第 22 卷 第 4 期
2007 年 12 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol.22 No. 4
Dec. 2007

基于广义 XTR 的 ElGamal 公钥体制和 Schnorr 签名方案

廖 嘉[1]，王立鹏[2]，刘寅立[1]
（1. 天津科技大学理学院，天津 300457；2. 河北工业大学计算机科学与软件学院，天津 300130）

摘 要：XTR 体制是一种基于有限域乘法群子群中元素迹紧制表示的公钥体制. 本文中提出了基于广义 XTR 的 ElGamal 体制，并根据 XTR 的特点和 Schnorr 签名构造出一种 XTR 签名.在同等安全条件下，使得加密和签名可以更有效，在计算量、存储量和通讯量上均大幅度降低，且比较容易应用到微机中.

关键词：迹；广义 XTR 公钥体制；ElGamal 体制；Schnorr 签名方案
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1672-6510（2007）04-0068-03

ElGamal Cryptosystem and Schnorr Signature Scheme Based on Extended XTR

LIAO Jia[1], WANG Li-peng[2], LIU Yin-li[1]
（1. College of Science, Tianjin University of Science & Technology, Tianjin 300457, China;
2. School of Computer Science and Engineering, Hebei University of Technology, Tianjin 300130, China）

Abstract: XTR is a public key system based on a method to represent subgroup's elements of a multiplicative group of a finite field. In this paper, we present ElGamal cryptosystem based on Extended XTR. And XTR signature scheme is given based on the characters of XTR and schnorr signature. Extended XTR can be easily used in personal computers. Under the same security, applying XTR is more efficient in the encrytion and signature, and can decrease the quantity of computations, memories, and communications.

Keywords: trace; Extended XTR public key cryptosystem; ElGamaml cryptosystem; Schnorr signature scheme

XTR（Efficient Compact Subgroup Trace Representation），即有效的紧制子群的迹表示. Lenstra 等提出了 XTR 公钥体制[1]，并给出了一些 XTR 公钥体制和签名方案. XTR 用 $GF(p^2)$ 中的运算来达到 $GF(p^6)$ 中安全性，而不用具体构造 $GF(p^6)$. XTR 和 ECC、RSA 相比在参数选择上更加容易，在计算量、存储量和通讯量上大幅度地减少. 文献［2］和文献［3］给出了 XTR 的一些改进算法，使其计算更快速. XTR公钥体制将是非常具有竞争力的公钥体制，将受到大家广泛的欢迎.

在文献[4]中首次提出了用有限域的扩展域和子群相结合的方法，使相互交换的 bit 数减少，但是文献[4]中提出的方法在计算方面不是有效的，而 XTR 却也把计算方面的问题解决了，XTR 用 $GF(p^2)$ 中元素的迹表示 $GF(p^6)$ 中阶为 p^2-p+1 子群中的元素，使数据量减少，但是安全性能并没有降低，并且在计算方面使用最优正规基使计算加快.

S.Lim 把 XTR 推广到 $GF(p^{6m})$ 上，用 $GF(p^{2m})$ 中元素的迹表示 $GF(p^{6m})$ 中阶为 p^2-p+1 子群中的元素，称之为广义 XTR 体制（Extended XTR）[1]，它所使用的计算数据可以用 word 单位来处理，从而可以用普通的计算机来快速实现，避免大数运算在普通计算机难以实现的问题，为 XTR 的广泛应用提供了必要的条件.

1 广义 XTR 体制

有关 XTR 的一些结果[1,4] 如下：

1.1 参数的选择

令 $p=2 \bmod 3$ 是一个素数，$g \in GF(p^{6m})^*$，g 的阶

收稿日期：2007-05-16
基金项目：天津科技大学自然科学基金资助项目（20060227）
作者简介：廖 嘉（1978—），女，天津人，讲师，硕士.

为 q，其中 $m\in N$ 并且满足要么 $2m+1$ 是一个 Fermat 素数，要么 $m,2m+1$ 都是素数，且 $q\mid p^{2m}-p^m+1$.

定义 1：对任意的 $x\in GF(p^{6m})$，称 $Tr(x)=x+x^{p^{2m}}+x^{p^{4m}}$ 为在 $GF(p^{2m})$ 上 x 的迹.

根据迹的定义，易知 $Tr(x)\in GF(p^{2m})$. 在给定 $Tr(g)$，由 g 生成的 q 阶子群称为 Extended XTR 群. 设 $c=Tr(g)$，在 $GF(p^{2m})$ 上三次多项式：

$$F(c,X)=X^3-cX^2+c^{p^m}X-1=(X-h_0)(X-h_1)(X-h_2)$$

其中：$c\in GF(p^{2m})$，$h_i\in GF(p^{6m})$，$i=0,1,2$，并且记 $c_n=h_0^n+h_1^n+h_2^n\in Z$. 由文献[1]中的引理 2.2.1 知 $c_n=Tr(g^n)$，再由文献[1]中的引理 2.3.4 和文献[5]可知 $c_{u+v}=c_u*c_v-c_v^{p^m}*c_{u-v}+c_{u-2v}$.

1.2 XTR 的安全性是基于离散对数问题的难解性

设 $<\gamma>$ 是在 $GF(p^t)$ 中的一个阶为 ω 的乘法群. DL 问题：设 $a=\gamma^x\in<\gamma>$，$0\leqslant x\leqslant\omega$，并且假设 ω 是素数. 根据现有的攻击离散对数的方法，离散对数问题的安全性取决于两个方面：$<\gamma>$ 的最小包含子域的大小；素数 ω 的大小. 如果 $GF(p^t)$ 本身就是 $<\gamma>$ 的最小包含子域并且 ω 足够大，可认为在 $<\gamma>$ 中的离散对数问题就和 $GF(p^t)$ 的一样复杂. XTR 的参数选择就是基于这个思想，使得 XTR 群的最小包含域恰好是 $GF(p^6)$，并且使得 p 不是很小，q 要足够大，那么从上面讨论中可以得出基于 XTR 群的离散对数问题的难度不低于在 $GF(p^6)$ 上的难度，但在计算量上和传输量上用 XTR 可以减小. 从文献[1]中 Theorem5.2.1 可知，基于 XTR 群的离散对数问题和基于 $<\gamma>$ 群的离散对数问题是等价的.

2 基于广义 XTR 的 ElGamal 公钥体制 XTR-ElGamal

设 Alice 选择出 XTR 公钥 $p,q,m,Tr(g)$，Alice 秘密随机选择 $k\in Z$，计算 $S_r(Tr(g))$ 并公开 $Tr(g^r)$. 假定 Alice 的 XTR 公钥为 $p,q,m,Tr(g),Tr(g^r)$.

2.1 加密过程

Bob 用 Alice 的公钥对明文消息 $M\in GF(p^{2m})$ 进行加密，步骤如下：

第一步：Bob 随机选择 $k\in Z$，$1<k<q-2$，用文献[1]中 Algorithm2.3.7 计算

$$S_k(Tr(g^r))=(Tr(g^{(k-1)r}),Tr(g^{kr}),Tr(g^{(k+1)r}))\in GF(p^{2m})^3$$

记 $y_1=Tr(g^{kr})$，并计算 $t_1=Tr(g^{3kr})$，若 $t_1=3$，则重新选择 k；

第二步：Bob 用 Algorithm 2.3.7 基于 $Tr(g^{kr})$ 计算 $t_2=Tr(g^{-kr}),t_3=Tr(g^{2kr})$；

第三步：Bob 计算

$$\beta=(t_2-t_3)\ (3-t_1)^{-1}\bmod GF\quad(p^{2m})$$；

第四步：Bob 用 Algorithm 2.3.7 计算 $S_k(Tr(g))=(Tr(g^{(k-1)}),Tr(g^k),Tr(g^{(k+1)}))\in GF(p^{2m})^3$，记 $\gamma=Tr(g^k)$；

第五步：Bob 计算密文 $E=M\cdot\beta(\bmod p^{2m})$，并把 (E,γ) 传给 Alice.

2.2 解密过程

当 Alice 收到 (E,γ)，解密步骤如下：

第一步：Alice 用 Algorithm 2.3.7 基于 γ 计算 $S_k(Tr(g^r))=(Tr(g^{(k-1)r}),Tr(g^{kr}),Tr(g^{(k+1)r}))\in GF(p^{2m})^3$;

第二步：Alice 解密 $M=E\cdot Tr(g^{kr})(\bmod p^{2m})$.解密正确性证明，根据文献[1]中的引理 2.3.4.i 可知

$$3=c_0=c_{n-n}=c_n*c_{-n}-c_n*c_{2n}+c_{3n},$$

$$c_n*(c_{-n}-c_{2n})(3-c_{3n})^{-1}=1,$$

$$Tr(g^{kr})(Tr(g^{-kr})-Tr(g^{2kr}))(3-Tr(g^{3kr}))^{-1}=1,$$

密文：

$$E=M\cdot(Tr(g^{-kr})-Tr(g^{2kr}))(3-Tr(g^{3kr}))^{-1}$$

明文：

$$M=E\cdot Tr(g^{kr})=M\cdot(Tr(g^{-kr})-Tr(g^{2kr}))(3-Tr(g^{3kr}))^{-1}Tr(g^{kr})=M$$

从而可知解密是正确的.

在 Bob 传输给 Alice (E,γ) 的消息中含有密文 E，它的长度依赖于明文 M 的长度. 而 γ 的长度和 M 的长度无关，γ 的长度和基于有限域的乘法群子群的离散对数的 ElGamal 体制相对应的数据比大约是 1∶3. 由于基于 XTR 群的离散对数问题和基于 $<\gamma>$ 群的离散对数问题是等价的，所以破解这个系统的难度不低于破解 $GF(p^{6m})$ 乘法群中离散对数系统难度. $\beta=(t_2-t_3)(3-t_1)^{-1}$，其中 $t_i,i=1,2,3$ 都是 $Tr(g^{kr})$ 的函数，因为 $Tr(g^{kr})$ 对攻击者来说是不可求的，也就是说 β 对攻击者来说是不可求的，所以 β 是安全的. 那么就可以认为这个系统是安全的.

3 XTR 签名

根据公钥系统的特点，总可以构造出相应的签名方案. 本文根据 XTR 的特点和 Schnorr 签名构造出一种 XTR 签名.

3.1 签名

3.1.1 初始化过程

选择 XTR 公钥 $p,q,m,Tr(g)$，Alice 选择私钥 k，

计算 $Tr(g^k)$，并将它公开，作为公钥. $H(\cdot)$ 为安全的 HASH 函数，m 为需要签名的消息.

3.1.2　Alice 的签名过程

第一步：Alice 随机秘密地选择 $u \in Z$，使 $1 < u < q-2$，并计算 $Tr(g^u), Tr(g^{k-u}), Tr(g^{k-2u})$；

第二步：Alice 计算 $t = Tr(g^{ku})$；

第三步：Alice 计算 $h = H(m)$；

第四步：Alice 计算

$$a = h - kt \bmod q,$$

$$b = h + ut \bmod q;$$

第五步：Alice 计算 $E = Tr(g^{k+u})$.将 $(m, E, a, b, Tr(g^u), Tr(g^{k-u}), Tr(g^{k-2u}))$ 作为消息 m 的签名.

3.1.3　Bob 验证过程

第一步：Bob 验证 a, b 是否在 $[0, q)$ 之间，如果不在，则验证失败；

第二步：Bob 验证 $E, Tr(g^u), Tr(g^{k-u}), Tr(g^{k-2u})$ 是否属于 $GF(p^{2m})$，如果不属于，则验证失败；

第三步：Bob 根据 $(Tr(g^k), Tr(g^u), Tr(g^{k-u}), Tr(g^{k-2u}), b, a)$，计算 $Tr(g^{bk+au})$ [2]；

第四步：Bob 计算 $h = H(m)$；

第五步：Bob 根据 E 计算 $Tr(g^{h(k+u)})$；

第六步：如果 $Tr(g^{h(k+u)}) = Tr(g^{bk+au})$，则签名正确.

这个签名体制的正确性可以由下面等式证明：

$$Tr(g^{bk+au}) = Tr(g^{(h+ut)k+(h-kt)u}) = Tr(g^{hk+hu}) = Tr(g^{h(k+u)})$$

3.2　安全性分析

在给定 $Tr(g^u), Tr(g^k)$ (其中 k, u 是未知的)时，计算 $t = Tr(g^{ku})$ 是不可能的，所以 t 是安全的.而 $(Tr(g^u), Tr(g^{k-u}), Tr(g^{k-2u}))$ 的公开是为了计算 $Tr(g^{bk+au})$，但是攻击者不能从 $(Tr(g^u), Tr(g^{k-u}), Tr(g^{k-2u}))$ 得到任何 k, u 的消息. 根据 a 和 b 可以得到 tk，但是 t, k 均是未知的，所以不能从 a 得到 t, k 任何之一. 同理，从 b 中也不能得到 t, u 任何之一. 所以签名是安全的.

4　结　论

在本文中提出了基于广义 XTR 的 ElGamal 体制和 Schnorr 签名方案. XTR 体制是一种基于有限域乘法群子群中元素迹紧制表示的公钥体制. 与 RSA 和 ECC 相比，在同等安全条件，应用 XTR 可以更有效，并且在计算量、存储量和通讯量上均大幅度降低，而广义 XTR 使用的数据单位是 word，比较容易应用到微机中，避免了大数运算在普通计算机上难以实现的问题.

参　考　文　献：

［1］ Lenstra A K, Verheul E R. Key improvements to XTR[C]// Advances in Cryptology Asiacrypt 2000. LNCS 1880, Springer-Verlag, 2000：1—19.

［2］ Martijin S, Lenstra A K. Speeding Up XTR[C]// Proceedings of Asiacrypt 2001, LNCS 2248. Springer-Verlag, 2001：125—143.

［3］ Lenstra A K, Verheul E R. Key improvements to XTR [C]// Proceedings of Asiacrypt, LNCS 1976, Springer-Verlag 2000：220—233.

［4］ Brouwer A E, Pellikaan R, Verheul E R. Doing more with fewer bits[C]// Proceedings Asiacrypt, LNCS 1716, Springer-Verlag, 1999：321—332.

［5］ Seongan Lim, Seungjoo Kim, Ikkwon Yie, at al. XTR Extended to $GF(p^{6m})$ [C]// SAC 2001, LNCS 2259, Springer-Verlag, 2001：301—312.