1997 IEEE Symposium on Security & Privacy - Sarvar Patel
Number Theoretic Attacks On Secure Password Schemes

总结：本文从数论角度对1992(EKE)及1993(confounder)中的协议及其变体进行分析，进行了吃含猜测攻击，并提供了一定的防范方法，最后作者提到了攻击可行的原因。

前言(EKE、攻击者分类及数论知识)

▲ EKE如何对抗离线字典攻击？
保证对吃的猜测无法通过网络中交互的信息验证，如加密随机公钥。

▲ 攻击者分类(根据能力划分)
① querying attacker (qa)：只能伪装成A，与B发起会话，根据响应发现吃 default
② eavesdropping attacker (ea)：窃听攻击。
③ active attacker (aa)：允许拦截、插入和删除消息

▲ 数论相关知识
a. 定理1：p为素数，且d|(p-1)，当 $a^{\frac{p-1}{d}} \equiv 1 \bmod p$ 时，$x^d \equiv a \bmod p$ 有解，a为d次剩余，反之则无 ⇒ 模p的d次剩余个数为：$\frac{p-1}{d}$
b. 定理2：p,q为素数，均有因子d，当且仅当 $a^{\frac{p-1}{d}} \equiv 1 \bmod p$ 且 $a^{\frac{q-1}{d}} \equiv 1 \bmod q$ 成立时，$x^d \equiv a \bmod n$ 有d次剩余 ⇒ 模n的d次剩余个数：$(\frac{p-1}{d})(\frac{q-1}{d})$

RSA版本EKE

1. A⇒B：A, n, P(e),　　验证猜测的吃需要穷举公钥和会话密钥的空间(困难)
2. B→A：$P(R^e \bmod n)$
…

▲ 可能的攻击
a. 划分攻击(信息泄露导致攻击)。
① 公钥e一定为奇数，ea窃听会话猜测P'解密P(e)，可根据结果的奇偶性来筛选P'，一般通过随机给e+1来解决
② 将最大大小为n的数字拟合到 2^m 的分组中，解密大于n的可拒绝，一般使两者差距尽可能小来避免。
③ n一般由大素数组成，若解密产生了小的素因子则可排除P'

b. 数论攻击(qa伪装成Alice，中的X代表P(e)，qa生成的随机值)
1. qa→B：A, n, X　　B得到X：$e = P^{-1}(X)$，生成随机R.
2. B→qa：$P(R^e \bmod n)$　　若e有小因子3，即 $e=3k$.

攻击者可尝试猜测P'，验证解了的结果是否有模n的立方剩余，根据定理2，想验证 $(Re)'$ 是否为模n的立方剩余，要验证它是p,q的立方剩余，要求 3|(p-1)，3|(q-1)，可根据如下式子来验证：

$(R^e)' \equiv (R^{3k})^{\frac{p-1}{3}} \bmod p \equiv R^{k(p-1)} \bmod p \xrightarrow{\text{费马小定理}} 1$

若e没有3作为小因子，则可选不同X得到e，执行上述过程，若对e，则最后的候选空间为空，否则会剩余1个正确的吃含总能产生立方剩余，找到一个e平均要3次。根据推论2，$\varphi(n)$ 个数中 $\frac{1}{3}\varphi(n)$ 产生立方剩余，若吃空间100万，平均6次会话才能得到P (6×3=18次)。

▲ 尝试的解决方案
a. 合法用户不响应有小因子的e。攻击者可根据是否有响应来得知是否有小因子，比如响应3，解密出现了小因子则可排除。
b. 合法用户用假数X响应有小因子的e，但合法用户不使用有小因子的e。ea可以窃听合法会话拿到P(e)，若P'解密出有小因子，可排除。
c. 合法用户产生e：一个随机X累加至找到无小因子作为e，发送X给B，对方使用同样方法找到e。与上述数论攻击相反，无小因子(如3)，则不产生立方余数则保留，反之剔除。　对RSA-EKE的攻击是有效的。

Diffie-Hellman版本的EKE(DH-EKE)

1. A→B：A, g, p, $P(g^{R_A} \bmod p)$.　　g^{R_A}, g^{R_B} 尽可能随机，
2. B→A：$P(g^{R_B} \bmod p)$, $k(C_B)$,

▲ 针对DH-EKE的数论攻击(qa伪装成Alice，X代表 $P(g^{R_A} \bmod p)$.
1. qa→B：A, g, p, X
2. B→qa：$P(g^{R_B} \bmod p)$ 足够随机.

g,p的选择可能带来问题：1中，qa发送 g^d, p, d为小素数，且d|(p-1)
B计算 $a=(g^d)^{R_B} \bmod p = g^{R_B d} \bmod p$，为模p的d次剩余，即有 $a^{\frac{p-1}{d}} \equiv 1 \pmod p$，(另：$g^{R_B \cdot d \frac{p-1}{d}} \pmod p = g^{R_B(p-1)} \bmod p \equiv 1 \bmod p$
qa可猜测吃解 $P(g^{R_B \cdot d} \bmod p) \Rightarrow g^{R_B d \frac{p-1}{d}}$，若 $\bmod p \equiv 1$，则保留，否则去除猜测P'(每次有$\frac{1}{d}$可得到1)

→ 对策：g必须为p的生成元，检查对于p-1的所有因子k，是否都有 $g^{\frac{p-1}{k}} \not\equiv 1 \bmod p$，满足则是生成元

▲ 半加密攻击(类型攻击，挑战有类型，0：A为发送者；1：B为发送者)
a. 第1条不加密：A, g, p, $g^{R_A} \bmod p$.　(qa伪装成A选择 R_A)
B收到生成 R_B，求出k，并给A发送信息。攻击者猜测P'可得 $g^{R_B} \bmod p$ 进而k'，若C_B有冗余信息(类型)，可根据解密类型为0或1筛选.
b. 第2条不加密：$g^{R_B} \bmod p$，aa拦截，伪装成B
aa自行选 R_B，猜P'解1⇒$(g^{R_A})'$⇒k'，但aa无法生成合法挑战，返回X
A接收则 $X \Rightarrow C_B, 1$，拒绝 $X \Rightarrow C_B, 0$. 但A可能都回应，比如接受了回应 $k^{-1}(X)$，否则为随机数，可知：若回应 $k^{-1}(X)$ 作为 C_B，则攻击者猜P' ⇒k' 看两个挑战 C_B 是否匹配，找到匹配已成找到了吃。若为随机数，则所有都不匹配，比如A发送 $(C_B', 0)$ 而非 $(C_B', 1)$，可筛选部分吃。
(一般可通过使用复杂类型来构造挑战，如64bit，攻击者将很难构造使 $k^{-1}(X) \Rightarrow (C_B', 111\cdots1111)$) 除非处理好类型，否则不用半加密

ElGamal版本EKE

1. A→B：A, q, p, $P(g^{R_A} \bmod p)$
2. B→A：$P(g^k \bmod p, R g^{R_A - k} \bmod p)$.

▲ 数论攻击，qa伪装成A，发送X　　$P^{-1}(X)$
同DH-EKE，qa收到响应 $P(g^{kd} \bmod p, R^{\frac{1}{k}} \bmod p)$
故手猜P' ⇒ $g^{kd \frac{p-1}{d}} \overset{?}{\equiv} 1 \pmod p$，可排除吃.

▲ 半加密攻击(EKE解释了第2条不可不加密)。
第一条，qa伪装成A，日日文发 $g^{R_A} \pmod p$，B响应后，qa可猜测P'⇒R'
qa向B发X，若B接受可解密出 $C_A', 0$，否则为 $C_A', 1$。只有复杂类型才能抵抗

GLNS(RSA)，使用随机数confounder充当一次一密的手段，其中对于协议不安全

a. Direct Authentication Protocol.　　初始A,B在无服务器情况下建立会话密钥
1. A→B：A, r_A, k_{able}, n.　　qa伪装为A，以X替换 $k_{ab}(e)$，且知n=pq
2. B→A：$(B, A, \cdots)^e \bmod n$.　　B解密得e，qa猜P'⇒e' 已知$\varphi(n)$⇒d'
代入1得B', A'，若恰好为B, A，则猜测正确 $((B,A)^{ed'} \bmod n \Rightarrow B'A')$

b. Secret Public key Protocol　(S给A,B分别发公钥，k_a, k_b为与S共享密钥)
1. A→S：A, B
2. S→A：A, B, $k_a(e_a)$, n_a, $k_b(e_b)$, n_b　　aa伪装成S，发送A,B,X_a,n_a,X_b,n_b
3. A→B：$(A,B,\cdots)^{e_a} \bmod n_a$, $k_b(e_b)$, n_b　　A解密X_a得e_a，aa猜测P'⇒e_a'
aa可根据e_a'⇒d_a'，代入3得A'B'验证

攻击可行的原因：非EKE版本的协议的要求被违背了，如对于生成元的要求。验证公钥系统假设是保证安全的必要条件