doi:10.3969/j.issn.1000-436x.2014.z2.026

新的基于变色龙的车载通信安全与隐私保护

张键红，甄伟娜，邹建成
（北方工业大学 理学院，北京 100041）

摘 要：在车载自组网（VANET）中许多服务和应用需要保护数据通信的安全，为提高驾驶的安全性和舒适性，一些与交通状况有关的信息就要被周期性地广播并分享给司机，如果用户的身份和信息没有隐私和安全的保证，攻击者就会通过收集和分析交通信息追踪他们感兴趣的车辆，因此，匿名消息身份验证是 VANET 中不可或缺的要求。另一方面,当车辆参与纠纷事件时，证书颁发机构能够恢复车辆的真实身份。为解决车载通信这一问题，郭等人在传统方案的基础上提出一种基于椭圆曲线的变色龙散列的隐私保护验证协议。虽然此方案较之前方案具有车辆身份可追踪性和高效率性，但分析表明此方案不满足匿名性。对郭等人的方案进行安全性分析并在此基础上做出改进。

关键词：隐私和安全；变色龙散列；匿名性认证；多项式
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0191-05

New chameleon Hashing of secure and privacy-preserving vehicular communications

ZHANG Jian-hong , ZHEN Wei-na, ZOU Jian-cheng
（College of Science, North China University of Technology, Beijing 100041, China）

Abstract: Many services and applications in vehicular ad-hoc networks (VANET) require preserving and secure data communications. To improve driving safety and comfort, the traffic-related status information will be broadcasted regularly and shared among drivers. Without the security and privacy guarantee, attackers could track their interested vehicles by collecting and analyzing their traffic messages. Hence, anonymous message authentication is an essential requirement of VANET. On the other hand, when a vehicle is involved in a dispute event of warning message, the certificate authority should be able to recover the real identity of this vehicle. To deal with this issue, Guo, *et al* proposed a new privacy-preserving authentication protocol with authority traceability using elliptic curve based chameleon Hashing. Although this scheme has vehicle identification traceability and high computational efficiency than the previous plan, but analysis shows that the scheme does not meet the anonymity. The security of Guo's scheme is analyzed and improvement is made based on Guo's protocol.

Key words: secure and privacy-preserving; chameleon Hash; anonymous authentication; polynomial

1 引言

车载自组网（VANET, vehicular Ad-Hoc network）是专为车辆间通信而设计的自组织网络，它创造性地将无线网络应用于车辆间的通信，实现了在网络信息平台上对所有车辆的状况信息进行有效管理和提供综合服务的功能[1~3]。

一个安全 VANET 的包括 2 部分节点：嵌入在车辆上的无线通信单元（OBU, on-board unit）和部署在道路两边关键点上为车辆提供服务的固定基础设施（RSU, road-side unit）；证书管理中心（CA, certificate authority）；CA 是 OBU 和 RSU 注册和认证中心，并且具有大量计算和存储能力，只有 CA 可以从 OBU 证书中恢复其真实身份。RSU 作为

收稿日期：2014-07-02
基金项目：青年拔尖人才支持计划基金资助项目（14075）
Foundation Item: The Young Talent Support Plan (14075)

OBU 和 CA 的中介部署在无人看管的车道两旁，它们负责从恶意或吊销车辆中过滤假消息并将 OBU 的证书信息报告给 CA。OBU 定期广播常规交通状态信息(如速度、位置、加速度)，帮助驾驶员更好地认识他们的驾驶环境，使其提前应对异常事件。车载自组网包括 2 种通信模式：车间通信（V2V, vehicle to vehicle）和车辆与基站通信（V2R, vehicle to road-side）。

随着车载自组网的发展，及其应用场合的重要性，信息安全和用户隐私保护问题至关重要，没有安全和隐私保证，恶意敌手就会通过追踪他们感兴趣的车辆位置进行攻击或滥用该车辆的移动模式。因此，车载自组网的协议必须保护用户隐私和信息不被攻击者篡改。

一个安全的隐私保护协议应符合以下要求。

1) V2R 相互认证：为抵御潜在的对手或恶意的 OBU，在 V2R 交换的私密或关键信息之前进行相互认证是至关重要的。

2) V2V 相互认证：即使没有 RSU，OBU 之间也可以相互验证，并发现可能的对手 OBU 传播虚假信息，确保车载自组网的安全。

3) 匿名身份验证：验证过程应该在 OBU 没有透露他们的身份的情况下验证其合法性。

4) 不可链接性：对手不能链接相同 OBU 发布的数据分组，即使通过开放的无线媒介窃听到传播消息。

5) 车辆身份可追溯性：一个具有挑战性的问题是在保证匿名身份验证过程中，证书管理中心能够追踪恶意车辆。

6) 高效率：大量车辆快速经过一个 RSU 节点，在 OBU 离开通信范围之前必须建立安全连接，这需要在很短时间内完成，所以身份验证过程应该是高效的。

然而，在 VANET 中保证信息匿名性验证是困难的，因为合法的车辆为获得更安全有效的交通环境会把自己的位置信息告诉 RSU，此过程存在的风险是恶意的车辆可以收集这些信息进行篡改或重放给 RSU，这种情况经常发生在当某一辆车牵涉到一宗事故并且试图逃避调查和责任时。传统的隐私保护必须保证用户相关信息（如姓名、车牌号、位置、行驶路线等）得到保护，并且当违法事故发生时，认证机构能够恢复用户的真实身份。因此，安全协议不仅要保证用户的隐私，也要保证用户真是身份被找回。针对这一问题，一系列方案被相继提出，但大部分方案由于计算成本高[4-6]而不太适合 VANET[7]，Guo 等人在传统方案基础上，为实现时间变化的匿名性证书，将变色龙签名和基于椭圆曲线的签名相结合，提出基于椭圆曲线的变色龙散列签名方案，即一种轻重量隐私保护（LPP, lightweight privacy-preserving）协议。虽然此方案较之前方案具有车辆身份可追踪性和高效率性，本文通过分析，Guo 等人的方案不满足匿名性和车辆不可连接性，本文对他的方案进行安全性分析并在此基础上做出改进。

2 相关知识

G_p 是由椭圆曲线上的点构成的阿贝尔（Abelian）群，p 是大素数，g 是群 G_p 的生成元。q 也是大素数并且能被 $|G_p|$ 整除，其中 $|G_p|$ 为群 G_p 的阶。$h(\cdot)$ 为强单向散列函数。任意取 $P\in G_p$，则系统参数为 $(p,P,q,h(\cdot))$。

本文基于椭圆曲线（elliptic curve）上的数学困难问题，即对于公式 $Q=kP$，其中 $P,Q\in G_p$，已知 k,P 求 Q 是容易的，但已知 P,Q 求 k 是困难的。

3 基于椭圆曲线的变色龙散列签名

变色龙散列签名，最早由 Krawczyk 和 Rabin 提出[8]，它是一种带陷门的单向散列函数，掌握陷门消息的人可以容易地计算出一个随机输入的碰撞，而没有陷门消息的人无法计算碰撞。变色龙散列的独有特点是非交互性验证、计算简单且有更高计算效率。传统的基于离散对数的变色龙散列签名算法(如基于身份的变色龙散列[9])需要出具相同的公钥，此公钥存在密钥泄漏缺陷，无法保证不可链接性。之后 Chen 等人提出无密钥泄漏的变色龙散列函数[10]，Guo 等人方案[11]和本方案都是基于椭圆曲线上的无密钥泄漏的变色龙散列函数。

一种变色龙散列签名方案步骤如下。

EC-based 变色龙散列签名的用户（证明者 A）签名和验证者 B 验证过程。

1) setup：取一个大素数 p，建立由椭圆曲线上点组成的 Abel 群 G_p，q 是一个大素数且 $q\,||\,|G_P|$，任取一点 $P\in G_p$。$h(\cdot)$ 是强安全单向散列函数，将任意长的字符串映射到 $[1,q-1]$ 中的一个值，系统参数 $params=(G_p,p,P,q,h(\cdot))$。

2) sign：用户 A 随机取 $S\in[1,q-1]$，计算变色

龙值 $C=SP$，其中，S 是 A 的私钥，C 为公钥。当 A 需要被 B 验证时，A 再随机取一个值 $\alpha\in[1,q-1]$ 作为新私钥，相应公钥 $y=\alpha P$。m 为辅助参数，它由碰撞发现算法 $CFind(\alpha,nonce,S)$ 生成。

$$m=CFind(\alpha,nonce,S)=S-\alpha\gamma$$
$$\gamma=h(y\oplus nonce)$$

其中，$nonce$ 是当前时间。然后，A 将 $(C,m,y,nonce)$ 发送给 B。

3) verify：B 接收 $(C,m,y,nonce)$，验证等式 $CH(m,y,nonce)=C$ 是否成立。

其中，变色龙散列函数

$$CH(m,y,nonce)=mP+\gamma y$$
$$=mP+h(y\oplus nonce)y$$

若成立，则用户 A 合法；否则非法，举报。

4　对 Guo 等人方案回顾并做安全性分析

4.1　Guo 等人的方案回顾

本文对 Guo 等人的方案做简要讲述，详细过程参考文献[11]。

OBU_b 和 RSU_a 的真实身份分别为 ID_b和ID_a，CA的公、私钥对为（K_{CA}^{+},K_{CA}^{-}），$\alpha_b^{(i)}$ 为 b 在第 i 次会话的私钥，$K_{a,b}^{(i)}$ 为 a和b 在第 i 次会话的共享密钥。

1) 注册阶段：OBU_b 随机取 $S_b\in[1,q-1]$ 作为私钥，计最初变色龙值 $C_b=S_bP$，将（C_b,ID_b）发送给 CA，CA 产生 OBU_b 的证书 $CER_b=\mathrm{sign}(C_b,K_{CA}^{-})$。

同理，RSU_a 的证书为 $CER_a=\mathrm{sign}(C_a,K_{CA}^{-})$，其中，$C_a=S_aP$。

2) 相互认证阶段：包括V2R和V2V 这 2 个认证阶段，在此回顾 V2V 认证过程，V2R和V2V 认证过程大致一样，详细过程参考文献[11]，基于普遍性，假设认证发生在第 i 次会话。

V2V 相互认证阶段如下所述。

① OBU_a 和 OBU_b 分别产生私钥 $\alpha_a^{(i)},\alpha_b^{(i)}\in[1,q-1]$，并计算相应公钥 $y_a^{(i)}=\alpha_a^{(i)}P$，$y_b^{(i)}=\alpha_b^{(i)}P$。

② OBU_a 和 OBU_b 分别计算共同密钥对 $K_{a,b}^{(i)}=\alpha_a^{(i)}y_b^{(i)}=\alpha_b^{(i)}y_a^{(i)}=K_{a,b}^{(i)}$。$OBU_a$ 和 OBU_b 分别加密各自证书 $CER_a^{'}=Encrpt(CER_a\oplus T_a^{(i)},K_{a,b}^{(i)})$ $CER_b^{'}=Encrpt(CER_b\oplus T_b^{(i)},K_{a,b}^{+})$。

③ OBU_b 利用公式 $m_b^{(i)}=CFind(\alpha_b^{(i)},T_b^{(i)},S_b)$ 计算辅助参数 $m_b^{(i)}$。

④ OBU_b 将（$CER_b^{'},y_b^{(i)},m_b^{(i)},T_b^{(i)}$）发送给 OBU_a。

⑤ OBU_a 接收（$CER_b^{'},y_b^{(i)},m_b^{(i)},T_b^{(i)}$）后，用 $K_{a,b}^{(i)}$ 解密 $CER_b^{'}$ 得到 $CER_b=Decrpt(CER_b^{'},K_{a,b}^{(i)})\oplus T_b^{(i)}$，再验证等式 $\mathrm{verify}(CER_b,K_{CA}^{+})=CH(m_b^{(i)},y_b^{(i)},T_b^{(i)})$ 是否成立，若成立，进行下一步协议，即 OBU_b 以相同的步骤及方法验证 OBU_a。

4.2　安全性分析

V2V 之间身份验证，假设 OBU_a 在第 i 次会话中验证 OBU_b 的身份。

由于

$$CER_b=\mathrm{sign}(C_b,K_{CA}^{-})$$
$$m=CFind(\alpha,nonce,S)=S-\alpha\gamma$$
$$\gamma=h(y\oplus nonce)$$
$$CH(m,y,nonce)=mP+\gamma y$$

所以

$$\mathrm{verify}(CER_b,K_{CA}^{+})=C_b$$
$$CH(\alpha_b^{(i)},y_b^{(i)},T_b^{(i)})=m_b^{(i)}P+\gamma y_b^{(i)}$$
$$=(S_b-\alpha_b^{(i)}\gamma)P+\gamma y_b^{(i)}$$
$$=S_bP-\gamma\alpha_b^{(i)}\cdot P+\gamma y_b^{(i)}$$
$$=S_bP$$
$$=C_b$$

虽然验证等式 $\mathrm{verify}(CER_b,K_{CA}^{+})=CH(m_b^{(i)},y_b^{(i)},T_b^{(i)})$ 成立，证明对方是合法的 OBU_b。

此方案是不安全的，车载自组网内的车辆针对网外的车辆满足匿名性，但对于自组网内的车辆之间不满足匿名性，每次会话中，OBU_a 验证 OBU_b 的身份时，不管 $m_b^{(i)},\alpha_b^{(i)}$ 如何变化，验证结果都为 OBU_b 的固定公钥 C_b。长时间内，在不同时间地点验证另一车辆身份结果都为常值 C_b，则可确定对方为 OBU_b，若 OBU_a 是恶意车辆，OBU_a 通过多次记录 OBU_b 的行车时间地点来推测 OBU_b 经常行车路线，从而进行追踪达到自己的目的，如获得 OBU_b 用户家庭住址、工作单位或盗窃该车，特别是 OBU_b 用户是知名人士或明星，匿名性得不到保护是很危险的。

5　本文改进新方案

本方案主要思想是将用户的公钥隐藏在多项式中[13,14]，即对方能多次验证该用户是合法，但不能通过记录数据推断出它是哪一辆具体的车辆，或者说具体的用户。

5.1　改进方案流程

本方案碰撞发现算法为 $CFind(\alpha,nonce,x)$

$$m = CFind(\alpha, nonce, x) = x - \alpha\gamma$$
$$\gamma = h(y \oplus nonce)$$

变色龙散列函数为

$$CH(m, y, nonce) = mP + \gamma y$$
$$= mP + h(y \oplus nonce)y$$

1）注册阶段

OBU 和 RSU 都要向 CA 注册。

OBU 的注册阶段：OBU_i 的身份为 $ID_{V,i}$，$i \in [1,n]$，$OBU_1, OBU_2, \cdots, OBU_n$ 将自己身份 $ID_{V,1}, ID_{V,2}, \cdots, ID_{V,n}$ 发送给 CA。

CA 接收到 $ID_{V,i}$ 后，计算 $a_i = h(ID_{V,i})$，建立有限域上的 n 次多项式 $f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$，CA 的私钥 $K_{CA}^- = a_0$，其中，a_0 是多项式 $f(x)$ 的常数项，公钥 $K_{CA}^+ = a_0 P$。令 $g^{f(x)} = 1$ 的 n 个解分别为 $x_{V,1}, x_{V,2}, \cdots, x_{V,n}$ 作为 $OBU_1, OBU_2, \cdots, OBU_n$ V2V 相互认证阶段，在第 m 次会话中的公钥，$x_{V,i}$ 对应 $ID_{V,i}, i \in [1,n], n \geqslant 2$。

CA 用自己私钥 K_{CA}^- 对 OBU_i 的身份 ID_i 进行签名产生证书 $CER_{V,i} = \text{sign}(x_{V,i}P \oplus T_{Exp}, K_{CA}^-)$，其中 T_{Exp} 为证书限制使用时间，CA 将（$CER_{V,i}, ID_i, x_{V,i}$）存储到数据库并将（$CER_{V,i}, x_{V,i}$）通过安全信道发送给 OBU_i。

同理，RSU_j 的证书为 $CER_{R,j} = \text{sign}(x_{R,j}P \oplus T_{Exp}, K_{CA}^-)$，其中，$x_{R,j}$ 是多项式 $f(x) = (x-b_1)(x-b_2)\cdots(x-b_n)$ 的解，$b_j = h(ID_{R,j})$，$j \in [1,n]$。

2) 相互验证阶段

V2R 相互认证阶段，在第 m 次会话中

① RSU_j 取 $\alpha_{R,j}^{(m)} \in [1, q-1]$，并计算相应公钥 $y_j^{(m)} = \alpha_{R,j}^{(m)} P$。计算 $\gamma_j^{(m)} = h(y_j^{(m)} \oplus T_j^{(m)})$，其中 $T_j^{(m)}$ 为当前时间。计算 $m_j^{(m)}$，将 $(CER_{R,j}, y_j^{(m)}, m_j^{(m)}, T_j^{(m)})$ 发送给 OBU_i。

② OBU_i 接收 $(CER_{R,j}, y_j^{(m)}, m_j^{(m)}, T_j^{(m)})$，验证 $\text{verify}(CER_{R,j}, K_{CA}^+) = CH(m_j^{(m)}, y_j^{(m)}, T_j^{(m)}) \oplus T_{Exp}$ 是否相等，若相等，进行下一步协议。

③ OBU_i 取随机数 $\alpha_{V,i}^{(m)} \in [1, q-1]$ 作为私钥，并计算相应公钥 $y_i^{(m)} = \alpha_i^{(m)} P$。并计算共同密钥 $K_{Rj,Vi}^{(m)} = \alpha_{V,i}^{(m)} y_j^{(m)}$。

④ OBU_i 将自己证书加密 $CER_{V,i}^{'} = Encrpt(CER_{V,i} \oplus T_{V,i}^{(i)}, K_{Rj,Vi}^+)$。

OBU_i 将（$CER_{V,i}^{'}, y_i^{(m)}, m_i^{(m)}, T_i^{(m)}$）发送给 RSU_j。

⑤ RSU_j 接收（$CER_{V,i}^{'}, y_i^{(m)}, m_i^{(m)}, T_i^{(m)}$）后，计算共同密钥 $K_{Rj,Vi}^{(m)} = \alpha_{R,j}^{(m)} y_i^{(m)}$。

⑥ RSU_j 用 $K_{Rj,Vi}^{(m)}$ 解密 $CER_{V,i}^{'}$ 得到 $CER_{V,i} = Decrpt(CER_{V,i}^{'}, K_{Rj,Vi}^{(m)}) \oplus T_{V,i}^{(m)}$。$RSU_j$ 要检查 $T_{V,i}^{(m)}$ 的有效性，更重要是检查 $CER_{V,i}$ 是否在 CA 对非法车辆的撤销列表里，如果在，RSU_j 立即终止协议。若不在，进行下一步协议。

⑦ RSU_j 验证 V2R 等式 $\text{verify}(CER_{V,i}, K_{CA}^+) = CH(m_{V,i}^{(m)}, y_i^{(m)}, T_{V,i}^{(m)}) \oplus T_{Exp}$ 是否成立，若成立，则 RSU_j 和 OBU_i 相互验证过程结束。

车辆间的相互过程，双方都要加密自己的证书，以保证是被合法的另一方接收，其他过程同上。

3) CA 追踪阶段

CA 追踪阶段发生在处理特殊事件时，OBU 的身份 ID 需要被追回。CA 收回相应的证书 CER，因为每一份证书都是唯一的，CA 通过数据库查找出与 OBU 相应的身份。

5.2 安全性分析

1) 正确性和匿名性。本方案可验证所有 RSU, OBU 都是合法的用户，因为验证总是正确的，例如 RSU_j 验证等式 $\text{verify}(CER_{V,i}, K_{CA}^+) = CH(m_{V,i}^{(m)}, y_{V,i}^{(m)}, T_{V,i}^{(m)}) \oplus T_{Exp}$。由于

$$CER_{V,i} = \text{sign}(x_{V,i} \oplus T_{Exp}, K_{CA}^-)$$
$$m = CFind(\alpha, nonce, x) = x - \alpha\gamma$$
$$\gamma = h(y \oplus nonce)$$
$$CH(m, y, nonce) = mP + \gamma y$$

所以

$$\text{verify}(CER_{V,i}, K_{CA}^+) = x_{V,i}P \oplus T_{Exp}$$
$$CH(m_{V,i}^{(m)}, y_{V,i}^{(m)}, T_{V,i}^{(m)}) \oplus T_{Exp}$$
$$= (m_{V,i}^{(m)} P + \gamma_{V,i}^{(m)} y_{V,i}^{(m)}) \oplus T_{Exp}$$
$$= [(x_{V,i} - \alpha_{v,i}^{(m)} \gamma_{V,i}^{(m)})P + \gamma_{V,i}^{(m)} y_{V,i}^{(m)}] \oplus T_{Exp}$$
$$= x_{V,i}P \oplus T_{Exp}$$
$$= x_{V,i}P \oplus T_{Exp}$$

成立，用户是合法的；更重要的是，本方案对自组网内的合法用户满足很好的匿名性，每次验证等式结果为 xP，由离散对数难题可知，敌手由 xP 推出 x 是

困难的，并且也不能确定 x 是多项式 $f(x)$ 的哪个解。验证者只能确定它是合法车辆，但不能追踪哪一个具体的车辆。从而满足了匿名性。

2) 不可追踪性。伪造一个合法基于 EC 的变色龙散列算法相当于解决 ECDLP。破解 EC-based 变色龙散列函数的唯一方法是分析同一个 RSU或OBU 发送的信息集合,如（$CER, m^{(k)}, y^{(k)}, T^k$), $1 \leqslant k \leqslant n$，根据碰撞发现函数的定义，对手可以建立一个线性方程系统，等式如下。

$$\begin{aligned} & m^{(1)} + \alpha^{(1)}\gamma^{(1)} = m^{(2)} + \alpha^{(2)}\gamma^{(2)} \\ & = \cdots \\ & = m^{(n)} + \alpha^{(n)}\gamma^{(n)} \end{aligned}$$

其中，$\gamma^{(k)} = h(y^{(k)} \oplus T^{(k)})$，$m^{(k)}$ 是已知的，$\alpha^{(m)}$ 是变量，注意到此线性方程系统有 k 个变量，但是只有 $k-1$ 个等式。也就是说，至少有一个变量如 $\alpha^{(m)}$ 由公式 $\alpha^{(m)}P = y^{(m)}$ 推测出，其中 $P, y^{(m)} \in G_p$。因此，伪造一个合法的基于椭圆曲线的变色龙散列算法相当于解决基于椭圆曲线上的离散对数难题，是困难的。

3) 高计算效率。原方案的优点就是运算简单，高效率。本方案与原方案具有相同计算复杂度。虽然在注册阶段可信任中心要将每个用户的身份散列，并且计算多项式，这些操作都是离线进行的，不影响会话过程中的在线计算高效性，本方案与原方案每次会话中方案一样，计算量相同，满足高效性。本方案满足匿名性和不可追踪性，比原方案更安全。

6　结束语

为解决车载通信匿名消息身份验证的问题，本文对郭等人提出的基于椭圆曲线的变色龙散列的隐私保护验证协议进行了改进，满足了匿名性和不可追踪性，性能较原方案有提升。

参考文献：

[1] FIEBIG B. European traffic accidents and purposed solutions [A].Proc of the ITU-T Workshop on Standardization in Telecommunication for Motor Vehicles [C]. 2003.24-25.

[2] PASSMANN C, BRENZEL C, MESCHENMOSER R. Wireless vehicle to vehicle warning system[A]. SAE 2000 World Congress, Detroit[C]. MI, USA, 2002.149-154.

[3] Internet ITS consortium[EB/OL]. http://www.internetits.org, 2006.

[4] LIN X, SUN X, HO P H, *et al*. GSIS: a secure and privacy- preserving protocol for vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2007,56(6):3442-3456.

[5] STUDER A, SHI E, BAI F, *et al*. Tacking together efficient authentication, revocation, and privacy in VANETs[A]. Proceeding of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks(SECON)[C]. 2009.1-9.

[6] LI R, LIN X, ZHU H, *et al*. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications[A]. Proceeding of the 27th Conference on Computer Communications (INFOCOM)[C]. IEEE, 2008.1229-1237.

[7] PENG Y, ABICHAR Z, CHANG J. Roadside-aided routing(RAR) in vehicular networks[A]. Proceeding of International Conference on Communications(ICC)[C]. 2006.3602-3607.

[8] KRAWCZYK H, RABIN T. Chameleon hashing and signatures[A]. Proceeding of Network and Distributed System Security 2000[C]. 2000.143-154.

[9] ATENIESE G, DE MEDEIROS B. Identity-based chameleon Hash and applications[J]. Financial Cryptography, 2004, 3(10):164-180.

[10] CHEN X, ZHANG F, KIM K. Chameleon hashing without key exposure[A]. ISC 2004[C]. Springer-Verlag, 2004.87-98.

[11] GUO S, ZENG D, XIANG Y. Chameleon hashing for secure and privacy-preserving vehicular communications[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 25(11): 2794-2803.

[12] BLAKE G S I, SMART N. Elliptic Curves in Cryptography[M]. Cambridge University Press, 1999.

[13] WANG B Y, LI H, LIU X F, *et al*. Preserving identity privacy on multi-owner cloud data during public verification[EB/OL]. http://www.wileyonlinelibrary.com.

[14] 张青波, 陈彩云, 陈鲁生等. 有限域上多项式形式的 EIGamal 体制及数字签名方案[J]. 通信学报, 2005, 26(5):69-72.
ZHANG Q B, CHEN C Y, CHEN L S, *et al*. In the form of polynomial over finite field EIGamal system and digital signature scheme[J]. Journal on Communications, 2005, 26(5):69-72.

作者简介：

张键红（1976-），男，北京人，北方工业大学副教授，主要研究方向为信息安全和密码学。

甄伟娜（1988-），女，河北邢台人，北方工业大学硕士生，主要研究方向为密码学。

邹建成（1966-），男，北京人，北方工业大学教授，主要研究方向为信息安全和图像处理。