基于广义 XTR 体制的签名方案 [1]

陈晓峰 王继林 王育民

(西安电子科技大学 ISN 国家重点实验室 陕西西安 710071)

摘 要: 与 RSA 和 ECC 相比较，同等安全程度下 XTR 密钥长度远远小于 RSA，最多只是 ECC 密钥长度的 2 倍；而 XTR 参数和密钥选取远远快于 ECC．该文利用有限域中元素迹的快速算法，给出了两种特殊的基于广义 XTR 体制的签名方案，其安全性等价于解广义 XTR 群中的离散对数困难问题，但是传输的数据量只有原来方案的 1/3．

关键词: 广义 XTR 公钥体制，数字签名，迹表示

中图分类号: TN918.1 **文献标识码**: A **文章编号**: 1009-5896(2004)04-0562-06

Signature Schemes Based on Extended XTR System

Chen Xiao-feng Wang Ji-lin Wang Yu-min

(*National Key Lab of ISN, Xidian University, Xi'an* 710071, *China*)

Abstract Compared with RSA and ECC, XTR keys are much smaller than RSA keys of equivalent security, and are at most twice as big as ECC keys, but parameter and key selections for XTR are much faster than ECC. With the fast method for computing the trace of the elements in the finite field, two blind signature schemes based on extended XTR system are presented in this paper, the security is equivalent to solving discrete logarithm problem of extended XTR group while the datum is only 1/3 of the previous schemes.

Key words Extended XTR public key system, Signature schemes, Trace representation

1 引言

XTR 公钥体制，即有效的紧致的子群迹表示，是由 Lenstra 等人 [1] 提出的，它是一种传统的基于子群离散对数问题的密码体系．它使用 GF(p^2) 的算术来达到 GF(p^6) 上的安全性，这样 XTR-DL 问题就比分解 $6\cdot\log_2 p$bit RSA 模更为困难．如果 p, q 取 170bit 的素数，则 XTR 就比 1020bit 的 RSA 更为安全．而且，XTR 的密钥和参数选取要比 ECC 简单，其指数计算比 ECC 标量乘计算快．所以，在同等的安全程度下，XTR 就大大减少了数据的存储量，计算量和通讯量．现在，许多新的改进和快速算法也已提出，XTR 已成为一种非常有吸引力的密码体制．

XTR 并不是最先使用迹表示和计算有限域的子群元素的方幂的体制，文献 [2] 首先提出使用有限域的扩域及其子群来降低所传输的数据量．然而，这种方法非常烦琐，效率不高．XTR 使用 GF(p^2) 的迹来表示 GF(p^6) 的阶为 p^2-p+1 子群的元素，从而使数据量大约降低到原来的 1/3．

近来，S. Lim[3] 等人将 XTR 体制推广到 GF(p^{6m})，我们称之为广义的 XTR 体制 (简记为 EXTR 体制)．由于现有的微处理器都是以 word 为单位对数据进行处理的，对特别大的整数必须用多个 word 表示，计算也非常复杂．广义的 XTR 体制可以选择与 word 相当的 p(如选

[1] 2002-11-02 收到，2003-03-03 改回
973 国家重大项目资助课题 (批准号: G19990358-04)

择 p 为一个大约 64bit 的素数)，从而避免了多精度运算的一些缺陷，如模规约运算、进位运算等。

S. Lim 等人指出： XTR 体制中的所有的基本算法和方案，如参数选取、迹的快速运算、密钥协商、消息加密、数字签名等都可以平行的推广到广义的 XTR 体制中。并且，他们对有些算法和协议进行了模拟。

然而，对一些特殊的方案如盲签名方案、群盲签名方案就无法平行的推广，这也许是由于有限域中元素的计算无法平行推广到元素迹的运算，如 $g^a g^b = g^{a+b}$，然而一般情形下 $\mathrm{Tr}(g^a)\mathrm{Tr}(g^b) \neq \mathrm{Tr}(g^{a+b})$。

利用基于离散对数问题的盲签名方案、群盲签名方案以及有限域中元素迹的快速算法，本文给出了基于广义 XTR 体制的盲签名方案和群盲签名方案，其安全性等价于解 EXTR-DL 困难问题。由于 EXTR 体制的优点，签名所交换的数据量约为原来的 1/3，这样就大大提高了盲签名方案、群盲签名方案的效率，从而也就大大提高了现有的基于离散对数体制的电子现金方案的效率。

2 EXTR 体制

2.1 系统参数

令 $p \equiv 2\mathrm{mod}3$ 是一个素数，$g \in \mathrm{GF}(p^{6m})^*$ 的阶为 q，其中 $m \in N$ 使得要么 $2m+1$ 是一个 Fermat 素数，要么 m, $2m+1$ 都是素数，$q | p^{2m} - p^m + 1$。对任意的 $a \in \mathrm{GF}(p^{6m})$, $\mathrm{Tr}(a) = a + a^{p^{2m}} + a^{p^{4m}} \in \mathrm{GF}(p^{2m})$ 是 a 的迹。给定 $\mathrm{Tr}(g)$，由 g 生成的 q 阶子群就称为 EXTR 群。

令 $c = \mathrm{Tr}(g)$，多项式 $F(c, X) = X^3 - cX^2 + c^{p^m} X - 1 \in \mathrm{GF}(p^2)[X]$。对整数 $n \in Z$ 我们定义 c_n 为 $F(c, X)$ 的根的 nth 方幂之和，即如果 $F(c, h_j) = 0$, $j = 0, 1, 2$, 则 $c_n = h_0^n + h_1^n + h_2^n = \mathrm{Tr}(g^n)$，显见 $c_1 = c$。关于 $F(c, X)$ 和 c_n 的一些基本性质及其详细的证明见文献 [1, 3]。

给定 c 和任意整数 n，可利用快速算法 [3] 计算 $\boldsymbol{S}_n(c) = (c_{n-1}, c_n, c_{n+1})$。用户选择秘密密钥 n 并通过计算 $\boldsymbol{S}_n(c)$ 得到对应的公钥。

2.2 EXTR 的一些基本性质

这一节我们简述 EXTR 的一些基本性质，细节可参阅文献 [3]。

定义 1　定义 $\boldsymbol{C}(V)$ 表示 3×3 矩阵 $\boldsymbol{V}$ 的中间列，而且

$$\boldsymbol{A}(c) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -c^{p^m} \\ 0 & 1 & c \end{pmatrix}, \qquad \boldsymbol{M}_n(c) = \begin{pmatrix} c_{n-2} & c_{n-1} & c_n \\ c_{n-1} & c_n & c_{n+1} \\ c_n & c_{n+1} & c_{n+2} \end{pmatrix}.$$

引理 1　给定 c 和 $\boldsymbol{S}_n(c)$ 则有 $\boldsymbol{C}(\boldsymbol{A}(c)^n) = \boldsymbol{M}_0(c)^{-1}(\boldsymbol{S}_n(c))^{\mathrm{T}}$。

引理 2　$c_{a+b} = \boldsymbol{S}_b(c)\boldsymbol{C}(\boldsymbol{A}(c)^a)$。

引理 3　因为 c_{n-1} (或 c_{n+1}) 可以通过 c, c_n 和 c_{n+1} (或 c_{n-1}) 表示出来，所以 c_{n-1}, c_{n+1} 就不必包括在 EXTR 公钥信息中。

证明　利用文献 [4] 的定理 5.1 和算法 5.2，可类似地推出引理 3。

3 迹的快速计算算法

有限域中元素的计算无法平行推广到元素迹的运算，如 $g^a g^b = g^{a+b}$，然而一般情形下 $\mathrm{Tr}(g^a) * \mathrm{Tr}(g^b) \neq \mathrm{Tr}(g^{a+b})$。所以，下面我们给出在 a, b 未知时利用 c_a, c_b 如何计算 c_{a+b} 的快速算法，这在盲签名及群盲签名方案中有着重要的作用。

算法 1　输入 c_a, c_b，输出 c_{a+b}。这里 a, b 是未知的整数。

步骤 1　使用文献 [2] 中算法 5.2 计算 c_{a+1}, c_{b+1}。

步骤 2　利用文献 [4] 中定理 5.1 计算 c_{a-1}, c_{b-1}，得到 $\boldsymbol{S}_a(c) = (c_{a-1}, c_a, c_{a+1})$, $\boldsymbol{S}_b(c) = (c_{b-1}, c_b, c_{b+1})$。

步骤 3 使用引理 1 计算 $\boldsymbol{C}(\boldsymbol{A}(c)^a) = \boldsymbol{M}_0(c)^{-1}(\boldsymbol{S}_a(c))^T$ 。

步骤 4 利用引理 2 计算 $c_{a+b} = \boldsymbol{S}_b(c)\boldsymbol{C}(\boldsymbol{A}(c)^a)$ ，输出 c_{a+b} 。

算法 2 令 $g,h \in \mathrm{GF}(p^{6m})^*$ 的阶为 q， $y = g^{-r}h^{-s}\mathrm{mod}q$ 。$\mathrm{Tr}(g), \mathrm{Tr}(h), \mathrm{Tr}(y) \in \mathrm{GF}(p^{2m})$ 分别是 g, h, y 的迹并公开 (g,h,y 不公开) 。那么对给定的 $\delta \in z_q$ ，则可快速计算出 $\mathrm{Tr}(y^\delta)$ 。

证明 因为素数 $q|p^{6m}-1$ ，则由 Lagrange 定理知 $\mathrm{GF}(p^{6m})^*$ 有一个 q 阶的循环子群，而且 g 可作为该子群的一个生成元。不妨设 $h = g^x\mathrm{mod}q$ ，于是 $y = g^{-r-sx}\mathrm{mod}q$ 。利用算法 1 就可快速计算出 $\mathrm{Tr}(y^2)$ ，重复调用算法 1 就可计算出 $\mathrm{Tr}(y^\delta)$ 。

当然，如果令 $\delta = \sum_{i=0}^{r}\delta_i 2^i$ ，其中 $\delta_r = 1$ 。使用 "平方乘" 算法可以更快地计算出 $\mathrm{Tr}(y^\delta)$ 。

证毕

4 基于 EXTR 体制的盲签名方案

盲签名由 D. Chaum[5] 提出，即签名者在未知消息 m 的情况下对 m 签名，任何人都可验证签名的正确性，然而签名者无法将消息-签名对与某一特定的签名协议联系起来。盲签名协议在电子现金方案的设计中有着重要的作用 [5−8] 。D. Chaum 给出了一种基于 RSA 体制的盲签名协议，后来 J. Camenisch[9] 提出了基于离散对数问题的盲签名方案。D. Pointcheval[10] 给出了一个随机预言模型下可证明安全的盲签名方案，下面我们将此方案推广到 EXTR 体制上。

4.1 EXTR-Blind-Okamoto-Schnorr 签名方案

令 $p \equiv 2\mathrm{mod}3$ 是一个素数， q 是 $\phi_{6m}(p)$ 的一个素因子。$g,h \in \mathrm{GF}(p^{6m})^*$ 的阶为 q, $\mathrm{Tr}(g)$, $\mathrm{Tr}(h) \in \mathrm{GF}(p^{2m})$ 公开 (g,h 不必公开) 。

A 的签名私钥为 $r,s \in z_q$ ，所对应的公钥为 $Y = \mathrm{Tr}(y) = \mathrm{Tr}(g^{-r}h^{-s}) \in \mathrm{GF}(p^{2m})$ 。B 所要签名的消息为 m ， $H(\cdot)$ 是一个安全的 hash 函数。

步骤 1 A 随机选择 $k,u \in z_q$ ，计算 $a = \mathrm{Tr}(g^k h^u) \in \mathrm{GF}(p^{2m})$ 并发送给 B 。

步骤 2 B 随机选择 β, γ, $\delta \in z_q^*$ ，利用算法 2 计算 $\alpha = \mathrm{Tr}(g^k h^u g^\beta h^\gamma y^\delta) \in \mathrm{GF}(p^{2m})$ 。

步骤 3 B 计算 $E = H(m,\alpha)$, $e = E - \delta\mathrm{mod}q$ 并发送 e 给 A 。

步骤 4 A 计算 $R = k + er\mathrm{mod}q$, $S = u + es\mathrm{mod}q$ 并发送 R, S 给 B 。

步骤 5 B 验证 $a = \mathrm{Tr}(g^R h^S y^e) \in \mathrm{GF}(p^{2m})$, 然后计算 $\rho = R + \beta\mathrm{mod}q$, $\sigma = S + \gamma\mathrm{mod}q$, 则对消息 m 的盲签名为 (ρ,σ,E) 。

验证 验证者首先计算 $\alpha' = \mathrm{Tr}(g^\rho h^\sigma y^E) \in \mathrm{GF}(p^{2m})$ ，如果 $H(m,\alpha') = E$ ，则签名正确。这是因为： $\alpha' = \mathrm{Tr}(g^\rho h^\sigma y^E) = \mathrm{Tr}(g^{R+\beta}h^{S+\gamma}y^{e+\delta}) = \mathrm{Tr}(g^{k+\beta}h^{u+\gamma}y^\delta) = \alpha$ 。

4.2 签名方案的分析

由于 XTR 体制本身的优点，签名方案中所交换的数据量是原来方案的 1/3 ，这样就大大提高了盲签名方案的效率，从而提高了电子商务中协议的效率。而且，类似于文献 [10] 的证明，我们可得到：在随机预言模型下，上述的 EXTR-Blind-Okamoto-Schnorr 签名方案是可证明安全的。

5 基于 EXTR 的群盲签名方案

群盲签名是 A.Lysyanskaya 和 Z.Ramzan 首次提出的。它在群签名的基础上增加了签名的盲性质：即签名者不能识别他签过的信息。引入群盲签名的主要目的是为了建立一个多银行的支付体系。最近，作者利用群盲签名方案给出了一种防止敲诈的电子现金方案 [5] 。

群盲签名方案的核心技术是基于双重离散对数知识证明盲签名和离散对数的 e 次方根知识证明盲签名。首先我们给出 EXTR 体制上知识签名的定义：

定义 2 令 $l \le k$ 是安全参数。对消息 m ，如果 $l+1$ 维向量 $(c,s_1,\cdots,s_l) \in \{0,1\}^k \times z_q^{*l}$ 满足方程 $c = H(m\|y\|g\|a\|t_1\|\cdots\|t_l)$ ，其中 $t_i = \begin{cases}\mathrm{Tr}(g^{a^{s_i}}), & c[i]=0\\ \mathrm{Tr}(y^{a^{s_i}}), & \text{其它}\end{cases}$ ，那么我们称它是 y 相

对于基 g, a 的双重离散对数知识签名，记为 SKLOGLOG$[\alpha : y = \mathrm{Tr}(g^{a^{\alpha}})](m)$. 这里 $H(\,)$ 是一个输出为 $k$bit 的安全的 hash 函数。

定义 3　令 $l \le k$ 是安全参数。对消息 m ，如果 $l+1$ 维向量 $(c, s_1, \cdots, s_l) \in \{0,1\}^k \times Z^l$ 满足方程 $c = H(m\|y\|g\|e\|t_1\|\cdots\|t_l)$ ，其中 $t_i = \begin{cases} \mathrm{Tr}(g^{s_i^e}), & c[i]=0 \\ \mathrm{Tr}(y^{s_i^e}), & \text{其它} \end{cases}$ ，那么我们称它是 y 相对于基 g 的 e 次方根的离散对数知识签名，记为 SKROOTLOG$[\alpha : y = \mathrm{Tr}(g^{a^e})](m)$.

5.1 基于 EXTR 体制的盲知识签名协议

我们只在图 1 中给出双重离散对数盲知识签名 (EXTR-BSKLOGLOG) 协议， e 次方根的离散对数知识盲签名 (EXTR-BSKROOTLOG) 协议可类似地给出。

在图 1 的协议中， λ, μ 是公开的安全参数， G_l 是一个 l 阶的置换群。

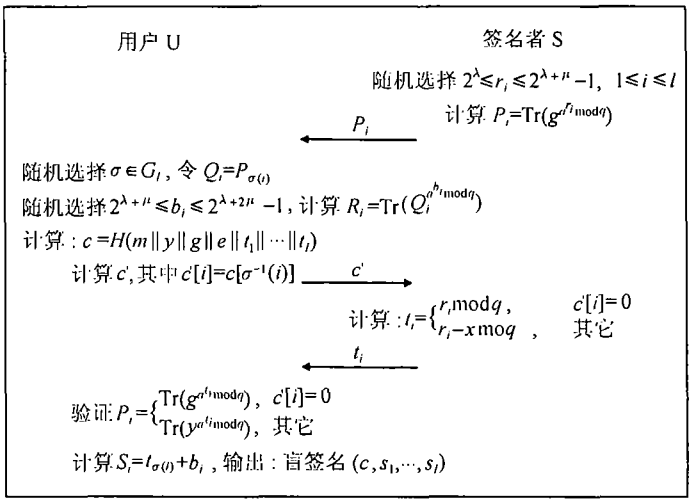

图 1　EXTR-BSKLOGLOG 协议

5.2 基于 EXTR 体制的群盲签名方案

我们的方案包括以下几个子协议：

(1) *群建立协议*　可信赖的第三方 TTP 充当群管理员，他选择如下的参数： RSA 公钥对 (n, e) ， EXTR 系统参数 $(\mathrm{GF}(p^{6m}), q, \mathrm{Tr}(g)), a$ 是模 n 的两个素因子都有大的乘数阶的 Z_n^* 中的固定元素。密钥上界 λ ，常数 ε 。群公钥是 $\Omega = (n, e, a, \mathrm{GF}(p^{6m}), q, \mathrm{Tr}(g), \lambda, \varepsilon)$ 。当一个用户 U 想加入该群体时，他通过图 2 的协议在 TTP 处注册并获得一个成员证书。

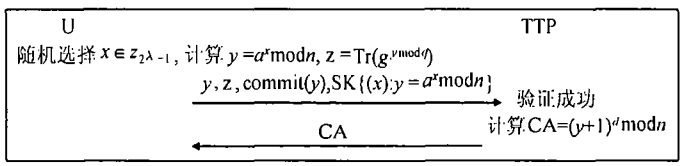

图 2　群建立协议

(2) *签名协议*　设签署的消息为 m ，用户 U 和签名者 S 通过图 3 所示的协议完成签名。

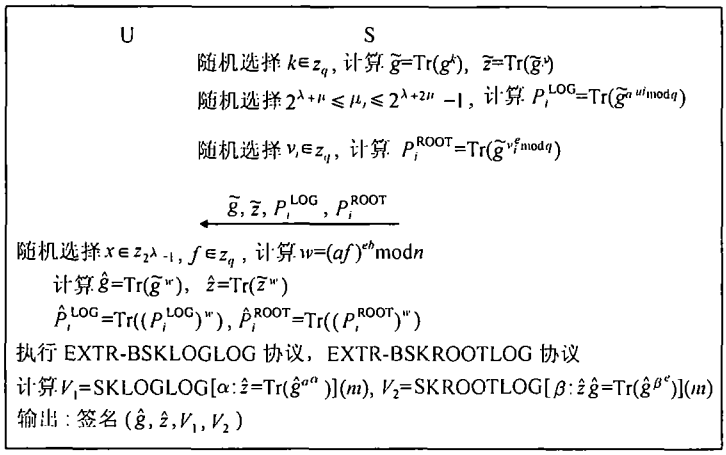

图 3 签名协议

(3) *追踪协议* 要追踪某个不诚实 (或恶意) 的用户，群管理员可通过搜索 y_P 使得 $\hat{z}=\mathrm{Tr}(g^{y_P \bmod q})$，$z=\mathrm{Tr}(g^{y_P \bmod q})$，即可找到该用户。时间复杂度为 $O(N)$，N 是群的大小。

方案安全性的论证类似于文献 [6]，方案所交换的数据量约是原有方案的 1/3 .

6 结论

XTR 是一种非常有吸引力的新的公钥密码体制。与目前实用的 RSA 和 ECC 公钥密码体制相比较 [11]，同等安全程度的 XTR 体制的实现在计算、密钥存储和通信方面的要求和 ECC 基本相同，但 XTR 的密钥生成要比 ECC 快的多，迹的计算也比点的标量乘运算要快。当然，如何进一步改进 XTR 的算法，优化参数选取，使 XTR 实用化，需要进一步的工作 [12−15]。广义的 XTR 体制可以选择与 word 相当的 p(如选择 p 为一个大约 64bit 的素数)，从而避免了多精度运算的一些缺陷，如模规约运算、进位运算等。

盲签名及群盲签名协议在电子方案的构造中起着非常重要的作用，本文利用迹的快速算法，给出了基于 XTR 的盲签名及其群盲签名方案，使所交换的数据量降低到原来的 1/3，从而大大提高了原有方案的效率。

当然，XTR(EXTR) 体制还有一些新的应用。最近，D. Han 等人 [16] 利用文献 [17] 中 Marking 的思想，基于 XTR 体制给出了一种防止敲诈的方案。

参 考 文 献

[1] Lenstra A K, Verheul E R. The XTR public key system. Crypto'2000, California, USA, LNCS 1880, Springer-Verlag 2000: 1–19.

[2] Brouwer A E, Pellikaan R, Verheul E R. Doing more with fewer bits. Proc. Asiacrypt'99, Singapore, LNCS 1716, Springer-Verlag, 1999: 321–332.

[3] Lim S, Kim S, Yie I, Kim J, Lee H. XTR extended to GF(p^{6m}). SAC 2001, Las Vegas, USA, LNCS 2259, 2001: 301–312.

[4] Lenstra A K, Verheul E R. Key improvements to XTR. Asiacrypt'2000, Kyoto, Japan, LNCS 1880, Springer-Verlag, 2000: 1–19.

[5] Chaum D. Blind signature for untraceable payments. Eurocrypt'82, Burg Feuerstein, Germany, Plenum Press, 1983: 199–203.

[6] Lysyanskays A, Ramzan Z. Group blind signatures: A scalable solution to electronic cash. Financial Cryptography'98, Anguilla, Britain, LNCS1465, Springer-Verlag, 1998: 184–197.

[7] Stadler M, Piveteau J M, Camenisch Jan. Fair blind signatures. Eurocrypt'95, St. Malo, France. LNCS 921, Springer-Verlag, 1995: 209–219.

[8] Brands S. Untraceable off-line cash in wallet with observes. Crypto'93, California, USA, LNCS 773, Springer-Verlag, Berlin, 1994: 302–318.
[9] Camenisch J L, Piveteau J M, Stadler M A. Blind signature based on discrete logarithm problem. Eurocrypt'94, Perugia, Italy. LNCS 950, Springer-Verlag, 1994: 428–432.
[10] Pointcheval D, Stern J. Provably secure blind Signature schemes. Asiacrypt'96, Kyongju, South Korea, LNCS 1163, Springer-Verlag, 1996: 252–265.
[11] Menezes A. Comparing the security of ECC and RSA, manuscript. 2000, www.carc.math.uwaterloo.ca/ajmeneze/misc/cryptopramartical.html. 2002-10-10.
[12] Verheul E R. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. Eurocrypt'2001, LNCS 2045, Innsbruck, Austria, Springer-Verlag 2001: 195–201.
[13] Lenstra A K, Verheul E R. Fast irreducibility and subgroup membership testing in XTR. PKC'2001, LNCS 1992, Cheju Island, Korea, Springer-Verlag, 2001: 78–86.
[14] Menezes A, Vanstoe S A. ECSTR(XTR): Elliptic curve singular trace representation. Rump Session of Crypto 2000, California, USA, http://www.cs. ucsd.edu/users/mihir/crypto2k/rump-subs.html. 2002-09-20.
[15] Stam M, Lenstra A K. Speeding up XTR, available from www.ecstr.com/2002-10-20.
[16] Han D, *et al.*. A practical approach defeating blackmailing. ACISP'02, Melbourne, Australia, LNCS 2384, Springer-Verlag, 2002: 464–481.
[17] Kugler D, Vogt H. Marking: A privacy protecting approach against blackmailing. PKC'01, LNCS 1992, Cheju Island, Korea, Springer-Verlag, 2001: 137–152.

陈晓峰：　男，1976 年生，博士生，感兴趣的研究方向为椭圆曲线密码与电子商务.
王继林：　男，1965 年生，博士生，副教授，研究方向为签字技术与电子商务.
王育民：　男，1936 年生，教授，IEEE 高级会员，博士生导师，长期从事信息论、信道编码、密码学和通信网的安全等研究.