基于分段加密和时效控制的 QR 码物流隐私保护方案

刘亮[1]，郭文博[1]，杨昱威[2]，郭怀宇[1]

（1. 四川大学网络空间安全学院，四川 成都 610207；
2. 四川大学电子信息学院，四川 成都 610065）

摘　要：针对现有物流系统在用户隐私保护上的一些弊端，提出了一种基于 QR 码分段加密、分级授权和时效控制的隐私保护方案。该方案将收件人所有信息进行分段 RSA 加密、Base64 编码，整合之后嵌入 QR 码中。在物流运输及派件过程中，对于不同的网点或转运中心授予不同级别的 QR 码解密权限，查看指定内容。同时在用户签收后 QR 码自动失效，以此达到保护用户个人隐私的目的。方案的核心思想是尽可能减少收件人信息的接触人群，降低用户信息泄露的可能性。

关键词：QR 码；分段加密；时效控制；双向认证；物流系统；隐私保护

中图分类号：TP309.2

文献标识码：A

doi: 10.11959/j.issn.2096−109x.2019039

Research on QR code logistics privacy based on segmented encryption and time-limited control

LIU Liang[1], GUO Wenbo[1], YANG Yuwei[2], GUO Huaiyu[1]

1. College of Cybersecurity, Sichuan University, Chengdu 610207, China
2. College of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China

Abstract: In view of the disadvantages of the existing logistics system in the market in user privacy protection, a privacy protection scheme based on QR code segmentation encryption, hierarchical authorization and time-limited control was proposed. This scheme segments all the recipient information into RSA and Base64 encryption,after integration, it is embedded into the QR code. In the process of logistics transportation and delivery, different levels of QR code decryption permissions are granted to different branches or transfer centers to view the designated content. At the same time, the QR code automatically becomes invalid after the user signs for it, so as to protect the user's privacy. The core idea of the scheme is to minimize the contact group of recipient information and reduce the possibility of user information disclosure.

Key words: QR code, segment encryption, aging control, two-way authentication, logistics system, privacy protection

收稿日期：2019−04−15；**修回日期：**2019−06−03

通信作者：郭文博，2338216055@qq.com

论文引用格式：刘亮, 郭文博, 杨昱威, 等. 基于分段加密和时效控制的 QR 码物流隐私保护方案[J]. 网络与信息安全学报, 2019, 5(4): 63-70.

LIU L, GUO W B, YANG Y W, et al. Research on QR code logistics privacy based on segmented encryption and time-limited control[J]. Chinese Journal of Network and Information Security, 2019, 5(4): 63-70.

1　引言

随着互联网技术的发展，电子商务所具有的众多优点，使电子商务在生活中应用得更加广泛，同时带动传统物流行业进一步发展，每年的包裹数保持着很高的增长率。2018 年 11 月期间，全国累积发送的包裹数迎来了大幅度增长，达到 58.6 亿件；而 2017 年同期为 47.1 亿件[1]。同时，2018 年全国快递服务企业业务量累计完成 507.1 亿件（如图 1 所示）。随着快递行业的高速发展，在促进国家经济的上升、便利人们生活的同时也带来了不容小觑的威胁。近几年来，因为快递单信息泄露而造成的财产损失甚至威胁人身安全的事件屡见不鲜，用户的个人信息裸露在公众视线中，给不法分子提供了可乘之机。2017 年 6 月，国家出台了《中华人民共和国网络安全法》，在法律层面上对个人的信息进行了保护，但推广较慢且针对性不强。目前，国内外对于快递信息的保护有很多方案。① 快递包裹标签法，利用一种特殊的快递标签，在用户收到包裹后直接拉住标签一端即可轻松撕掉相关信息。② *K*−匿名模型法，这种方法在快递单上仍然保留着用户的姓名、电话号码，对个人信息没有起到有效保护[2]。③基于二维码的隐藏方法，该方法应用比较广泛，但它直接将用户的信息载入二维码中，仅做了简单的隐藏和加密，其存在着极大的隐患。首先是密码泄露的问题，其次是快递完成之后二维码依然有效，这也对用户的信息造成很大的威胁[3]。鉴于上述存在的问题，本文提出基于分段加密和时效控制的 QR 码物流隐私系统，旨在实现个人信息的完全隐藏，让用户不再担心快递泄密事件的发生。

2　国内外研究现状

由于物流行业在发展过程中暴露出的隐私泄露问题越来越多，目前国内外已有一些专家学者和企业在研究物流中的隐私保护问题，并取得了一定的成效。

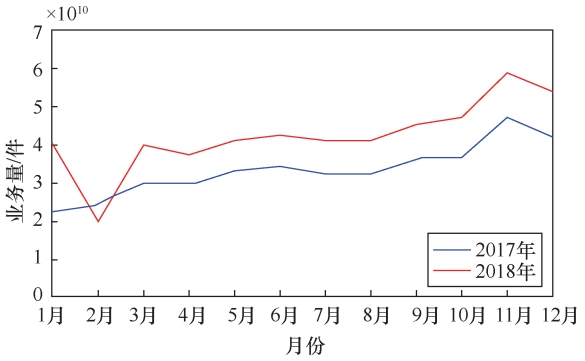


图 1　2017 年和 2018 年快递业务变化

国外针对物流信息系统（LIS，logistics information systems）[4]的个人隐私信息保护主要通过政府、法律的形式对物流行业进行规范和监督。例如，英国邮政管理委员会规定，在物流运营商的许可证中必须明确关于邮政安全的相关条款，并以法律的形式强制执行；美国快递员在就业时必须提供社会安全号。上述的法律法规或行业规范在一定程度上可以解决部分隐私泄露的问题，但用户的个人隐私信息依然存在泄露的可能性。

国内物流行业对于用户隐私泄露问题给予了一定程度的重视。一些快递公司推出了隐私面单，将个人信息隐藏，但就目前看来并未有大规模的应用[5]。用户隐私泄露问题依然严峻。一方面，小部分为了谋取利益，在行业内部存在隐私交易的可能性；另一方面，快递单在签收之后的随意丢弃也容易泄露信息，威胁人身财产安全。另外，如果服务器的数据大规模泄露，更有可能对用户的个人隐私产生无法挽回的损失。

针对上述情况，本文提出了基于分段加密和实效控制的 QR 码的物流隐私系统，以期待更好地解决物流行业存在的用户隐私安全问题。

3　物流隐私保护方案

3.1　隐私保护方案框架

在本文提出的基于分段加密和实效控制的 QR 码[6]的物流隐私系统方案中，采用信息加密隐藏技术，将用户的所有信息进行分段加密，然后将加密的信息整合嵌入快递面单的 QR 码中，系统自动生成对应的权限查看密钥，分发给不同级别的物流集件中心管理人员，完成对不同角色访问查看的控制。

隐私保护方案中主要包含信息加密模块、密钥管理模块、订单管理模块。

下面介绍隐私保护方案的业务流程。

① 在用户下单后，其收件地址、电话等相关信息被寄件方所知，寄件方根据所寄物品，使用物流 App 填写相关的快递面单，填写完成后提交到系统服务器中保存并做进一步处理。

② 服务器接收到客户端提交的寄件面单后，自动根据事先设定好的加密算法对寄件单上的用户信息进行分层 RSA[7]加密，分层加密后整合生成对应嵌入信息的 QR 码，同时将加密的公私密钥保存在数据库中，对于不同的密钥授予不同级别的访问权限，用于之后的各级获取密钥后授权解密。

③ 服务器生成 QR 码后，将加密后的 QR 码返回给快递公司，快递公司获取 QR 码，将其贴在包裹表面，用于保存与标识用户的快递信息。

④快递公司运输包裹到省级集件中心，省级集件中心分派人员从数据库中获取省级授权私钥，对市级的网点信息进行解密并分派快件；市级收到分派来的快件后，通知相关分派人员从数据库中获取市级授权私钥，对县级网点信息进行解密，同时将快件运输到对应的县级网点；县级网点采用同样的方式从数据库获取县级授权私钥，解密收件人具体地址，通知快递员派件。需

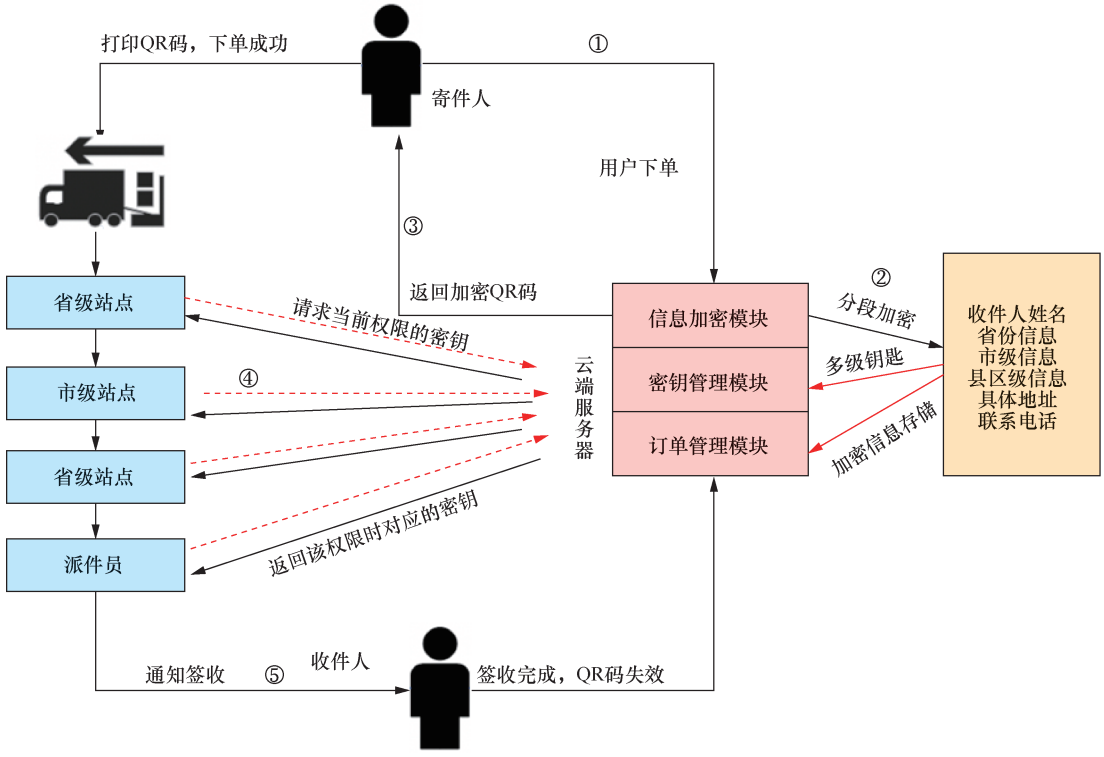


图 2　隐私保护方案框架

要注意的是，高一级的私钥只能对下一级的信息进行解密，即高一级的人员无法查看跨级的更具体的收件人信息。

⑤ 快递员派件。快递员知道用户的收件地址和物品信息，用户的电话信息是采用统一号码加密的，只能通过 App 直接拨打或发短信，进一步提高安全性。

⑥ 用户接到快递到达短信后，对快递进行现场签收。在核对签收完成后，手持终端机提交签收成功信息到服务器中，服务器收到请求，立即销毁先前创建的包含用户隐私的 QR 码，保证用户的隐私信息不被泄露。

3.2 分段加密设计

分段加密设计是本文的核心，也是创新所在。根据该方案框架的设计，采用分段加密的方式对用户的快递信息进行保护。在快递单上用户的信息一般包括姓名、住址、邮编、电话以及寄件物品的种类[8]。在整个寄件的过程中，不同的转运中心会查看不同的信息，针对这个特点采用分段加密的方式对用户的订单信息进行加密，如式(1)所示。

$$C = E_{Base64}\left(E_{RSA}\left(E_{RSA1}m_1 \| E_{RSA2}m_2 \| E_{RSA3}m_3 \| E_{RSA4}m_4\right)\right) \tag{1}$$

其中，$m_i(i=1,2,\cdots,n)$代表不同的地址信息；RSA_i $\left(i=1,2,\cdots,n\right)$代表不同级别的密钥。

在信息加密模块中，服务器端采取分级加密的方式保障用户个人信息安全。以用户购物下单为例，在接收到客户端提交的订单信息后，服务器端对信息内容进行分级加密处理，主要的快件信息包括寄件人姓名、联系电话、订单物品的信息以及地址信息。

1) 对订单物品信息不加密，打印到快递单中方便物流途中的运输。

2) 对寄件人姓名、联系电话进行一次 RSA 加密，为方便理解，命名为 R1。

3) 对地址信息进行分层处理，如订单地址为四川省成都市双流区西航港 xxx，服务器会将四川省设置为省级，单独进行一次 RSA 加密（即为 R2），以此类推成都市设置为市级（即为 R3），双流区设置为县级（即为 R4），西航港 xxx（具体地址）为 R5。

3.2.1 密钥管理模块

分段加密方案对快件采用随机生成的密钥。对于密钥管理，本文提出两种方案。方案一是数据量不大时所采用的。为了最大限度地保护用户的隐私信息，本文对于每一个快件采用不同的密钥加密。方案二是针对大规模数据量（“双十一”等特殊时段）查询的情况，采用分时更新密钥方案，即每一级站点在某一时间段中所有的快件采用同样的公私钥。同时为了防止密钥泄露，采用对密钥进行定时更新。在这两种方案中会产生很多密钥，对密钥的授权管理也是该项目的重中之重。该模块设计主要采用分级授权管理方式，在生成快递面单时，服务器将面单信息进行分段，然后对每一段分别采用 RSA 加密，同时将不同分段加密的密钥保存在不同的数据库中，对于不同的数据库授予不同的访问权限，分别对应省级、市级和县级；当快件达到某一级时，某一级相关管理人员向服务器提出请求，服务器接受请求后根据其所属访问权限在数据库中获取相应的解密密钥返回给请求端，相应级别的请求端根据收到的密钥解析下一级的网点信息并分派快件。需要注意的是，各级所有密钥均统一管理，每一级的解密密钥只能解析出下一级的信息，每一级所获取信息均十分有限，仅最后一级快递派送员能获取收件人具体地址，尽可能地保护收件方的隐私安全。

3.2.2 物流模块

对于整个方案来说，物流模块也是极其重要的。之前所做的一切都是在为该模块做铺垫，在

传统的物流方案中[9]，用户的信息泄露基本是出于该环节。在快件的运输过程中，用户的包裹经过很多网点，会接触到很多内部人员。而这每一个网点都可能成为泄密的源头（曾经出现快递公司内部员工倒卖用户数据的情况）。该方案采用分段加密、分级授权的方法减少这一环节的信息泄露。现有的物流系统都是分级运输的方式，如一个由成都市寄往江苏省扬州市宝应县东门社区安宜东路 6 号的快递，一般的流程是先将快件运输到江苏省集散中心，然后运送到扬州市的快件中心，接着下一站点是宝应县，最后是派件的过程，派件员根据具体地址将用户的快递送达。在这个过程中，对于上一级的快递网点，只需要知道下一级的目的地即可，而其他的信息无关紧要。本文方案就是基于这样的原理，采用分级授权的机制。在信息加密的模块将收件人的所有信息全部分段加密，分别生成密钥，存储在服务器端。当快件前往下一个站点时，扫描 QR 码，服务器根据该站点的权限，下发对应的私钥，然后解密查看下一级的地址，而其余的信息则仍处于加密状态无法正常读取，如图 3 所示。

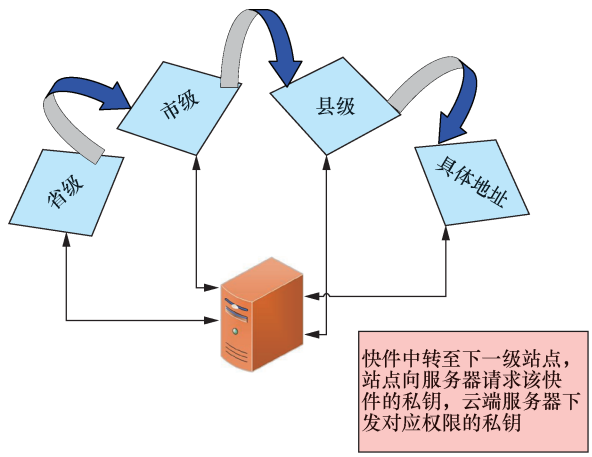


图 3　分级授权解密示意

这样既防止了用户信息的泄露，又可以让该快件根据扫描的信息顺利前往下一级网点。在整个过程的末端——派件的过程中，派件员根据其所具有的权限解密用户的名字、电话和具体地址。这对于用户的隐私存在极大的风险，所以在这一级不将 QR 码扫描出的结果直接显示给派件员。对于用户的具体地址，后台会根据扫描的结果直接智能地规划派件路线并显示在派件端。如果派件员需要短信通知或者电话联系收件人，该方案提供了一键拨号和发送短信的功能。派件员单击一键拨号，系统会给用户直接拨打电话，同时采用双向通信隐藏的方案。在这个过程中，用户接收到的号码是一个被标注的虚拟号码，派件员看到的电话号码也不是真正的用户电话。这样就实现了用户号码的保护。如果派件员需要发送短信，需要单击发送短信的按钮，服务器发送取件短信给用户，然后将发送的结果返回给派件员，提示其短信是否发送成功。这样派件员无法查看用户的具体信息但派件工作又可顺利完成。

3.3　双向认证设计

在日常的生活中经常会发生这样的事：你没有在网上购买任何商品，但却莫名奇妙地接收到取件的短信通知，最后不得不通过现场支付的方式接收快件。这其实是一种诈骗手段，非法分子通过伪造取件短信然后诱骗用户为假快递买单。这种问题存在的主要原因是快递流程中缺乏末端的[10]双向验证，之前所有的快递基本是单向认证的。用户出示身份证或者取件码，派件员核实之后将快递交给用户。但这个过程中，从来没有对派件员的真实身份进行认证，以致出现上述的假冒问题。基于这样的背景，本文创造性地引入了双向认证机制（mutual authentication）[11]。在整个物流的末端，用户出示快件的 QR 码，派件员使用专用的手持机对其进行扫描，然后在后台进行快件信息与扫描信息的匹配，如果信息匹配成功，则自动在后台完成签收，将签收状态信息发送给用户。整

个过程中，因为只有真正的快递公司员工才拥有登录手持机的权限，所以能很好地认证其身份的真实性。双向认证机制可以很好地解决假冒的问题，在物流末端为用户提供强有力的隐私保护。

3.4 时效控制设计

虽然目前市面上有采用 QR 码进行加密的快递，但普遍存在一个问题[12]。在快递签收之后，快递单上的 QR 码还是有效的，可以正常进行扫描访问。如果用户的密码发生泄露，即使完成了签收，不法分子还是可以通过扫描签收过后的 QR 码读取用户的个人隐私。这对用户的信息会造成很大的威胁，这里提出了时效控制方案。通过对 QR 码以及密钥设置有效时间来限制其访问。对密钥的时间控制也是通过分级进行实现的。当每一级实现解密访问之后，该级的密钥就失效，以防止内部人员进行私自访问。在整个物流周期结束之后，QR 码自动失效，这样就能实现用户隐私的全方位保护。

4 实验设计&结果分析

4.1 实验设置

为了验证本文的分段加密设计以及时效控制等方案，本文使用 QR 码存储快递单的加密信息，然后使用测试程序进行验证，同时和文献[2]进行对比分析。

4.2 分段加密

分段加密思想是对快件信息进行分级加密。不同级别的地址采用不同的密钥进行加密，同时每一个快件的密钥都是不同的，这样可以最大限度地保护用户的个人隐私信息。这里首先对地址信息“甘肃省金昌市永昌县四川大学江安校区”以及收件人信息“郭文博”（电话“13258280000”）进行加密。分段加密的过程如表 1 所示。

表 1 分段加密过程

明文信息	密钥	密文
甘肃省	*RSA*1	*C*1
金昌市	*RSA*2	*C*2
永昌县	*RSA*3	*C*3
四川大学江安校区 郭文博 13258280000	*RSA*4	*C*4
C1‖C2‖C3‖C4	*RSA*5‖*Base*64	*C*5

加密之后生成的 QR 码如图 4 所示。

图 4 个人信息集成后的 QR 码

接下来进行扫描测试。首先使用普通的扫描工具进行扫描。该过程中没有解密的密钥，所以扫描的结果是已经加密的，如图 5 所示。

图 5 常规扫描软件扫描结果

然后使用授权的软件进行扫描，这里测试的是市级密钥，所以扫描的结果应该是下一级（即县级单位）的信息，如图 6 所示。

图 6 授权密钥解密结果

4.3　时效控制

时效控制是通过在快件的地址信息后加入一个 Time_Expire 值设置超时时间来实现 QR 码自动失效的。当生成 QR 码时，服务器端在快件信息后加入 Time_Expire 值，再进行分段加密。当服务器端接收到查询请求后，通过对 Time_Expire 值进行判断，决定是否返回明文信息。若 QR 码的 Time_Expire 值未超时，则返回相应权限的明文信息；若超时，则返回 QR 码失效提示。

仍以地址信息“甘肃省金昌市永昌县四川大学江安校区”为例生成 QR 码，时效控制过程如下。

使用授权的软件进行扫描，此时 QR 码还未失效，可以正常地得到明文信息扫描的结果，如图 6 所示。

接下来，QR 码失效后，再次进行扫描，扫描后不会得到明文信息，而是弹出 QR 码失效提示。扫描结果如图 7 所示。

图 7　QR 码时效扫描结果

4.4　双向认证

在双向认证中，如果用户签收，需要对快递员出示快件 QR 码。而 QR 码必须用户登录账号后才可以查看。系统后台自动匹配快件信息，如果匹配成功，则自动完成签收（如图 8 所示）；如果信息不匹配的话，就无法完成签收。

图 8　双向认证签收效果

4.5　对比分析

本文参考“基于二维码和信息隐藏的物流系统隐私保护方案”一文[2]。对其中的物流隐私方案进行了改进并对比分析，表 2 为本文方案与文献[2]方案的对比结果。

从表 2 中可以看出，对于加密方案来说，分段加密采用 RSA、Base64 算法更加安全。对于用户验证方案来说，派件员扫描收件人出示的 QR 码进行双向验证，在此过程中可以实现派件员以及收件人的互相认证，可以提供更好的身份验证效果，而验证码存在伪冒风险且无法对派件员身份进行鉴别。对于时效控制来说，文献[2]中无时效控制，用户签收之后 QR 码继续有效，这就增加了信息泄露的风险。对于用户签收来说，个性化的 QR 码设计可以增加可辨识度，提高签收效率。

5　结束语

针对目前物流信息系统中用户个人隐私泄露以及市场上已存在物流系统保护用户隐私方法的缺陷，本文提出了一种基于 QR 码分段加密、分级授权和时效控制的方案，并且详细介绍了该方案的系统架构和模块设计以及实际应用流程。该方案根据实际快递物流个人信息实现分段 RSA、Base64 加密，并且针对不同区域，从省到市再到

表 2　2 种方案对比分析

方案	加密方案	用户验证方案	QR 码时效	收件效率
本文方案	分段加密	双向验证	签收后失效	高（个性化 QR 码有助于标识）
文献[2]方案	信息隐藏	验证码验证	签收后继续有效	低（无法区分快件）

县级分别授予不同的权限，当前一级只能查看当前和下一级的网点信息，并且 QR 码具有一定的时效性，包含用户信息的 QR 码在用户签收后立即失效，有效地提高了整个物流系统的安全性，很好地解决了传统物流系统中个人隐私泄露的问题，在尽量保证便捷的同时，提升系统的安全性。

随着互联网时代的飞速发展，物流快递的需求随之增长，人们对于个人隐私保护的意识逐渐提高，希望本文方案的设计在不久的将来能得到进一步的改进与应用；同时，对于方案中加密算法的高效性以及实际应用安全性和便捷性的研究还有待进一步深入。

参考文献：

[1] 中华人民共和国国家邮政局. 中国快递发展指数报告[R]. 2018. State Post bureau of the People's Republic of China. China Express Development Index Report [R]. 2018.

[2] 严文博, 姚远志, 张卫明, 等. 基于二维码和信息隐藏的物流系统隐私保护方案[J]. 网络与信息安全学报, 2017, 3(11): 22-28. YAN W B, YAO Y Z, ZHANG W M, et al. Privacy-preserving scheme for logistics systems based on 2D code and information hiding[J]. Chinese Journal of Network and Information Security, 2017, 3(11): 22-28.

[3] TAMM U. Possible applications of information theory in logistics[C]// Information Theory & Applications Workshop. 2011.

[4] ÖMÜR Y, SAATÇIOĞLU, DEVECI D A, CERIT A G. Logistics and transportation information systems in turkey: e-government perspectives[J]. Transforming Government People Process & Policy, 2009, 3(2):144-162.

[5] BRYCE J, KLANG M. Young people, disclosure of personal information and online privacy: control, choice and consequences[J]. Information Security Technical Report, 2009, 14(3):160-166.

[6] ZHANG X, LI H, YANG Y, et al. LIPPS: logistics information privacy protection system based on encrypted QR code[C]//IEEE Trustcom/BigDataSE/ISPA. 2016: 96-100.

[7] THIRANANTN , LEE Y S , LEE H. Performance comparison between RSA and elliptic curve cryptography-based QR code authentication[C]//IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA) 2015: 278-282.

[8] BOOKBINDER, JAMES H, DILTS D. Logistics information systems in a just-in-time environment[J]. Journal of Business Logistics, 1989, 10(1).

[9] BERGHEL H. Identity theft, social security numbers, and the Web[J]. Communications of the ACM, 2000,43(2).

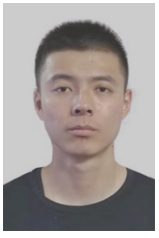
[10] HUANG C T , ZHANG Y H , LIN L C , et al. Mutual authentications to parties with QR-code applications in mobile systems[J]. International Journal of Information Security, 2016.

[11] SAXENA S,SANYAL G AND SRIVASTAVA S. Mutual authentication protocol using identity-based shared secret key in cloud environments[C]//International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014). 2014: 1-6.

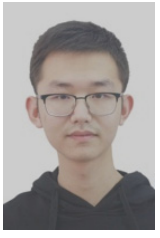
[12] KROMBHOLZK ,FRÜHWIRT, PETER, KIESEBERG P, et al. QR code security: a survey of attacks and challenges for usable security[C]// International Conference on Human Aspects of Information Security. 2014.

[作者简介]

刘亮（1982− ），男，四川叙永人，博士，四川大学工程师，主要研究方向为恶意代码检测、漏洞挖掘、大数据安全。



郭文博（1998− ），男，甘肃镇原人，主要研究方向为 Web 安全。



杨昱威（1999− ），男，陕西汉中人，主要研究方向为信息与通信工程。

郭怀宇（1998− ），男，四川自贡人，主要研究方向为网络空间安全。