Shared generation of authenticators and signatures*

(Extended Abstract)

Yvo Desmedt
EE & CS Department
University of Wisconsin-Milwaukee
Milwaukee, WI 53201
desmedt@cs.uwm.edu

Yair Frankel
EE & CS Department
University of Wisconsin-Milwaukee
Milwaukee, WI 53201
yair@cs.uwm.edu

Abstract

Often it is desired that the power to sign or authenticate messages is shared. This paper presents methods to collectively generate RSA signatures, provably secure authenticators and unconditionally secure authenticators. In the new schemes, l individuals are given shares such that $k \leq l$ are needed to generate a signature (authenticator) but less than k can not. When the k people have finished signing (authenticating), nobody can perform an impersonation or substitution attack. These schemes are called threshold signature (authentication) schemes. Clearly these schemes are better than each of the k individuals sending a separate authenticator for each message or if each of the k individuals each send their share to a *"trusted"* person who will sign for them.

In all of the schemes we assume that the shareholders (senders) and receiver have secure workstations but the network and servers are not necessarily secure.

1 Introduction

The idea of combining cryptosystems with secret sharing (threshold) schemes [Bl, Sh] has been introduced in several papers recently [CH, DQV, DF90]. Shared generation of authenticators using Diffie-Hellman [DH] was presented in [CH], but it is completely insecure against substitution. Threshold decryption of private messages was introduced in [DF90]. Shared verification of authenticators was introduced in [DQV], but the available message space is small. *An important problem not discussed in these papers is the shared generation of secure signatures.* Issuing checks for a corporation is a vivid example of this well-known problem. For security reasons, it may be a company's policy that checks be signed by k individuals rather than one person. An organization may choose l individuals and allow any subset consisting of $k \leq l$ people to sign its checks. This is similar to the concept of threshold schemes [Bl, Sh]. This paper presents *threshold* (a) *RSA* signatures, (b) *provably secure* authenticators and (c) *unconditionally secure* authenticators. Using mental games [GMW], this can be achieved conditionally but the scheme is highly interactive and very impractical.

*Research is being supported by NSF Grant NCR-9106327

J. Feigenbaum (Ed.): Advances in Cryptology - CRYPTO '91, LNCS 576, pp. 457-469, 1992.

Our paper presents techniques where k out of l individuals are required to generate a signature (or authenticator) for a message. This is clearly better than having each of the k individuals create k signatures (authenticators) which would cause an increase in bandwidth overhead. The receiver would also be required to perform more calculations and store a larger key directory. *No interaction between shareholders* is necessary for the generation of signature (authenticator) and the secret key is not revealed to any individual even after signatures (or authenticators) have been created with our schemes. We assume that the shareholders (senders) and receiver have secure workstations but the network and servers are not necessarily secure. A byproduct of this research is a homomorphic group based threshold scheme (see Section 4.2).

Our threshold RSA signature scheme is based on interpolation polynomials over the integers (see Section 3). Even though there exists no threshold scheme over any infinite ring [BS] (see also [CK]), our scheme is secure. A threshold signature scheme based on algebraic integers is also discussed.

RSA signatures [RSA] are weak and not proven secure [Da, Den, dJC, Mo]. Therefore, we present a proven secure solution for threshold authenticators (see Section 4) based on a new *homomorphic threshold scheme over a finite Abelian group* in which inverses can be calculated in polynomial time. These Abelian groups must have an exponent[†] with large prime factors[‡]; the exponent needs to only be known to the distribution center that makes the shares[‡].

A threshold unconditionally secure authentication scheme is presented (see Section 5). It is based on finite geometry.

2 The model and notation

Let (S, R) be a signature or an (interactive or non-interactive) authentication scheme, where S is the sender and R is the receiver. Instead of S, we have a set $\mathcal{A}$ ($|\mathcal{A}| = l$) such that any subset $\mathcal{B}$, where $|\mathcal{B}| = k$, can replace S as the signature (authenticator) generator. Each time S would send a bit string in (S, R) then all individuals in $\mathcal{B}$, in our $(\mathcal{A}, R)$ signature scheme, will send a *partial result* to some (not necessarily trusted) Combiner C. Then C combines the partial results and sends a bit string similar as S would. Observe that no interaction is required between the shareholders and C to create the bit string (see Figure 1). It must be impossible for C to impersonate when C is

[†]For a group G, the exponent is the smallest integer e such that $\forall x \in G, x^e = 1$.

[‡]Our homomorphic threshold scheme over a finite Abelian group can be adapted to any exponent and there is no need for the key distributor to know the exponent [DF91].

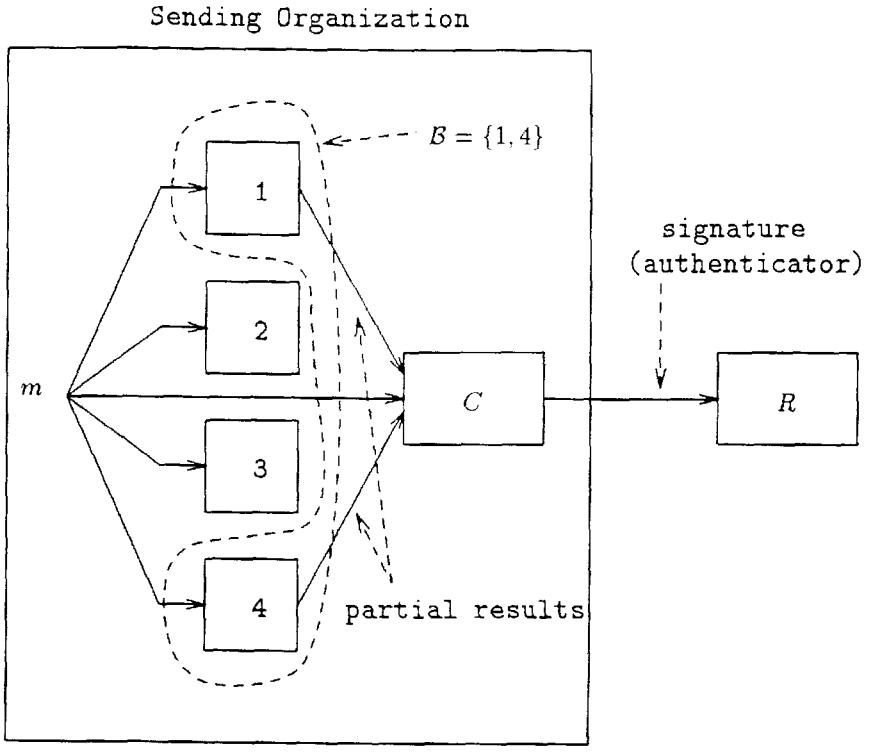

Figure 1: An example of a two out of four threshold signature (authentication) scheme.

collaborating with any $k-1$ shareholders and for C to substitute a message when C receives additionally k partial results (for the same message). We assume that neither C nor the shareholders will jam the signature generation.

3 Threshold RSA signatures

Let $n = pq$ where p, q are safe primes. One condition for p to be a safe prime is that $p = 2p' + 1$ where p' is a prime [BB78, BB79], similarly $q = 2q' + 1$. Normally RSA is defined with the ϕ function, however it could just as well have been defined with the λ function[§]. Due to the method we chose n note that $\lambda(n) = 2p'q'$. The secret key is d which was chosen at random such that $\gcd(d, \lambda(n)) = 1$. So d is odd. An RSA signature of a message m is $S_m \equiv m^d \bmod n$. In our method, each individual $i \in \mathcal{B}$ will generate a modified share $a_{i,\mathcal{B}}$ such that $\sum_{i \in \mathcal{B}} a_{i,\mathcal{B}} \equiv d - 1 \bmod \lambda(n)$. Each $i \in \mathcal{B}$ will calculate

[§] λ is the Carmichael function, i.e., the exponent of $Z_n^*(\cdot)$.

the partial result $s_{m,i,\mathcal{B}} \equiv m^{a_{i,\mathcal{B}}} \bmod n$ and send it to C. To create the signature, C calculates $S_m \equiv m \cdot \prod_{i \in \mathcal{B}} s_{m,i,\mathcal{B}} \bmod n$.

3.1 Polynomial approach

As in the Lagrange interpolation scheme of [Sh], let $f(x)$ be a polynomial of degree $k-1$ such that $f(0)$ is the secret. However, parts of our calculations will be performed over the integers rather than over a field and $f(0) \equiv d - 1 \bmod \lambda(n)$. We now discuss a method to calculate $a_{i,\mathcal{B}}$ which circumvents the problem of calculating inverses [DF90] even when $\lambda(n)$ must remain secret to the shareholders. To simplify our discussion[¶], we assume that $\lambda(n) = 2p'q'$, where p' and q' are large primes. This implies that not all $x_i - x_j$ have inverses modulo $2p'q'$ (*e.g.*, when $x_i - x_j$ is even, it has no inverse). Let all the x_i be odd and all $f(x_i)$ be even and let $f(0) = d - 1$ (d is odd in RSA). Thus, a share distribution center will choose p, q and d, and will send to each i the share

$$K_i' = \frac{f(x_i)/2}{\left(\prod_{\substack{j \in \mathcal{A} \\ j \neq i}} (x_i - x_j)\right)/2} \pmod{p'q'}.$$

Observe now that *no inverses have to be calculated by the shareholder* because

$$f(x) = \sum_{i \in \mathcal{B}} K_i' \prod_{\substack{j \notin \mathcal{B} \\ j \in \mathcal{A}}} (x_i - x_j) \prod_{\substack{j \in \mathcal{B} \\ j \neq i}} (x - x_j) \pmod{2p'q'}.$$

The correctness of the previous two equations is proven in Theorem 3.1. Let $q_{i,\mathcal{B}} = \prod_{\substack{j \notin \mathcal{B} \\ j \in \mathcal{A}}} (x_i - x_j) \prod_{\substack{j \in \mathcal{B} \\ j \neq i}} (0 - x_j)$, then the modified share, $a_{i,\mathcal{B}}$, is an integer where

$$a_{i,\mathcal{B}} = K_i' \cdot q_{i,\mathcal{B}}.$$

Due to exponentiation, the threshold scheme is actually performed in $Z_{\lambda(n)}$, thus this is not conflicting with [BS]. The above scheme seems to be secure. Some modifications are needed to prove that the scheme is as secure as RSA (see final paper).

Theorem 3.1 *When $n = pq$ for p, q safe primes and $|\mathcal{A}| \geq 2$, the above scheme creates an RSA signature.*

Proof: **(Sketch)** Even though $\lambda(n)$ is not known by the shareholders, the exponentiation operation is performed modulo $\lambda(n)$. Using the Chinese remainder theorem the

[¶]In general, it is sufficient to assume that $\lambda(n)/2$ is the product of large primes.

above computation is correct modulo 2 (since it is always even) and modulo $p'q'$ (since the inverses exist). Thus the scheme generates the correct signature. ∎

3.2 The use of extensions of rings

Since in the above method $q_{i,\mathcal{B}}$ becomes a very large integer when l is large, we discuss a different method using algebraic extensions (see [Ja85]) over $Z_{\lambda(n)}$. Let u be a root to the irreducible polynomial $p(x) = x^h + a_{h-1}x^{h-1} + \cdots + a_1 x + a_0$ over $Z_{\lambda(n)}$. We remind the reader that an algebra A over a commutative ring R is a pair of A, a ring and an R-module A where the additive group for the ring and the R-module are the same and $\alpha(ab) = (\alpha a)b = a(\alpha b)$ for $a, b \in A$ and $\alpha \in R$ (see [Ja89, p. 43]). We can now view $Z_{\lambda(n)}[u]$ as an algebra over $Z_{\lambda(n)}$. The regular representation of an algebra A is the map $x \rightarrow x_L$ for each $x \in A$ where x_L is the map $a \rightarrow xa$ in A. This is a homomorphism from A to $\mathrm{End}_R A$[‖]. A matrix representation $\rho(x)$ for x_L can be made for each $x \in A$. When the inverse of x exits, we define $\overline{x} = x^{-1} \cdot N(x)$ where $\mathrm{N}(x) = \det(\rho(x))$ is the norm of x (see also [Ja85, pp. 422-425]). Note that $\rho(x)$ is invertible iff x is invertible. This framework provides us with an alternative method to the polynomial approach.

Now $f(x)$ is a polynomial over $Z_{\lambda(n)}[u]$ with $f(0) = d-1$. Let the x_i's be chosen such that $\forall i, j \in \mathcal{A} : x_i, x_j \in Z_{\lambda(n)}[u]$ and $\mathrm{N}(x_i - x_j) < C_p(l)$ where $C_p(l)$ is a small integer independent of x_i and $\gcd(\mathrm{N}(x_i - x_j), \lambda(n)) = 1$. We now let

$$q'_{i,\mathcal{B}} = \prod_{\substack{j \in \mathcal{A} \\ j \notin \mathcal{B}}} \mathrm{N}(x_i - x_j) \prod_{\substack{j \in \mathcal{B} \\ j \neq i}} (\overline{x_i - x_j}) \prod_{\substack{j \in \mathcal{B} \\ j \neq i}} (0 - x_j)$$

and $K''_i = f(x_i) / \prod_{\substack{j \neq i \\ j \in \mathcal{A}}} \mathrm{N}(x_i - x_j)$. Note that $a_{i,\mathcal{B}} = K''_i \cdot q'_{i,\mathcal{B}}$. We define functions $\mathrm{F}_i : R[u] \rightarrow R$ such that $\mathrm{F}_i(b_0 + \cdots + b_h u^h) = b_i$. Since $d - 1 \in Z_{\lambda(n)}$, we see that $\sum_{i \in \mathcal{B}} \mathrm{F}_0(a_{i,\mathcal{B}}) = \sum_{i \in \mathcal{B}} a_{i,\mathcal{B}} \equiv d - 1 \bmod Z_{\lambda(n)}$. So each $i \in \mathcal{B}$ will calculate $s_{m,i,\mathcal{B}} \equiv m^{F_0(a_{i,\mathcal{B}})} \bmod n$ and send $s_{m,i,\mathcal{B}}$ to the Combiner as mentioned earlier in Section 3.

Modification of the extension ring method can enhance our threshold scheme over some Abelian groups (see Section 4.2) as done in [DF91].

We now analyze the order of the number of multiplications needed in the modified RSA by one shareholder. For that purpose we analyze the largest coefficient in absolute value of $q'_{i,\mathcal{B}}$. Let $|a|$ denote the absolute value of the integer a and let $p(x) = x^h + a_{h-1}x^{h-1} + \cdots + a_0$ be an irreducible polynomial mod $\lambda(n)$ with u a root and $a_i < \lambda(n)$. Let, $c(u) = b(u) \cdot b'(u) = (b_{h-1} \cdot u^{h-1} + \cdots + b_0) \cdot (b'_{h-1}u^{h-1} + \cdots + b'_0) = \sum_{j=0}^{2h-2} c_j u^j$ then

[‖] $\mathrm{End}_R A$ is the ring of homomorphisms going from the R-module A into itself.

$c_j = \sum_{i=0}^{j} b_i \cdot b'_{j-i}$. We see that when $|b_i| \leq B$ and $|b'_i| \leq B'$, then $|c_j| \leq hBB'$. Now let $c'(u) \equiv c(u) \pmod{\lambda(n), p(u)}$. Since $\lambda(n)$ is unknown to $k-1$ shareholders, each of them cannot do the above reduction. So we define $c''(u) \equiv c(u) \bmod p(u)$ without reducing it modulo $\lambda(n)$ and we use the relation $u^h = -a_{h-1}u^{h-1} - \cdots - a_0$ for c_j with $j > (h-1)$. Thus by calculating the absolute value of the largest coefficient in $c''(u)$, we find that it is less than $hBB'\lambda(n)^{(h-1)}$. When the largest coefficient of $y_i(u)$ are in absolute value less than A, then by induction the absolute value of the largest coefficient in $y_1(u) \cdot y_2(u) \cdots y_T(u)$ is at most $h^{T-1}A^T\lambda(n)^{(T-1)(h-1)}$. We now will use this formula to calculate the largest coefficient in absolute value of $\prod_{j\in\mathcal{B}, j\neq i} x_j$ and of $\prod_{j\in\mathcal{B}, j\neq i}(\overline{x_i - x_j})$.

It is easy to see that the largest coefficient in absolute value of $\prod_{j\in\mathcal{B}, j\neq i} x_j$ is less than: $h^{k-2}\lambda(n)^{(k-2)h+1}$. The calculation of $(\overline{x_i - x_j})$ cannot be made in a straight forward manner since $\lambda(n)$ is not known to the shareholders. It is clear that using the extended Euclidean algorithm over the rationals, that $(\overline{x_i - x_j})$ and $\mathrm{N}(x_i - x_j)$ can be computed**. We note that the absolute value of the quotients computed in the Euclidean algorithm are bounded [Kn] by $\alpha = \lambda(n)^{2h-1}(h+1)^h$. We also note that the extended Euclidean algorithm terminates in $\log(h)$ steps. So using the *extended* Euclidean algorithm the largest coefficient in absolute value of $(\overline{x_i - x_j})$ is less than $\beta = \log(h)h^{\log(h)-1}\alpha^{\log(h)}$. So the largest coefficient in absolute value of $\prod_{j\in\mathcal{B}, j\neq i}(\overline{x_i - x_j})$ is less than: $h^{k-2}\beta^{k-1}\lambda(n)^{(k-2)(h-1)}$.

Now $N(x_i - x_j) \leq C_p(l)$, so $|\prod_{j\in\mathcal{A}, j\notin\mathcal{B}} \mathrm{N}(x_i - x_j)| \leq C_p(l)^{l-k}$. Let $L_{i,\mathcal{B}}$ be the largest coefficient in $q'_{i,\mathcal{B}}$. Then $\log(L'_{i,\mathcal{B}}) \in O(kh\log(h)\log(\lambda(n)) + (l-k)\log C_p(l))$, because h must be much smaller than $\lambda(n)$. We now recall from the first method that $q_{i,\mathcal{B}} = (\prod_{j\notin\mathcal{B}, j\in\mathcal{A}}(x_i - x_j))(-1^{T-1})\prod_{j\in\mathcal{B}, j\neq i} x_i$. Observe that the x_i in $q_{i,\mathcal{B}}$ are integers. Let $D_{i,\mathcal{B}}$ be the absolute value of $q_{i,\mathcal{B}}$. In fact $x_i < 2i$, so $D_{i,\mathcal{B}} < (2l)^{l-k} \cdot (k-1)!2^{k-1}$. So using Stirling's approximation $\log(D_{i,\mathcal{B}}) \in O((l-k)\log(l) + (k-1)\log(k-1))$. So depending from l, k, h, $C_p(l)$, and $\log(\lambda(n))$ one should choose one of the methods. Evidently we can see that the extension ring method can be improved when one optimizes the norms $(C_p(l))$ and h. It seems as though this optimization problem is difficult.

A third method to obtain threshold RSA signatures, which can be used, is based on matrices where the determinant is small. This is similar to the method used in [DF90]. Each of the methods of the threshold RSA signatures performs differently depending on k, l, h, $C_p(l)$, and $\log(\lambda(n))$.

**In some cases this method does not find the actual conjugate and the actual norm. As long as all shareholders and the key distributor use the same method it does not matter in our context.

4 A provably secure threshold authentication scheme

4.1 Attempt at a group based homomorphic threshold scheme

We first want to develop a homomorphic threshold scheme [Be] for an Abelian group G whose exponent has only large prime factors. Let e'_G be a multiple of the exponent of G such that e'_G is of similar form as e_G. Let $\{g_1, g_2, \cdots, g_m\}$ generate G and e'_G and g_j be known to the key distribution center. Define secret $s = g_1^{\gamma_1} g_2^{\gamma_2} \cdots g_m^{\gamma_m}$. For $0 < j \leq m$, let $f_j(x)$ be independently chosen polynomials of degree $k-1$ such that $f_j(0) = \gamma_j$. Similar to the method of Section 3.1, the key distribution center calculates

$$K'_{j,i} = \frac{f_j(x_i)}{\left(\prod_{\substack{t \neq i \\ t \in \mathcal{A}}} (x_i - x_t) \right)} \in Z_{e'_G}, \ \forall i \in \mathcal{A} \text{ and } \forall j \in \{1, \cdots, m\}.$$

In this scheme, however, the share for i is $A_i = g_1^{K'_{1,i}} g_2^{K'_{2,i}} \cdots g_m^{K'_{m,i}} \in G$ and the modified share for i in $\mathcal{B}$ is $a_{i,\mathcal{B}} = (A_i)^{q_{i,\mathcal{B}}}$ where $q_{i,\mathcal{B}}$ is defined as in Section 3.1. Thus $s = \prod_{i \in \mathcal{B}} a_{i,\mathcal{B}}$. This scheme is not practical since the key distribution center must solve the discrete log problem and additionally know the generators and e'_G. A similar remark in the context of multiplicative sharing schemes was made in [Be]. For many groups, the discrete logarithm is considered hard [Od, MVO].

4.2 Homomorphic threshold scheme over an Abelian group

Since the first attempt is not practical for most purposes, we propose a variation which *requires only that e'_G is known to the key distributor and has only large prime factors.* Let $\{A_1, A_2, \cdots, A_{k-1}\}$ be independently randomly chosen elements in G. Then by letting $\mathcal{X}_j = \{1, 2, \cdots, k-1, j\}$ with $j \geq k$, the key distribution center can calculate

$$A_j = (s \cdot \prod_{\substack{i \neq j \\ i \in \mathcal{X}_j}} A_i^{-q_{i,\mathcal{X}_j}})^{q_{j,\mathcal{X}_j}^{-1}}.$$

The use of A_j is as in Section 4.1. Observe that any combination of $k-1$ shareholders do not learn anything new about e_G, the exponent of G, when given the fact that e_G has only large prime factors. The following concept goes further. The concept of a sharing scheme not revealing anything about the secret *or anything else* is called a zero-knowledge sharing scheme [DF91]. We remind the reader that knowing the exponent of Z_n^* allows one to factor n. Using extensions, similar to Section 3.2, we have proposed

a zero-knowledge homomorphic threshold scheme for *any* l and k no matter what the exponent e_G is [DF91].

4.3 The provable scheme

A provable secure *authentication* scheme based on a zero-knowledge version of [GMR] was presented in [Des]. Its advantage is that no authentication tree is needed.

Let $R \in D_n$ where $D_n = \{x \in Z_n \mid (x \mid n) = 1 \text{ and } 0 < x < n/2\} = G$ and $n = p \cdot q$ where p and q safe primes such that: $p \equiv 3 \bmod 8$ and $q \equiv 7 \bmod 8$. The tuple (R, n) is our public key. First observe that $D_n(*)$ is an Abelian group in which the operation is defined as:

$$x * y = \begin{cases} xy \,(\mathrm{mod} n) & \text{if } xy \,(\mathrm{mod} n) < n/2, \\ -xy \,(\mathrm{mod} n) & \text{if } xy \,(\mathrm{mod} n) \geq n/2, \end{cases}$$

where $x, y \in D_n$. In D_n we will use this multiplication from now on. The function $f_0(x) = x*x$ in D_n and $f_1(x) = 4*x*x$ in D_n. When $\langle M \rangle$ is the prefix-free encoding [Ga] of M then $\langle M \rangle$ is never a prefix of $\langle M' \rangle$ $(M \neq M')$. Now, $f_{\langle M \rangle}$ is defined as $f_{\langle M \rangle}(x) = f_{i_d}(f_{i_{d-1}}(\cdots f_{i_1}(f_{i_0}(x)) \cdots))$, where $\langle M \rangle = i_d i_{d-1} \ldots i_1 i_0$ in binary. One has to read $f^{-1}_{\langle M \rangle}$ as $(f_{\langle M \rangle})^{-1}$ so that $f^{-1}_{\langle M \rangle}(f_{\langle M \rangle}(x)) = x$. We define $|\langle M \rangle| = d + 1$. When a limit on the length of the prefix free encoding of the message, called α, is known beforehand, [Des] works when one knows $\sqrt[2^\alpha]{R}$ and $\sqrt[2^\alpha]{4}$ (see also [Go]). We recall that if n is as in Section 3.1, then the exponent of D_n is $p'q'$, satisfying our conditions. In our scheme the key distributor gives shares of $\sqrt[2^\alpha]{R}$ and $\sqrt[2^\alpha]{4}$ using our group based threshold scheme. In a homomorphic threshold scheme when A_j is a share for s and A'_j is a share for s', $A_j \cdot A'_j$ is a share for $s \cdot s'$. When $|\langle M \rangle| \leq \alpha$, each shareholder can calculate, using his shares, his part of $f^{-1}_M(R_j)$, which we call $S_{i,M}$.

To authenticate a message the following protocol is executed. First C sends the message M to the receiver, called the verifier V. Then repeat $|n|$ times:

Step 1 The shareholder $i \in \mathcal{B}$ randomly chooses a $t_i \in D_n$ and squares it $|\langle M \rangle|$ times to obtain $X_i = t_i^{(2^{|\langle M \rangle|})} \pmod n$ and sends X_i to C. Then C calculates $X = \prod_i X_i \pmod n$ and sends X to V.

Step 2 V sends a random bit E to C, who broadcasts it.

Step 3 Each shareholder calculates $Y_i = t_i \cdot (S_{i,M})^E \pmod n$ and sends it to C. Then C calculates $Y = \prod_i Y_i \pmod n$ and sends it to V.

Step 4 V verifies Y by using multiplications, and the organization's public key.

Our method does not leak the factors of n to a collusion of $k-1$ shareholders. It is not difficult to prove that if k is polynomial in $|n|$ that the view that C has is easy to simulate, so that it not necessary to trust C. So the shareholders could have secure workstations using an insecure local network to communicate with C (who communicates with the verifier).

Observe that the distributor in the above does not need to be one trusted individual. Mental games [GMW] allow for this.

5 An unconditionally secure version

We now develop a method for the threshold unconditionally secure authenticators using a geometric scheme. The method will be performed in Z_p^{k+1}, a $(k+1)$-dimensional vector space over a large prime p. We denote one of the axis in Z_p^{k+1} as $\mathcal{M}$ and points as $p=(x_1,x_2,\cdots,x_k,n)\in Z_p^{k+1}$ where n is the $\mathcal{M}$ coordinate. Let P_m, called the message plane for m, contain all points satisfying the equation $n=m$. A secret line l_s known to the receiver, R, and not parallel to P_0 is generated by the key distribution center D (see Figure 2); D may be R. The secret shares generated by D are k-dimensional

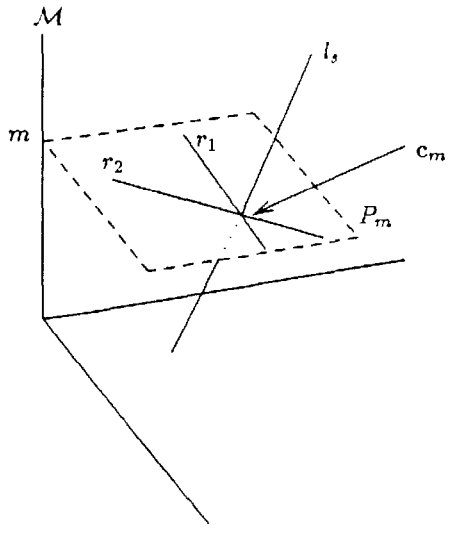

Figure 2: The geometric scheme for a 2 out of l authenticator generator. C calculates the codeword given two planes $R_{i,m}$, which intersect P_m at r_i.

planes A_i such that the intersection of any k planes, A_i, is l_s. The receiver accepts as an authenticated m, a point $c_m = (x_1, x_2, \cdots, x_k, m) \in l_s$, called the codeword.

To generate the codeword, each individual $i \in \mathcal{B}$ will send to C a k-dimensional random plane $R_{i,m}$ which contains the intersection of A_i and P_m. C can now generate the codeword c_m given the k planes $R_{i,m}$ and the plane P_m. Since the planes are random, C will gain no information about l_s other than the point $p_m \in l_s$ and therefore C cannot perform a substitution attack even if $k-1$ individuals would help additionally. A projective geometry method is easily derived from the above method. In [DF], a method based on polynomials to achieve the above is given.

6 Conclusion

Often it is desired that the power to sign or authenticate messages is shared. Key sharing schemes on their own are not suited for this because once used the key is revealed. Our heuristic (RSA), proven secure and unconditionally secure schemes solve this problem. In our scheme the shareholders do not have to interact with one another, while in mental games they do heavily. In all of our schemes we assume that the shareholders (senders) and receiver have secure workstations but the network and servers are not necessarily secure. It is an open problem to determine which systems in general can be executed in a non-interactive distributive way.

7 Acknowledgements

The authors would like to thank Josh Benaloh, Bob Blakley, Burt Kaliski and Gus Simmons for discussions and expressing their interest in this work.

References

[BB78] B. Blakley and G. R. Blakley. Security of number theoretic public key cryptosystems against random attack. *Cryptologia*, 1978. In three parts: Part I: 2(4), pp. 305–321, October 1978; Part II: 3(1), pp. 29–42, January 1979; Part III: 3(2), pp. 105–118, April 1979.

[BB79] G. R. Blakley and I. Borosh. Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages. *Computers & Mathematics with Apllications*, 5(3):169–178, 1979.

[Be] J. C. Benaloh. Secret sharing homomorphisms: Keeping shares of a secret secret. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pages 251–260. Springer–Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15.

[Bl] G. R. Blakley. Safeguarding cryptographic keys. In *Proc. Nat. Computer Conf. AFIPS Conf. Proc.*, pages 313–317, 1979. vol.48.

[BS] G. R. Blakley and L. Swanson. Infinite structures in information theory. In D. Chaum, R.L. Rivest, and A. T. Sherman, editors, *Advances in Cryptology. Proc. of Crypto'82*, pages 39–50. Plenum Press N. Y., 1983. Crypto '82, Santa Barbara, CA, August 1982.

[CH] R. A. Croft and S. P. Harris. Public-key cryptography and re-usable shared secrets. In H. Beker and F. Piper, editors, *Cryptography and coding*, pages 189–201. Clarendon Press, 1989. Royal Agricultural College, Cirencester, December 15–17, 1986.

[CK] B. Chor and E. Kushilevitz. Secret sharing over infinite domains. In G. Brassard, editor, *Advances in Cryptology — Crypto '89, Proceedings (Lecture Notes in Computer Science 435)*, pages 299–306. Springer-Verlag, 1990. Santa Barbara, California, U.S.A., August 20–24.

[Da] G. I. Davida. Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem. Tech. Report TR-CS-82-2, University of Wisconsin-Milwaukee, October 1982.

[Den] D. E. R. Denning. Digital signatures with RSA and other public-key cryptosystems. *Comm. ACM 27*, pages 388–392, 1984.

[Des] Y. Desmedt. Abuse-free cryptosystems: Particularly subliminal-free authentication and signature. Submitted to the Journal of Cryptology, under revision, April 1989.

[DF] Y. Desmedt and Y. Frankel. Unconditionally secure threshold authentication. In preparation (Available from authors when completed).

[DF90] Y. Desmedt and Y. Frankel. Threshold cryptosystems. Santa Barbara, California, U.S.A., August 20–24, 1990.

[DF91] Y. Desmedt and Y. Frankel. Perfect zero-knowledge sharing schemes over any finite Abelian group. Presented at Sequences '91, June 17–22, 1991, Positano, Italy, to appear in: the Proceedings Springer-Verlag, 1991.

[DH] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT–22(6):644–654, November 1976.

[dJC] W. de Jonge and D. Chaum. Attacks on some RSA signatures. In *Advances in Cryptology: Crypto '85, Proceedings (Lecture Notes in Computer Science 218)*, pages 18–27. Springer-Verlag, New York, 1986. Santa Barbara, California, U.S.A., August 18–22, 1985.

[DQV] M. De Soete, J.-J. Quisquater, and K. Vedder. A signature with shared verification scheme. In G. Brassard, editor, *Advances in Cryptology — Crypto '89, Proceedings (Lecture Notes in Computer Science 435)*, pages 253–262. Springer-Verlag, 1990. Santa Barbara, California, U.S.A., August 20–24.

[Ga] R. G. Gallager. *Information theory and reliable communication.* John Wiley and Sons, New York, 1968.

[GMR] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *Siam J. Comput.*, 17(2):281–308, April 1988.

[GMW] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the Nineteenth ACM Symp. Theory of Computing, STOC*, pages 218 – 229, May 25–27, 1987.

[Go] O. Goldreich. Two remarks concerning the Goldwasser-Micali-Rivest signature scheme. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pages 104–110. Springer-Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15, 1986.

[Ja85] N. Jacobson. *Basic Algebra I*, volume 1. W. H. Freeman and Company, 2nd edition, 1985.

[Ja89] N. Jacobson. *Basic Algebra II*, volume 2. W. H. Freeman and Company, 2nd edition, 1989.

[Kn] D. E. Knuth. *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms.* Addison-Wesley, Reading, MA, 1981.

[Mo] J. H. Moore. Protocol failures in cryptosystems. *Proc. IEEE*, 76(5):594–602, May 1988.

[MVO] A. Menezes, S. Vanstone, and T. Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the Twenty third annual ACM Symp. Theory of Computing, STOC*, pages 80–89, 1991.

[Od] A. M. Odlyzko. Discrete logs in a finite field and their cryptographic significance. In N. Cot T. Beth and I. Ingemarsson, editors, *Advances in Cryptology, Proc. of Eurocrypt'84 (Lecture Notes in Computer Science 209)*, pages 224–314. Springer–Verlag, 1984. Paris, France April 1984.

[RSA] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Commun. ACM*, 21:294–299, April 1978.

[Sh] A. Shamir. How to share a secret. *Commun. ACM*, 22:612 – 613, November 1979.