u)$。对 $\forall ID_u\in N-F$，$\forall ID_{c_i}\in F$，由式(15)得

$$\begin{aligned}G(ID_u,ID_{c_i})&=\boldsymbol{UP}(ID_{c_i})[ID_u^{\,0}\quad ID_u^{\,1}\quad\cdots\quad ID_u^{\,m}]\\&=[g_{ID_{c_i}}^{[c_i^1]}(ID_u)\quad g_{ID_{c_i}}^{[c_i^2]}(ID_u)\quad\cdots\quad g_{ID_{c_i}}^{[c_i^m]}(ID_u)]',\\&\quad 1\leqslant i\leqslant mt+1\end{aligned}\tag{16}$$

其中，序列 $\langle c_i^1,c_i^2,\cdots,c_i^m\rangle$ 表示节点 ID_{c_i} 上多项式部署序列，它是序列 $\langle 1,2,\cdots,m\rangle$ 在节点 ID_{c_i} 的排列。由于部署到各节点的多项式是对称多项式，所以，对 $\forall ID_{c_i}\in F$，有

$$\begin{aligned}&G(ID_{c_i},ID_u)\\&=G(ID_u,ID_{c_i})\\&=[g_{ID_{c_i}}^{[c_i^1]}(ID_u)\quad g_{ID_{c_i}}^{[c_i^2]}(ID_u)\quad\cdots\quad g_{ID_{c_i}}^{[c_i^m]}(ID_u)]'\\&=[g_{ID_u}^{[i_1]}(ID_{c_i})\quad g_{ID_u}^{[i_2]}(ID_{c_i})\quad\cdots\quad g_{ID_u}^{[i_m]}(ID_{c_i})]',\\&\quad 1\leqslant i\leqslant mt+1\end{aligned}\tag{17}$$

其中，式(17)中序列 $\langle i_1,i_2,\cdots,i_m\rangle$ 是肯定存在的 $\langle 1,2,\cdots,m\rangle$ 的一种排列，对于攻击者来说该序列是

表 2 符号定义

参数	参数含义	参数取值
m	节点部署多项式个数	
t	多项式阶数	
p	素数	
n	节点个数	
GF(p)	特征为 p 的有限域	
ID	节点标识	$ID\in[1,p-1]$
N	节点 ID 集合	$\{ID_1,ID_2,\cdots,ID_{n-1},ID_n\}$
F	被俘获节点 ID 集合	$\{ID_{c_1},ID_{c_2},\cdots,ID_{c_{mt}},ID_{c_{mt+1}}\}(c_i\in[1,n],1\leqslant i\leqslant mt+1)$
$\boldsymbol{E}$	$(m+1)\times(mt+1)$ 矩阵	$\boldsymbol{E}(i,j)=e_{i-1,j-1}$
X	关于变量 x 的向量	$X=[x^0\quad x^1\quad x^2\cdots x^{mt-1}\quad x^{mt}]'$
Y	关于变量 y 的向量	$Y=\left[y^m\quad(-1)y^{m-1}\quad y^{m-2}\cdots(-1)^m y^0\right]$
$\boldsymbol{UP}(ID_i)$	ID_i 上 m 个一元 t 阶多项式系数矩阵	$size(\boldsymbol{UP}(ID_i))=[m\quad t+1]$
$\boldsymbol{CUP}$	由 $mt+1$ 个 $\boldsymbol{UP}(ID_i)$ 矩阵组成的三维矩阵	$\boldsymbol{CUP}=[\boldsymbol{UP}(ID_{c_1})\quad\boldsymbol{UP}(ID_{c_2})\quad\cdots\quad\boldsymbol{UP}(ID_{c_{mt+1}})]$

未知，该序列由节点 ID_{c_i} 多项式部署序列 $\langle c_i^1, c_i^2, \cdots, c_i^m \rangle$ 和节点 ID_u 两者多项式部署序列 $\langle u_i^1, u_i^2, \cdots, u_i^m \rangle$ 共同决定。因此有式（18）成立。

$$\{g_{ID_u}^{[j]}(ID_{c_i}) \mid 1 \leqslant j \leqslant m\} = \{g_{ID_{c_i}}^{[j]}(ID_u) \mid 1 \leqslant j \leqslant m\} \quad (18)$$

由式(18)可计算得 $mt+1$ 组 $g_{ID_u}^{[j]}(ID_{c_i})$ 的实例值。

step2　求解 $E(x)$。$E(x)$ 是由 $E_j(x)(0 \leqslant j \leqslant m)$ 构成的多项式集合，如式(19)所示，其中，$E_0(x)=1$，$E_j(x)(1 \leqslant j \leqslant m)$ 是由式（20）决定的一元 jt 阶多项式。

$$E(x) = \begin{bmatrix} E_0(x) & E_1(x) & \cdots & E_m(x) \end{bmatrix}' = EX \quad (19)$$

$$E_j(x) = \sum_{S \subset \lfloor m \rfloor, |S|=j} \prod_{i \in S} g_{ID_u}^{[i]}(x) \quad (20)$$

定理 2　对于 $\forall ID_u \in N-F$，$E_j(x)(1 \leqslant j \leqslant m)$ 是关于 $g_{ID_u}^{[i]}(x)$ 对称的，它由部署在节点 ID_u 上的多项式决定的，与多项式部署顺序无关。

证明　令 $x_1 = g_{ID_u}^{[1]}(x), \cdots, x_m = g_{ID_u}^{[m]}(x)$，则由式（20）决定的 $E_j(x)$ 可表示为式（21）所示的关于 $x_1, \cdots, x_m$ 的 m 元多项式 $ME_j(x_1, \cdots, x_m)$

$$ME_j(x_1, \cdots, x_m) = \sum_{S \subset \lfloor m \rfloor, |S|=j} \prod_{i \in S} x_i \quad (21)$$

序列 $\langle a_1, \cdots, a_m \rangle$ 为序列 $\langle 1, \cdots, m \rangle$ 的任意排列，若 $\left| ME_j(x_1, \cdots, x_m) \right|$ 表示多元多项式 $ME_j(x_1, \cdots, x_m)$ 的项数，则对于 $\forall j \in [1,m]$ 有式（22）成立。

$$\left| ME_j(x_1, \cdots, x_m) \right| = \left| ME_j(x_{a_1}, \cdots, x_{a_m}) \right| = C_m^j \quad (22)$$

设 $ME_j(x_1, \cdots, x_m)$ 中的任意一项，$SE_j(x_1, \cdots, x_m) = \prod_{i=1}^{j} x_{b_i}, b_i \in [1,m]$，由式（21）可知，$ME_j(x_{a_1}, \cdots, x_{a_m})$ 中必定存在一项 $SE_j(x_{a_1}, \cdots, x_{a_m})$，使式（23）成立。

$$SE_j(x_{a_1}, \cdots, x_{a_m}) = SE_j(x_1, \cdots, x_m) \quad (23)$$

由式(22)和式(23)可得到式(24)成立。

$$ME_j(x_1, \cdots, x_m) = ME_j(x_{a_1}, \cdots, x_{a_m}) \quad (24)$$

因此，$ME_j(x_1, \cdots, x_m)$ 为关于 $x_1, \cdots, x_m$ 的 m 元对称多项式。故 $E_j(x)(1 \leqslant j \leqslant m)$ 是关于 $g_{ID_u}^{[i]}(x)$ 对称的，它由部署在节点 ID_u 上的多项式决定，与多项式部署顺序无关。

证毕。

由定理 2 可知，在不能确定式（17）中序列 $\langle i_1, i_2, \cdots, i_m \rangle$ 的情况下，可通过式（18）确定的 $mt+1$ 组 $g_{ID_u}^{[j]}(ID_{c_i})$ 的实例值来确定 $mt+1$ 个 $E_j(x)$ 实例值，如式（25）所示。

$$\begin{aligned} E_j(ID_{c_i}) &= \sum_{S \subset \lfloor m \rfloor, |S|=j} \prod_{i \in S} g_{ID_u}^{[i]}(ID_{c_i}) \\ &= \sum_{S \subset \lfloor m \rfloor, |S|=j} \prod_{i \in S} g_{ID_{c_i}}^{[i]}(ID_u) \end{aligned} \quad (25)$$

由式（4）和式（25）可得式（26）。

$$\begin{aligned} E_j(x) &= \sum_{d=0}^{jt} e_{jd} x^d \\ &= [e_{j0} \quad \cdots \quad e_{jt} \quad 0 \quad \cdots \quad 0][x^0 \quad x^1 \quad \cdots \quad x^{mt}]' \\ &= E(j+1,:)[x^0 \quad x^1 \quad \cdots \quad x^{mt}]', 0 \leqslant j \leqslant m \end{aligned} \quad (26)$$

其中，e_{jd} 为多项式 $E_j(x)(0 \leqslant j \leqslant m)$ 次数为 d 的单项式的系数，$E(1,1)=1$，$E(j, jt+2:mt+1)=0$。

由式（19）和式（26）可进一步确定 $E(x)$ 和描述 $E(x)$ 的系数矩阵 $\boldsymbol{E}$。

step3　构造二元多项式 $Q(x,y)$。

$$\begin{aligned} Q(x,y) &= \boldsymbol{Y}E(x) \\ &= \boldsymbol{YEX} \\ &= \sum_{j=0}^{m} \sum_{d=0}^{jt} (-1)^j e_{jd} x^d y^{m-j} \end{aligned} \quad (27)$$

step4　对 $Q(x,y)$ 进行两元因式分解。

$$Q(x,y) = \prod_{i=1}^{m} (y - \boldsymbol{UP}(ID_u)(i,:)[x^0 \quad x^1 \quad \cdots \quad x^t]') \quad (28)$$

定理 3　有限域 GF(p) 上的任一次数≥1 的多项式 $Q(x,y) = \boldsymbol{YE}(x)\boldsymbol{X}$ 都可以分解成 GF[x,y] 中 m 个不可约多项式的乘积，更进一步，如果式（29）是 $Q(x,y)$ 分解成不可约多项式的 2 种方法，那么一定有 $r=s=m$，并且适当重排因式顺序后有 $p_i(x)=c_i q_i(x)$，其中，$c_i(i=1,2,\cdots,r)$ 是 GF(p) 中一些不等于零的元素。

$$\begin{aligned} Q(x,y) &= (y-p_1(x))(y-p_2(x))\cdots(y-p_r(x)) \\ &= (y-q_1(x))(y-q_2(x))\cdots(y-q_s(x)) \end{aligned} \quad (29)$$

证明　可分解性。假设存在如式（30）所示的多项式 $Q'(x,y) \in$ GF[x,y]，其中，$f_i'(x) \in$ GF[x]($1 \leqslant i \leqslant m$)。

$$Q'(x,y) = (y-f_1'(x))(y-f_2'(x))\cdots(y-f_m'(x)) \quad (30)$$

则对 $Q'(x,y)$ 展开并进行化简可得式(31)。

$$Q'(x,y)=y^m-y^{m-1}\sum_{S\subset[m],|S|=1}\prod_{i\in S}f_i'(x)\cdots+(-1)^m\sum_{S\subset[m],|S|=m}\prod_{i\in S}f_i'(x) \tag{31}$$

令 $E_j'(x)=\sum_{S\subset[m],|S|=j}\prod_{i\in S}f_i'(x)$，当 $g_{ID}^i(x)=f_i'(x)$ 时，$E_j'(x)=E_j(x)(1\leqslant j\leqslant m)$，从而有式（32）成立。

$$Q'(x,y)=Q(x,y) \tag{32}$$

因此，$Q(x,y)$ 可分解为 $(y-p_1(x))(y-p_2(x))\cdots(y-p_m(x))$ 的形式，且有 $\{p_i(x)\,|\,1\leqslant i\leqslant m\}=\{g_{ID}^i(x)\,|\,1\leqslant i\leqslant m\}$。

唯一性。由有限域上多元多项式唯一分解定理可知，$Q(x,y)$ 可分解为 GF$[x,y]$ 中有限个不可约多项式的乘积，并且，如果不计常数因子及乘积中因式的次序，这些不可约多项式是唯一决定的[16]。因为 $Q(x,y)$ 可分解为 $(y-p_1(x))(y-p_2(x))\cdots(y-p_m(x))$ 的形式，所以 $Q(x,y)=(y-p_1(x))(y-p_2(x))\cdots(y-p_m(x))$ 是唯一决定的。故如果 $Q(x,y)=(y-p_1(x))(y-p_2(x))\cdots(y-p_r(x))=(y-q_1(x))(y-q_2(x))\cdots(y-q_s(x))$，那么一定有 $r=s=m$，并且适当重排因式顺序后有 $p_i(x)=c_iq_i(x)$，其中，$c_i(i=1,2,\cdots,m)$ 是 GF(p) 中一些不等于零的元素。

证毕。

由式（28）可知，$\boldsymbol{UP}(ID_u)=[\boldsymbol{UP}(ID_u)(1,:)\cdots\boldsymbol{UP}(ID_u)(m,:)]'$ 即为所求。

$$\begin{aligned}G(x,ID_u)&=[g_{ID_u}^{[1]}(x)\quad g_{ID_u}^{[2]}(x)\quad\cdots\quad g_{ID_u}^{[m]}(x)]'\\&=\boldsymbol{UP}(ID_u)[x^0\quad x^1\quad\cdots\quad x^m]\end{aligned}$$

即为存储在节点 ID_u 上的一元多项式。由定义 2 可知，PMP 方案被攻破。

5.3 复杂度分析

上述攻击过程的计算复杂性主要体现在对求解 $E(x)$ 以及对 $Q(x,y)$ 的因式分解，通过一种复杂度为 $O(m\log m\log\log m)$ 的快速傅里叶变换算法可快速实现对 $E(x)$ 的求解[17]，由基于概率的有限域多元多项式的分解算法可知[18~20]，分解 $Q(x,y)$ 的计算发杂度为 $O((mt+m)^{4.89}\log^2(mt+m)\log p)$。因此，本文提出的基于黑盒的攻击方法完全可以在多项式时间内完成对 PMP 方案的破解，并没有像文献[12]预期的攻击方法那样存在 NP 问题。

6 实例分析

为进一步验证本文所提出的基于黑盒的多项式攻击方案的可行性，本文在 MATLAB 2009 环境中进行实例分析。假设 $m=5,t=3,p=997,n=512$，按照 PMP 方案选择部署节点中的多项式，随机选择 $mt+1$ 个俘获节点为，$F=\{454,62,316,507,19,321,313,85,123,272,359,91,476,14,317,203\}$，随机选择需攻破的节点为 $ID_u=40$。

由式(26)可求的 $E(x)$，并可表示为

$$\begin{aligned}E_0(x)&=1\\E_1(x)&=142+694x+132x^2+240x^3\\E_2(x)&=678+254x+978x^2+690x^3+399x^4+828x^5+12x^6\\E_3(x)&=934+801x+599x^2+48x^3+604x^4+794x^5+389x^6+138x^7+697x^8+451x^9\\E_4(x)&=882+666x+935x^2+307x^3+172x^4+17x^5+502x^6+275x^7+489x^8+321x^9+479x^{10}+246x^{11}+377x^{12}\\E_5(x)&=339+742x+527x^2+937x^3+35x^4+362x^5+51x^6+746x^7+67x^8+805x^9+493x^{10}+326x^{11}+68x^{12}+256x^{13}+445x^{14}+401x^{15}\end{aligned} \tag{33}$$

由式(27)和式(33)构造二元多项式 $Q(x,y)$ 为

$$Q(x,y)=y^5E_0(x)-y^4E_1(x)+y^3E_2(x)-y^2E_3(x)+yE_4(x)-E_5(x) \tag{34}$$

对式(34)因式分解并进行化简可得式(35)。

$$\begin{aligned}Q(x,y)=&[y-(40+328x+400x^2+607x^3)]\\&[y-(462+546x+100x^2+590x^3)]\\&[y-(760+927x+872x^2+226x^3)]\\&[y-(495+856x+793x^2+965x^3)]\\&[y-(379+31x+958x^2+643x^3)]\end{aligned} \tag{35}$$

假设多项式 $f_1(x)$、$f_2(x)$、$f_3(x)$、$f_4(x)$、$f_5(x)$ 可表示为

$$\begin{aligned}f_1(x)&=40+328x+400x^2+607x^3\\f_2(x)&=462+546x+100x^2+590x^3\\f_3(x)&=760+927x+872x^2+226x^3\\f_4(x)&=495+856x+793x^2+965x^3\\f_5(x)&=379+31x+958x^2+643x^3\end{aligned} \tag{36}$$

则部署在 ID_u 上的一元多项式集合 $G_{ID_u}=\{g_{ID_u}^{[i_1]},g_{ID_u}^{[i_2]},g_{ID_u}^{[i_3]},g_{ID_u}^{[i_4]},g_{ID_u}^{[i_5]}\}$ 可表示为

$$G_{ID_u} = \{f_1(x), f_2(x), f_3(x), f_4(x), f_5(x)\} \quad (37)$$

经验证由黑盒攻击方案获得的多项式集合 $\{f_1(x), f_2(x), f_3(x), f_4(x), f_5(x)\}$ 与存储在节点 ID_u 上的 5 个一元 3 次多项式构成的多项式集合相等，由定义 2 可知 Guo 等提出 PMP 方案被攻破。

7　结束语

本文对 WSN 中的基于乱序对称多项式的密钥管理方案进行了分析，并提出了一种攻击方案。该方案通过构造黑盒的方式构造一个特定的二元多项式，并对其进行因式分解，从而通过求解多项式集合的方式实现对乱序多项式的破解，使多项式排列顺序在多项式破解中失去作用。文中通过定理证明和实例分析的方式对提出的基于黑盒的攻击方案的确定性、可行性进行了分析，证明了在多项式时间内能够破解 Guo 等提出的 PMP 方案，而非文献[12]描述的那样为 NP 困难问题。因此，PMP 方式不能抵御大规模节点俘获攻击，未能突破多项式的容忍门限，是不安全的密钥管理方案。

参考文献：

[1] RAGHINI M, MAHESWARI N U, VENKATESH R. Overview on key distribution primitives in wireless sensor network[J]. Journal of Computer Science, 2013, 9(5): 543.

[2] BARUA M P, INDORA M S. Overview of security threats in WSN[J]. International Journal of Computer Science and Mobile Computing, ISSN, 2013, 2(7): 422-426.

[3] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[A]. Proceedings of the 9th ACM Conference on Computer and Communicalion Security[C]. Washington, DC, USA, 2002. 41-47.

[4] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[A]. Proceedings of the 2003 Symposium on Security and Privacy[C]. Carnegie Mellon，PA，USA, 2003. 197-213.

[5] LIU D, NING P. Location-based pairwise key establishments for static sensor networks[A]. Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks[C]. New York, NY, USA, 2003. 72-82.

[6] LIU D, NING P, LI R. Establishing pairwise keys in distributed sensor networks[J]. ACM Transactions on Information and System Security (TISSEC), 2005, 8(1): 41-77.

[7] DU W, DENG J, HAN Y S. A key predistribution scheme for sensor networks using deployment knowledge[J]. IEEE Transactions on Dependable and Secure Computing, 2006, 3(1): 62-77.

[8] BLOM R. An optimal class of symmetric key generation systems[A]. Proceedings of the EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques[C]. New York, USA, 1985. 335-338.

[9] BLUNDO C, DE SANTIS A, HERZBERG A. Perfectly-secure key distribution for dynamic conferences[A]. Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology[C]. London, UK, 1993. 471-486.

[10] YU C M, LU C S, KUO S Y. Noninteractive pairwise key establishment for sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(3): 556-569.

[11] ZHANG W, TRAN M, ZHU S. A random perturbation-based scheme for pairwise key establishment in sensor networks[A]. Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing[C]. New York, USA, 2007. 90-99.

[12] GUO S, LEUNG V, QIAN Z. A permutation-based multi-polynomial scheme for pairwise key establishment in sensor networks[A]. 2010 IEEE International Conference on Proceedings of the Communications (ICC) [C]. Cape Town,SouthAfrica, 2010. 1-5.

[13] ALBRECHT M, GENTRY C, HALEVI S. Attacking cryptographic schemes based on perturbation polynomials[A]. Proceedings of the 16th ACM Conference on Computer and Communications Security[C]. 2009. 1-10.

[14] MEIJERING E. A chronology of interpolation: from ancient astronomy to modern signal and image processing[J]. Proceedings of the IEEE, 2002, 90(3): 319-342.

[15] AR S, LIPTON R J, RUBINFELD R. Reconstructing algebraic functions from mixed data[J]. SIAM Journal on Computing, 1998, 28(2): 487-510.

[16] FENG K, YU H. Integers and Polynomials[M]. Beijing: Higher Education Press, 1999.

[17] GATHEN J. Algebraic complexity theory[J]. Annual Review of Computer Science, 1988, 3(1): 317-348.

[18] GRIGOR'EV D Y E. Factoring polynomials over a finite field and solving systems of algebraic equations[J]. Zapiski Nauchnykh Seminarov POMI, 1984, 137:20-79.

[19] KALTOFEN E. A polynomial-time reduction from bivariate to univariate integral polynomial factorization[A]. Proceedings of the 23rd Annual Symposium on Foundations of Computer Science[C]. Washington, DC, USA, 1982. 57-64.

[20] WAN D Q. Factoring multivariate polynomials over large finite fields[J]. Mathematics of Computation, 1990, 54(190):755-770.

作者简介：

王爱文（1979-），男，湖北蕲春人，东北大学博士生，沈阳化工大学工程师，主要研究方向为无线网络安全。

温涛（1962-），男，陕西宝鸡人，东北大学教授、博士生导师，主要研究方向为网络安全、知识组织。

张永（1981-），男，山东莱芜人，大连东软信息学院副教授，主要研究方向为无线网络安全。

朱奉梅（1980-），女，辽宁沈阳人，辽宁金融职业学院讲师，主要研究方向为网络安全。

吴镝（1979-），男，辽宁辽阳人，东北大学博士生，主要研究方向为网络安全。