对一个基于身份的密钥协商协议的分析与改进

郭 华[1] 张 帆[1] 李舟军[1] 周晓娟[2]
(北京航空航天大学计算机学院 北京 100083)[1] (河南经贸职业学院信息管理系 郑州 450002)[2]

摘 要 根据2007年王圣宝等人提出的一类基于身份的密钥协商协议的特点,对私钥泄漏模仿攻击的分类进行了扩充,之后具体分析了王等人的协议,发现该协议不能抵抗扩充的私钥泄漏模仿攻击。进一步分析了存在攻击的原因,并对协议进行了改进,最后对改进后的协议的安全性质进行了分析。

关键词 基于身份的密码学,认证密钥协商协议,双线性配对,模仿攻击
中图法分类号 TP309 **文献标识码** A

Cryptanalysis and Improvement of a New Identity-based Key Exchange Protocol

GUO Hua[1] ZHANG Fan[1] LI Zhou-jun[1] ZHOU Xiao-juan[2]
(School of Computer Science & Engineering, Beihang University, Beijing 100083, China)[1]
(Department of Information Management, Economic and Trade Vocational College of Henan, Zhengzhou 450002, China)[2]

Abstract This paper extended the definition of key-compromise-impersonate attack according to a new kind of identity-based key exchange protocol presented by Wang in 2007, then showed that this protocol can't resist the extending key-compromise-impersonate attack. This paper also conducted a detailed analysis on the flaw. To avoid this shortcoming, an improvement of the identity-based protocol was proposed based on the original scheme.

Keywords Identity-based cryptography, Authenticate key agreement protocol, Bilinear pairing, Impersonate attack

1 引言

基于身份的密码学(Identity Based Cryptography, IBC)的概念最早由 Shamir[1] 于 1984 年提出。在该体制下,终端用户可任意选取一个身份字符串作为自己的公钥,存在一个可信密钥产生中心(KGC),秘密持有一个主私钥,它将主私钥和用户身份相结合生成用户私钥。2001 年,Boneh 和 Franklin[2] 利用双线性对(Bilinear Pairing)给出了第一个可证安全的基于身份的加密(Identity Based Encryption, IBE)方案,之后,Smart[3] 结合文献[2]的加密方案和 Joux[4] 的基于双线性对的三方密钥协商协议,第一个使用双线性对设计了基于身份的认证密钥协商协议。此后,如何使用双线性对构造基于身份的密钥协商协议成为一个研究热点[5-12]。但这些协议的安全性都不是在标准模型下证明的。

2006 年,Gentry[13] 提出了一个全新的基于身份的加密方案,并第一次在标准模型下证明了方案的安全性。之后,王圣宝[14] 等人基于 Gentry[13] 的体制构造了一个基于身份的认证密钥协商协议,同样也在标准模型下证明了协议的安全性,从而保证协议满足一些基本的安全性质,如已知密钥安全、抗密钥泄漏伪装攻击(KCI)及抗未知密钥共享等。这是截至目前为止第一个在标准模型下可证安全的基于身份的密钥协商协议。但该协议中用户的私钥不仅依赖于 KGC 的主私钥,还依赖于它产生的一个随机数,从而即使 KGC 的主私钥泄漏,只要随机数没有泄漏,用户的私钥就不会被泄漏。鉴于此,我们认为对此类协议除了要考虑一般意义下的密钥泄漏模仿攻击,还要考虑 KGC 主私钥泄漏时的模仿攻击。因此,本文扩展了私钥泄漏模仿攻击的定义,即引入了主私钥泄漏模仿攻击的概念。随后分析了文献[14]中的协议,发现该协议不能抵抗此类攻击,给出了存在攻击的原因。之后对协议进行改进,最后分析了改进后协议的安全性质。

2 对密钥泄漏模仿攻击的扩展定义

本节回顾密钥泄漏模仿攻击的定义,并在此基础上给出主密钥泄漏模仿攻击及增强的密钥泄漏模仿攻击的扩展定义。假设实体 A 和 B 是两个协议参与者。

定义 1[15](密钥泄漏模仿攻击,Key Compromise Impersonation, KCI) 密钥泄漏模仿攻击是一种已知密钥的攻击,即当 A 的长期私钥泄漏之后,攻击者可以向 A 冒充 B。

上述定义考虑了实体 A 的长期私钥的泄漏,在传统的 PKI 体制下可满足需要。但在 IBC 体制中,私钥包括用户私钥和 KGC 的私钥。截至目前,除了文献[13,14],其它已知的 IBC 体制中用户私钥均由 KGC 利用用户的身份和主私钥生

到稿日期:2009-11-13 返修日期:2010-02-04 本文受国家自然科学基金项目(60473057,60973105),国家密码发展基金密码理论课题(200706039),北京航空航天大学博士生创新基金(211619)资助。

郭 华(1980—),女,博士生,主要研究方向为安全协议的可证明安全理论,E-mail:hguo.xyz@163.com;张 帆(1981—),女,博士生,主要研究方向为密码协议;李舟军(1963—),男,博士,教授,CCF 会员,主要研究方向为信息安全;周晓娟(1979—),女,硕士,助教,主要研究方向为信息安全。

成，主私钥 s 的泄漏即相当于所有用户私钥的泄漏。因此当考虑这种协议的 KCI 攻击时，通常假设攻击者获得了一个实体的私钥(如 A 的私钥 d_A)，而不允许主私钥 s 的泄漏。在文献[14]的协议中，KGC 产生用户私钥时除了使用主私钥 s，还要使用自己的一个随机数。此时即使 s 泄漏，只要 KGC 的随机数(每个给定的身份 ID 都赋予固定的随机数)没有泄漏，实体的私钥就不会泄漏。因此，在这类协议中除了要考虑实体私钥的泄漏，还要考虑 KGC 主私钥的泄漏。

下面引入主私钥泄漏模仿攻击和增强的私钥泄漏模仿攻击的概念。

定义 2(主私钥泄漏模仿攻击，Master-Key Compromise Impersonation，MKCI) 若实体的私钥不完全依赖于 KGC 的主私钥，则当 KGC 的主私钥泄漏之后(实体私钥未泄漏)，攻击者可以向一个实体(如 A)冒充另一个实体(如 B)。

定义 3(增强的私钥泄漏模仿攻击，Strengthen Key Compromise Impersonation，SKCI) 若实体的私钥不完全依赖于 KGC 的主私钥，则当 KGC 的主私钥和实体 A 的长期私钥泄漏之后，攻击者可以向 A 冒充 B。

易知，一个协议若可抵抗增强的私钥泄漏模仿攻击，则一定能抵抗私钥泄漏模仿攻击和主私钥泄漏模仿攻击。

3 王等人的协议

王圣宝等人在文献[14]中给出了两个基于身份的密钥协商协议 IBAK-1 及 IBAK-2，其中 IBAK-1 带有密钥托管性质，IBAK-2 去除了密钥托管性质，因此本文只分析 IBAK-2。若后者不能抵抗主密钥泄漏模仿攻击和增强的密钥泄漏模仿攻击，则前者也不能抵抗。首先回顾协议 IBAK-2。

设群 G_1 及 G_2 的阶皆为素数 p，且 $e:G_1\times G_1\to G_2$ 是一个可接受的双线性配对。协议包括 3 个阶段：系统建立、用户密钥提取及密钥协商。设用户 A 和 B 希望利用协议 IBAK-2 协商获取一个共享的会话密钥，协议描述如下：

• 系统建立阶段(Setup)。私钥生成中心 KGC 首先随机选择 3 个生成元 $g,h,t\in G_1$ 及一个随机整数 $\alpha\in Z_p$，然后计算 $g_1=g^{\alpha}\in G_1$。KGC 将系统公共参数 params 设置为 $\langle g,g_1,h,t\rangle$，主私钥设置为 α。

• 私钥生成阶段(Key-Gen)。在替身份为 $ID\in Z_p$ 的用户生成长期私钥之前，KGC 首先随机选取 $r_{ID}\in Z_p$ 并输出该用户的长期私钥 $d_{ID}=\langle r_{ID},h_{ID}\rangle$，其中 $h_{ID}=(ht^{-r_{ID}})^{1/(\alpha-ID)}$。KGC 确保 $\alpha\neq ID$ 且对每个给定的身份 ID 都赋予固定的 r_{ID}。

分别令 $g_A=g_1g^{-ID_A}$，$g_B=g_1g^{-ID_B}$ 及 $g_T=e(g,t)$。A 和 B 的长期私钥分别为 $\langle r_A,h_A\rangle$ 及 $\langle r_B,h_B\rangle$。协议执行如下：

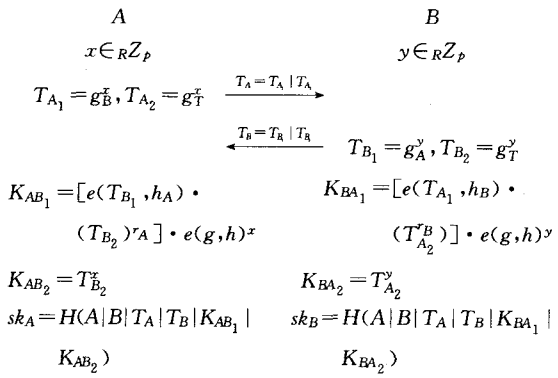

图 1 协议 IBAK-2

• 密钥协商阶段(Key Agreement)。A、B 首先分别随机选取临时私钥 $x,y\in Z_p$，并计算相应的临时公钥 $T_{A_1}=g_B^x$，$T_{A_2}=g_T^x$ 及 $T_{B_1}=g_A^y$，$T_{B_2}=g_T^y$。之后相互交换数据 $T_A=T_{A_1}|T_{A_2}$ 和 $T_B=T_{B_1}|T_{B_2}$，如图 1 所示。

收到 T_B 后，A 计算共享秘密如下：

$$K_{AB_1}=e(T_{B_1},h_A)\cdot(T_{B_2})^{r_A}\cdot e(g,h)^x=e(g,h)^{x+y}$$

$$K_{AB_2}=T_{B_2}^x=e(g,t)^{xy}$$

同样地，B 计算共享秘密如下：

$$K_{BA_1}=e(T_{A_1},h_B)\cdot(T_{A_2})^{r_B}\cdot e(g,h)^y=e(g,h)^{x+y}$$

$$K_{BA_2}=T_{A_2}^y=e(g,t)^{xy}$$

通过运行一次协议，A 和 B 成功地协商获得了共享秘密 $K_1=K_{AB_1}=K_{BA_1}$ 及 $K_2=K_{BA_2}=K_{AB_2}$，从而最终的会话密钥为 $sk=H(A|B|T_A|T_B|K_1|K_2)$，其中 $H:\{0,1\}^*\to\{0,1\}^k$ 为密钥抽取函数，k 表示会话密钥的长度，即 $k=|sk|$。

4 对协议 IBAK-2 的分析

文献[14]利用文献[11]中定义的安全模型，在标准模型下证明了协议 IBAK-2 的安全性，即协议可保持已知密钥安全的性质，并可抵抗 KCI 攻击及未知密钥共享攻击。本节发现该协议不能抵抗第 2 节定义的扩展的私钥泄漏模仿攻击。

4.1 主私钥泄漏模仿攻击

首先分析协议不能抵抗主私钥泄漏模仿攻击。

假设一个攻击者 C 获得了主私钥 α(但产生用户长期私钥所需的随机数未泄漏)，则 C 试图向 A 模仿 B 如下：

• A 随机选取一个临时私钥 $x\in Z_p$ 并计算相应的临时公钥 $T_{A_1}=g_B^x$ 与 $T_{A_2}=g_T^x$。之后发送 $T_A=T_{A_1}|T_{A_2}$ 给 B。

• C 拦截消息 T_A 并随机选取一个临时私钥 $z\in Z_p$，计算相应的临时公钥 $T_{C_1}=g_A^z$ 及 $T_{C_2}=g_T^z$。之后，C 发送 $T_C=T_{C_1}|T_{C_2}$ 给 A。

• 收到 T_C 后，A 计算共享秘密(the shared secret)如下：

$$K_{AB_1}=e(T_{C_1},h_A)\cdot(T_{C_2})^{r_A}\cdot e(g,h)^x=e(g,h)^{x+z}$$

$$K_{AB_2}=T_{C_2}^x=e(g,t)^{xz}$$

• 由于 C 知道 α，由 $T_{A_1}=g_B^x=g^{(\alpha-ID_B)\cdot x}=(g^x)^{\alpha-ID_B}$，$C$ 首先计算 g^x。C 进一步计算其共享秘密如下：

$$K_{CA_1}=e(g^x,h)\cdot e(g,h)^z=e(g,h)^{x+z}$$

$$K_{CA_2}=T_{A_2}^z=e(g,t)^{xz}$$

一次协议运行结束后，C 成功地模仿 B 与 A 协商获得了一个会话密钥 $sk=H(A|B|T_A|T_C|K_{CA_1}|K_{CA_2})$，如图 2 所示。

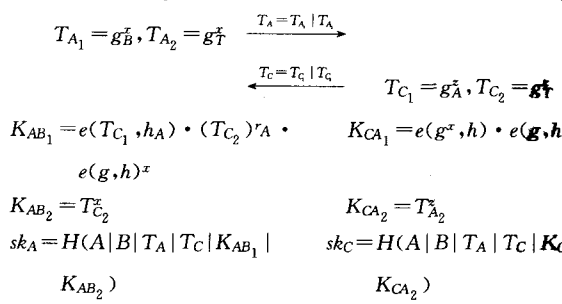

图 2 主私钥泄漏模仿攻击

4.2 增强的私钥泄漏模仿攻击

由上节知，该协议不能抵抗主私钥泄漏模仿攻击，那么由

定义 3，该协议也不能抵抗增强的私钥泄漏模仿攻击。本节给出一种不同的增强的私钥泄漏模仿攻击。

假设一个攻击者 C 获得了用户 A 的长期私钥 $\langle r_A, h_A\rangle$ 及 KGC 的主私钥 α（但产生用户长期私钥所需的随机数未泄漏），则 C 试图向 A 模仿 B。攻击如下：

• A 随机选取一个临时私钥 $x \in Z_p$ 并计算相应的临时公钥 $T_{A_1}=g_B^x$ 及 $T_{A_2}=g_T^x$。之后发送 $T_A=T_{A_1}\mid T_{A_2}$ 给 B。

• C 拦截消息 T_A 并随机选取一个临时私钥为 $z\in Z_p$，计算相应的临时公钥 $T_{C_1}=g_B^z$ 及 $T_{C_2}=g_T^z$。之后，C 发送 $T_C=T_{C_1}\mid T_{C_2}$ 给 A。

• 收到 T_C 后，A 计算共享秘密（the shared secret）如下：

$$\begin{aligned}K_{AB_1}&=e(T_{C_1},h_A)\cdot(T_{C_2})^{r_A}\cdot e(g,h)^x\\&=e(g_B^z,h_A)\cdot(g_T^z)^{r_A}\cdot e(g,h)^x\\&=e(g,ht^{-r_A})^{\frac{z\cdot(\alpha-ID_B)}{\alpha-ID_A}}\cdot e(g,t)^{z\cdot r_A}\cdot e(g,h)^x\end{aligned}$$

$$K_{AB_2}=T_{C_2}^x=e(g,t)^{xz}$$

• 由于 C 知道 α，由

$$T_{A_1}=g_B^x=g^{(\alpha-ID_B)\cdot x}=(g^x)^{\alpha-ID_B}$$

C 首先计算 g^x。利用 A 的私钥 $\langle r_A, h_A\rangle$，C 进一步计算共享秘密如下：

$$\begin{aligned}K_{CA_1}&=e(g_B^x,h_A)\cdot(T_{C_2})^{r_A}\cdot e(g^x,h)\\&=e(g,ht^{-r_A})^{\frac{z\cdot(\alpha-ID_B)}{\alpha-ID_A}}\cdot e(g,t)^{z\cdot r_A}\cdot e(g,h)^x\end{aligned}$$

$$K_{CA_2}=T_{C_2}^x=e(g,t)^{xz}$$

一次协议运行结束后，C 成功地模仿 B 与 A 协商获得了一个最终的会话密钥 sk，如图 3 所示。

A		$C(B)$
$x\in_R Z_p$		C 拦截，C 选择 $z\in_R Z_p$
$T_{A_1}=g_B^x, T_{A_2}=g_T^x$	$\xrightarrow{T_A=T_{A_1}\mid T_{A_2}}$	
	$\xleftarrow{T_C=T_{C_1}\mid T_{C_2}}$	$T_{C_1}=g_B^z, T_{C_2}=g_T^z$
$K_{AB_1}=e(T_{C_1},h_A)\cdot(T_{C_2})^{r_A}\cdot e(g,h)^x$		$K_{CA_1}=e(T_{C_1},h_A)\cdot(T_{C_2})^{r_A}\cdot e(g^x,h)$
$K_{AB_2}=T_{C_2}^x$		$K_{CA_2}=T_{A_2}^z$
$sk_A=H(A\mid B\mid T_A\mid T_C\mid K_{AB_1}\mid K_{AB_2})$		$sk_B=H(A\mid B\mid T_A\mid T_C\mid K_{CA_1}\mid K_{CA_2})$

图 3　增强的私钥泄漏模仿攻击

文献[11]指出，给出的安全模型涵盖了已知密钥安全、抗 KCI 攻击及抗未知密钥共享攻击等基本安全属性。由于王圣宝等人在该模型下证明了 IBAK-2 安全性质，因此 IBAK-2 也应满足上述基本的安全属性。但由上述分析，我们发现该协议不能抵抗主私钥泄漏模仿攻击和增强的私钥泄漏模仿攻击。通过对协议及安全模型的分析，我们从两个不同的角度给出导致已经证明安全的协议存在攻击的原因。

首先回顾文献[11]中的安全模型。当收到 corrupt 询问时，被询问的协议参与者返回自己的长期私钥，但不能返回 KGC 的主私钥，因此无法反映 KGC 主私钥泄漏的情况。也就是说，该模型不允许泄漏 KGC 的主私钥。这是不太现实的。因为在 IBC 中，KGC 是一个可信的私钥生成器，它利用一个固定的主私钥为域内所有用户产生并分发私钥。恶意攻击者可能通过一些非常手段获得主私钥，如果用户的私钥不仅仅依赖于 KGC 的主私钥，则我们希望主私钥的泄漏不影响协议的安全性质。其次，从协议本身来看，文献[14]指出，他们提出的协议只能够提供双向隐式密钥认证。由协议的消息流可以看出，两个参与者之间缺少相互的实体认证，因此攻击者拦截得到 A 的消息后，可以冒充 B 产生消息并发送给 A 而不被 A 所察觉。参与者继续执行协议，最终生成一个会话秘密，而攻击者也可以利用自己已有的知识产生一个完全相同的会话秘密，从而最终与 A 建立一个共享的会话密钥。

4.3　协议的改进及分析

本节给出协议的改进。改进的思想是：参与者发送第一个消息及其签名。当收到对方发送的消息后，首先对消息进行验证。若验证通过，则计算最终的会话秘密。改进后的协议如图 4 所示。

协议运行结束后，A 计算最终的会话秘密为：

$$K_{AB_1}=e(T_{B_1},h_A)\cdot(T_{B_2})^{r_A}\cdot e(g,h)^x=e(g,h)^{x+y}$$

$$K_{AB_2}=T_{B_2}^x=e(g,t)^{xy}$$

同时，B 计算最终的会话秘密为

$$K_{BA_1}=e(T_{A_1},h_B)\cdot(T_{A_2})^{r_B}\cdot e(g,h)^y=e(g,h)^{x+y}$$

$$K_{BA_2}=T_{A_2}^y=e(g,t)^{xy}$$

A		B
$x\in_R Z_p$		$y\in_R Z_p$
$T_{A_1}=g_B^x, T_{A_2}=g_T^x$		$T_{B_1}=g_A^y, T_{B_2}=g_T^y$
$T_{A_3}=Sig_{d_A}(g_B^x)$		$T_{B_3}=Sig_{d_B}(g_A^y)$
	$\xrightarrow{T_A=T_A\mid T_A\mid T_A}$	
	$\xleftarrow{T_B=T_B\mid T_B\mid T_B}$	
验证 T_{A_3}，若通过则计算		验证 T_{B_3}，若通过则计算
$K_{AB_1}=e(T_{B_1},h_A)\cdot(T_{B_2})^{r_A}\cdot e(g,h)^x$		$K_{BA_1}=e(T_{A_1},h_B)\cdot(T_{A_2})^{r_B}\cdot e(g,h)^y$
$K_{AB_2}=T_{B_2}^x$		$K_{BA_2}=T_{A_2}^y$
$sk_A=H(A\mid B\mid T_A\mid T_B\mid K_{AB_1}\mid K_{AB_2})$		$sk_B=H(A\mid B\mid T_A\mid T_B\mid K_{BA_1}\mid K_{BA_2})$

图 4　改进后的协议

下面分析改进后协议的安全性质。

• 已知密钥安全（Known Key Security）。由于最终产生的共享的会话秘密只与当前会话中的临时私钥 x, y 有关，因此当两个协议参与者之间共享的某个会话密钥泄露之后，攻击者无法根据已获得的会话密钥求出其它会话密钥。

• KGC 前向安全（Perfect Forward Security，KGC-FS）。由于协议参与者的长期私钥不仅仅依赖于 KGC 的主私钥，因此 KGC 前向安全性不再蕴涵完美前向安全性，需将两者分开考虑。首先考虑 KGC 前向安全性。若攻击者获得 KGC 的主私钥，则可分别计算 $e(g,h)^x$ 与 $e(g,h)^y$，从而可计算会话秘密的第一个分量 $e(g,h)^{x+y}$。但攻击者不能计算第二个分量 g_T^{xy}，因为根据 g_T, g_T^x 和 g_T^y 计算共享秘密 g_T^{xy} 是群 G_2 上的计算性 Diffie-Hellman（Computational Diffie Hellman，CDH）难问题，所以无法计算获得 A 和 B 之间的共享会话密钥。

• 完美前向安全（Perfect Forward Security，PFS）。若两个协议参与者的长期私钥都泄露，此时攻击者可以计算会话秘密的第一个分量，但攻击者不能计算获得第二个分量 g^{xy}，因为根据 g_T, g_T^x 和 g_T^y 计算共享秘密数 g_T^{xy} 是群 G_2 上的

CDH 难问题，所以无法计算用户 A 和 B 之间的共享会话密钥。

·增强的密钥泄漏模仿攻击(Strengthen Key Compromise Impersonation resilience)。假设攻击者获得了 KGC 的主私钥和 A 的私钥，则当攻击者用自己的私钥对第一个消息分量签名并发送给 A 时，由于 A 认为拟定的接收者为 B，因此利用 B 的身份信息进行验证。一旦 A 验证失败，A 立即知道有人冒充 B 与自己执行协议，因此 A 取消协议。从而攻击者 C 不能冒充 B 与 A 建立共享的会话秘密。由定义 1、定义 2 及定义 3 可知，协议若能抵抗增强的私钥泄漏模仿攻击，则一定能抵抗私钥泄漏模仿攻击和主私钥泄漏模仿攻击。

结束语 本文比较近几年基于身份的密钥协商协议后，认为王等人提出的基于身份的密钥协商协议比较特殊。根据该协议的特点，首先对私钥泄漏模仿攻击的分类进行了扩充，具体分析了王等人的协议，发现他们的协议不能抵抗主私钥泄漏模仿攻击与增强的私钥泄漏模仿攻击。之后分析了存在攻击的原因，并对协议进行了改进。最后分析了改进后协议的安全性质。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology- Crypto'84. Springer, Heidelberg, 1984, LNCS 196: 47-53

[2] Boneh D, Franklin M. Identity based encryption from the Weil pairing[C]// Advances in Cryptology-Crypto'2001. Springer, Heidelberg, 2001, LNCS 2139: 213-229

[3] Smart N P. An identity based authenticated key agreement protocol based on the Weil pairing[J]. Electro. Lett., 2002, 38: 630-632

[4] Joux A. A one-round protocol for tripartite Diffie-Hellman[C]// Algorithmic Number Theory Symposium-ANTS-IV. Springer, Heidelberg, 2000, LNCS 1838: 385-394

[5] Shim K. Efficient ID-based authenticated key agreement protocol based on the Weil pairing[J]. Electron Lett, 2003, 39: 653-654

[6] Chen L, Kudla C. Identity based authenticated key agreement from pairings[C]// IEEE Computer Security Foundations Workshop. 2003: 219-233

[7] Ryu E, Yoon E, Yoo K. An efficient ID-based authenticated key agreement protocol from pairings[C]// Networking 2004. Springer, Heidelberg, 2004. LNCS 3042: 1458-1463

[8] McCullagh N, Barreto P S L M. A new two-party identitybased authenticated key agreement[C]// Topics in Cryptology-CT-RSA 2005. Springer, Heidelberg, 2005, LNCS 3376: 262-274

[9] Choie Y, Jeong E, Lee E. Efficient identity-based authenticated key agreement protocol from pairings[J]. Appl. Math. Comput, 2005, 162: 179-188

[10] Chow S S M, Choo K-K R. Strongly-secure identity-based key agreement and anonymous extention[C]// ISC 2007. Springer, Heidelberg, 2007, LNCS 4779: 203-220

[11] Chen L, Cheng Z, Smart N P. Identity-based key agreement potocols from pairings[J]. International Journal Information Security, 2007, 6: 213-241

[12] Zhu R W, Yang Guomin, Wong Duncan S. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices Source[J]. Theoretical Computer Science, 2007, 378(2): 198-207

[13] Gentry C. Practical identity based encryption without random oracles[C]// Proceedings of the EUROCRYPT'06. Springer Verlag, Berlin, 2006, LNCS 4004: 445-464

[14] 王圣宝，曹珍富，董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报，2007，30(10)：1842-1852

[15] Boyd C, Mathuria A. Protocols for Authentication and a Key Establishment[M]. Berlin: Springer Verlag, 2003

(上接第 70 页)

[2] Guvenc I, Arslan H. On the Modulation Options for UWB Systems[C]//Boston. IEEE Mil. Commun. Conf. 2003, 2: 892-897

[3] Gong Yun-rui, He Di, He Chen, et al. Efficient Modulation on the Performance of Coherent Receivers for Pseudo-chaotic TH-UWB System[C]//Macao. IEEE Asia Pacific Conf. on Circ. and Syst. 2008: 1094-1097

[4] Weisenhorn M, Hirt W. Robust Noncoherent Receiver Exploiting UWB Channel Properties[C]//Kyoto. IEEE UWB Systems Joint with Conf. on UWB Syst. and Technol. Joint UWBST & IWUWBS. Intl. Workshop. 2004: 156-160

[5] Yang Liu-qing, Giannakis G B, Swami A. Noncoherent Ultra-Wideband(De)Modulation[J]. IEEE Transactions on Communications, 2007, 55(4): 810-819

[6] Goeckel D L, Mehlman J, Burkhart J. A Class of Ultra Wideband (UWB) Systems with Simple Receivers[C]// Orlando. IEEE Mil. Commun. Conf. 2007, 10: 1-7

[7] Godara B, Blamon G, Fabre A. UWB: A New Efficient Pulse Shape and its Corresponding Simple Transceiver[C]// Siena. IEEE 2nd Intl. Symposium on Wireless Commun. Syst. 2005, 9: 365-369

[8] Zaman A A, Islam N. Modulation Schemes and Pulse Shaping in Ultra-wideband[C]// Huntsville. IEEE Southeastcon. 2008, 4: 142-146

[9] Win M, Scholtz R A. Impulse Radio: How It Works [J]. IEEE Commun. Letters, 1998, 2: 36-38

[10] Zhang L, Wang S, Deng T P, et al. A Novel Demodulation Method based on Zero-Crossing Detection for UWB Signal Reception[C]// Beijing. WiCom '09. 5th Intl. Conf. on Wireless Comm. Networks Sec. Networking and Mobile Computing. 2009, 9: 1-4

[11] Foerster J. Channel modelling sub-commitee report final[R]. IEEE P802. 15-02/368r5-SG3a. 2002