Fair Public-Key Cryptosystems

by

Silvio Micali

Laboratory for Computer Science
Massachusetts Institute of Technology
545 Technology Square, Cambridge, MA 02139

(Rough Draft)

Abstract. We show how to construct public-key cryptosystems that are *fair*, that is, strike a good balance, in a democratic country, between the needs of the Government and those of the Citizens. Fair public-key cryptosystems guarantee that: (1) the system cannot be misused by criminal organizations and (2) the Citizens mantain exactly the same rights to privacy they currently have under the law.

We actually show how to transform any public-key cryptosystem into a fair one. The transformed systems preserve the security and efficiency of the original ones. Thus one can still use whatever system he believes to be more secure, and enjoy the additional properties of fairness. Moreover, for today's best known cryptosystems, we show that the transformation to fair ones is particularly efficient and convenient.

As we shall explain, our solution compares favorably with the Clipper Chip, the encryption proposal more recently put forward by the Clinton Administration for solving similar problems.

Note For The Reader. Since privacy and law enforcement interest most of society, and since we would welcome an informed debate before making crucial policy decisions in this area, we have made a sincere attempt to reach a broad audience. We thus hope that at least the goals and the properties of our approach will be understandable by the Government official and the Citizen who do not have any familiarity with cryptography. Further, the basic technical ideas of our solution --which are quite simple to begin with--are presented at a very intuitive level, so as to be enjoyable for the reader generally familiar with the field of cryptography, though not necessarily an expert in secure protocol design. Such an expert will not have great difficulty in filling in the formalization and the occasionally subtle technical details that have been omitted in this draft. (We actually hope to have given her sufficient indications to make her journey through this draft as short as possible.)

We apologize for not having the time to write different versions of this paper for different audiences.

1. Introduction

A wrong debate

Currently, Court-authorized line tapping is an effective method for securing criminals to justice. More importantly, in our opinion, it also prevents the further spread of crime by deterring the use of ordinary communication networks for unlawful purposes. Thus, there is a legitimate concern that wide-spread use of public-key cryptography may be a big boost for criminal and terrorist organizations. Indeed, many bills propose that a proper governmental agency, under the circumstances allowed by the law, be able to obtain the clear text of any communication over a public network. At the present time, this requirement would translate into coercing citizens into either (1) *using weak cryptosystems* --i.e., cryptosystems that the proper authorities (but also everybody else!) could crack with a moderate effort-- or (2) *surrendering, a priori, their secret key* to the authority. It is not surprising that such alternatives have legitimately alarmed many concerned citizens, generating the feeling that privacy should come before national security and law enforcement.

It is our opinion that this debate is wrong. It is wrong because it is a "one-bit debate," that is, it envisages either unconstrained privacy or no privacy at all. Extreme positions are more likely to be unjust and, indeed, having to choose only between the above alternatives is quite uncomfortable. Fortunately, we are not bound to choose only among what is currently available. It is indeed the goal of Science to understand reality and to change it to our advantage, so as to enlarge our options.

Broadening the debate

In this paper we show how cryptographic protocols can be successfully and efficiently used to build cryptosystems that are fairer, that is, that strike a better balance, in a democratic country, between the needs of society and those of the individual. More precisely, we show a *simple* and *general* methodology for transforming any public-key cryptosystem into a *fair* one, that is, one enjoying the following properties:

1 *(Unabusing)* The privacy of the law-obeying user *cannot* be compromised, while

2 *(Unabusable)* Unlawful users *will not* enjoy any privacy.

Our transformation preserves the original security of the underlying cryptosystem and its efficiency. Since we believe that public-key cryptosystems are best suited for adoption in a large nation, in this paper we solely focus on making fair this type of cryptosystems.

2. Public-Key Cryptosystems

A conventional cryptosystem allows two users X and Y, who have previously agreed on a common secret key (e.g., by meeting in a secure physical location) to exchange private messages over a public network. The usefulness of such systems is quite limited. While there is plenty of need for private communication, agreeing on a common secret key without the help of a modern communication network is quite cumbersome. In the case of the military it may not be too inconvenient, since in this application it may be clearer beforehand with whom one will need to exchange private messages. But in other cases, as in business applications, it is very hard to know a priori with whom one will need to talk in private and thus establish a common secret key in advance. The type of cryptosystem best suited for these latter settings is a *public-key cryptosystem* (PKC for short) as introduced by Diffie and Hellman in [DiHe]. While in a conventional cryptosystem each secret key was used both for encrypting and decrypting, in a PKC the encryption and decryption processes are governed by pairs of *matching* keys, which are generated together so to satisfy the following three properties: letting (E,D) be one such pair of matching encryption/decryption keys, 1 Any message can be encrypted using E.

2 Knowledge of D enables one to read any message encrypted with E; on the contrary, ignoring D it is practically impossible to understand messages encrypted with E.

3 Knowing E does not enable one to compute its corresponding decryption key D.

PKCs thus dismiss the need for agreeing beforehand on a common secret key, by using instead a bit of initial interaction. Assume that a user X generates a pair of matching encryption/decryption keys (E_X,D_X), and that a user Y wants for the first time to send him a private message and tells him so. Then X sends E_X to Y over the phone; Y easily encrypts her message to X with E_X because of Property 1; X easily decrypts it because of Property 2; and, because of Properties 2 and 3, no one else can understand the message so exchanged. Interaction (like in the case of electronic mail) is not however always available, and PKCs are thus most useful by having stipulating what *de facto* is a "*social agreement*" between users and a *key-management center*. Each user X comes up with a pair of matching encryption and decryption keys (E_X,D_X). After generating a (E_X,D_X) pair, the user keeps D_X for himself and gives E_X to the key-management center. The center is responsible (and is trusted!) for *updating* and *publicizing* a directory of *correct* encryption keys, one for each user --i.e., a list of entries of the type (X,E_X) which, for example, may be publicized in a "phone-book format" or via a "411-like service." If, as in the latter example, this distribution occurs over a public network, a digital authentication that E_X comes from the center must be provided, for instance by using one of the existing digital signature schemes. Clearly the users must trust the center, as an untrustworthy center may enable a user Y to read the messages intended for user X by falsely claiming that E_Y is X's encryption key. Thus, in ultimate analysis, the security of a PKC depends on the key-management center. Since setting up such a center on a grand scale requires a great deal of effort by society, the precise protocols the center must follow (and thus its properties) must be properly chosen.

Every advantage has a drawback, and public-key cryptography is no exception. Here a main disadvantage is that any such system can be abused; for example, by terrorists and criminal organizations who can now conduct their illegal business with great secrecy and yet with extreme convenience. Very often scientists have jumped into new technical ventures without giving much thought to the consequences of their actions. Developing nuclear plants without solving first their associated nuclear waste problems is a notable example of the social blindness of Science in this century. Certainly, all of us envisage good uses for public-key cryptography, but the risk exists that the main fruits of this development may be harvested by criminal organizations, and it is thus our responsibility to give a more thorough thought to the matter. *Fair Public-Key Cryptosystems* (Fair PKCs for short) are our proposal to enjoy public-key cryptography while protecting society from the problems arising from its blind utilization. We hope that our proposal will start a fruitful scientific debate, and other scientific solutions will be sought to this important problem in order to avoid further plaguing a crime-ridden world.

3. Fair PKCs

3.1 The Informal Notion of a Fair PKC

Let *S* be a public-key cryptosystem. Informally speaking, we say that

S is a Fair PKC if it guarantees a special agreed-upon party --and solely this party!-- under the proper circumstances envisaged by the law --and solely under these *circumstances!-- to understand all messages encrypted using S, even without the users' consent and/or knowledge.*

That is, the philosophy behind a Fair PKC is *improving* the security of the existing communication systems while *keeping the legal procedures* already holding and accepted by the society. The following proposition immediately follows from the above definition.

Proposition: Let C be a ciphertext exchanged by two users in a Fair PKC S. Then, under the proper circumstances envisaged by the law, the proper third party will either

1) find the *cleartext* of C relative to S (whenever C was obtained by encrypting a message according to S) or

2) obtain a (court-presentable) *proof* that the two users were not using S for their secret communication.

Of course, if using any other type of public-key cryptosystem were to be made *illegal*, Fair PKCs would be most effective in guaranteing both private communication to law-obeying citizens and law enforcement. (In fact, if a criminal uses a phone utilizing a Fair PKC to plan a crime, he can still be secured to justice by court-authorized line tapping. If he, instead, illegally uses another cryptosystem, the content of his conversations will never be revealed even after a court authorization for tapping his lines, but, at least, he will be convicted for something else: his use of an unlawful cryptosystem.) Nonetheless, as we shall discuss in section 4, Fair PKCs are quite useful even without such a law.

3.2 An Abstract Way for Constructing Fair PKCs

We shall now present, in a very *abstract* way, our prefered method for constructing Fair PKCs. We shall see in section 5 that this very abstract and almost paradoxical method can not only be concretly implemented, but actually be implemented in a most efficient way.

Below, for concreteness of presentation, we shall use the *Government* for the special agreed-upon party, a *court order* for the circumstances contemplated by the law for monitoring a user's messages, and the *telephone system* for the underlying method of communication. We also assume the existence of a key-distribution center as in an ordinary PKC.

In a Fair PKC there are a fixed number of predesignated *trustees* and an arbitrary number of users. The trustees may be federal judges (as well as different entities, such as the Government, Congress, the Judiciary, a civil rights group, etc.) or computers controlled by them and especially set up for this purpose. Even if efforts have been made to choose *trustworthy* trustees, a Fair PKC does not blindly rely on their being honest. The trustees, together with the individual users and the key-distribution center, play a crucial role in deciding which encryption keys will be publicized in the system. Here is how.

For concreteness of exposition, assume that there are 5 trustees. Each user independently chooses his own public and private keys according to a given double-key system. Since the user himself has chosen both keys, he can be sure of their "quality" and of the privacy of his decryption key. He then breaks his private decryption key into five *special* "pieces" (computing from his decryption key 5 special strings/numbers) possessing the following properties:

1) The private key can be reconstructed given knowledge of all five special pieces;

2) The private key cannot be reconstructed if one only knows (any) 4, or less, of special pieces;

3) For *i=1,...,5,* the *i*-th special piece can be *individually* verified to be *correct.*

Comment. *Of course, given all 5 special pieces, one can verify that they are correct by checking that they indeed yield the private decryption key. The difficulty and power of property 3 consists of the fact that each special piece can be verified to be correct (i.e., that together with the other 4 special pieces yields the private key) individually; that is, without knowing the secret key at all, and without knowing the value of any of the other special pieces! (How these special pieces can be generated is explained in the full paper. Below we will show how they can be used.)*

The user then privately (e.g., in encrypted form) gives trustee *i* his own public key and the *i*-th piece of its associated private key. Each trustee individually inspects his received piece, and, if it is correct, *approves* the public key (e.g., signs it) and safely *stores* the piece relative to it. These approvals are given to the key-management center, either directly by the trustees, or (possibly in a single message) by the individual user who collects them from the trustees. The center, which may or may not coincide with the Government, itself approves (e.g., it itself signs) any public key which *is approved by all trustees.* These center-approved keys are the public keys of the Fair PKC and they are distributed and used for private communication as in an ordinary PKC.

Since the special pieces of each decryption key are privately given to the trustees, an adversary who taps a user's communication line possesses the same information as in the underlying, ordinary PKC. Thus if this is secure, so is the Fair PKC. Moreover, even if the adversary were one of the trustees himself, or even a cooperating collection of any 4 out of five of the trustees, due to property 2, he would still have the same information as in the underlying ordinary PKC. Since the possibility that an adversary corrupts 5 out of 5 federal judges is absolutely remote, the security of the resulting Fair PKC is the same as in the underlying, ordinary one.

When presented with a court order, and only in this case, the trustees will reveal to the Government the pieces of a given decryption key in their possession. This enables the Government to reconstruct the given key. Recall that, by property 3, each trustee has already verified that he was given a correct piece of the decryption key in question. Thus, the Government is *guaranteed* that, *in case of a court order*, it will be given all correct pieces of any given decryption key. By property 1, it follows that the Government will be able to reconstruct any given decryption key if necessary.

4. Basic Questions About Fair PKCs

Before addresing the real technical question of how Fair PKCs can be concretly constructed, let us consider some legitimate and broader questions.

Q: *Are Fair PKCs less secure?*

A: No. Unless an adversary corrupts 5 out of 5 trustees --a rather unlikely event-- they provably provide just the same security as the underlying, ordinary PKC. (Only the Government, and in case of a court order, may have the cooperation of all 5 trustees.)

Q: *Are Fair PKCs less efficient?*

A: No. Communication is exactly as efficient as in an ordinary PKC. The only differences are (1) when a public-key is registered, and (2) when a private key is, in a lawful manner, retrieved by the Government. Each user validates his public key only once. Thus only once does he need to give pieces of his private key to the trustees. Moreover, as we have seen in section 4, this step can be implemented by sending 5 short messages, one to each trustee. Second, the lawful reconstruction of a private key by the Government is essentially instantaneous once the five special pieces are obtained from the trustees. Collecting these five pieces electronically is no more cumbersome than issuing or checking a court order as it is needed in a lawful procedure. (As we have seen in section 4, private-key reconstruction may just consist of receiving 5 short messages and one addition.)

Q: *In a totalitarian system, what confidence can we have in a Fair PKC?*

A: Most probably, in a totalitarian system the trustees will be selected with rather different criteria. It is thus conceivable that all of them (whether individuals or organizations) may routinely conspire so as to reconstruct all private keys, destroying all confidence in the privacy of a Fair PKC. On the other hand, believing that ordinary PKCs may be the way to guarantee individual privacy during a dictatorship is quite *naive*. Outlawing any form of PKC will be among the first measures taken by any dictator. Indeed, public use of cryptography is a gift of democracy (and it is important that this gift cannot be turned against it). In fact, Fair PKCs are close in spirit to Democracy itself, in that power is not trusted to any chosen individual (read "trustee") but to a multiplicity of delegated individuals.

Q: *Aren't Fair PKCs the same as ordinary PKCs in which users are obliged to give the Government the private key corresponding to every public key?*

A: No. This deprives the individual of his right to privacy *a priori* and without any just cause. Someone who has not committed (nor is suspected to have committed) a crime should not be required to surrender his right to private communication to anybody, not even to the Government. And this is exactly what he would be obliged to do by revealing his own private key at the time of registering his public one with the key-management authority.

People consent that their right to privacy may be taken away under special circumstances, but do not agree to lose it in an automatic manner. Fair PKCs guarantee the users that they will keep exactly the same rights they currently have in a phone network, and with greater security. (In fact, due to technological advances or collusions with phone operators, eavesdropping ordinary phone conversations will become easier and easier for unauthorized parties.)

Q: *What is the difference between a Fair PKC and a PKC with a "hidden trapdoor" chosen by the Government?*

A: There are three main differences:

1) A PKC with a hidden trapdoor is very dangerous: if an enemy finds it, the security of the entire system is compromised.

By contrast, in a Fair PKC, each user chooses his key independently. Thus even if a single user's key is compromised, this does not affect other users at all.

2) Society may never consent to using a PKC with a hidden trapdoor, since this is equivalent to asking the citizen to surrender their right to privacy even before being suspected of any wrong doing! (On the other hand, should a government maliciously ask its citizens to use a special type of PKC concealing the presence of a master secret key, things may get quite unpleasant if the existence of such a key is later discovered!)

3) PKCs with a hidden trapdoor may be weaker than ordinary PKCs, since in the former case the public and private keys must be chosen in a constrained way. In fact, enforcing the existence of a single master secret key for all public keys in the system is a very severe constraint in choosing the individual users' keys. Indeed, it is easy to speak of a system with a single master key, but it is also quite conceivable that any such cryptosystem may be easy to break.

By contrast, a Fair PKC, unless all trustees unlawfully collaborate, offers *the same* security of the underlying PKC. Even if 4 out of 5 trustees are traitors, the time that an adversary should invest for understanding anything about a message encrypted in a Fair PKC *provably equals* the time he needs to invest when the same message has been encrypted in the underlying ordinary PKC.

Q: *Granted that Fair Cryptosystems protect Society and the individual. But what is their advantage if criminals do not use them for their communications?*

A: We must distingush two settings: First, when the use of any PKC which is not Fair is made illegal. Second, when all commercially available PKCs are Fair (e.g., because thay are the only ones to be standardized), even though non-Fair PKC are not illegal.

Setting 1 has a short answer: a criminal who uses a non-Fair PKC could be brough to justice at least on this charge (recal that Al Capone was convicted for tax evasion).

Let us now consider setting 2. First, note that this is the current setting: anyone in the U.S.A. can use any cryptosystem he or she chooses (though the market for encryption product has not yet reached its full potential). Still, if Society ensures, via standardization, that all *easily available* PKCs are Fair, there are big advantages to be gained.

1) Criminals will have difficulty in distributing their own keys.

In fact, they could not enjoy the convenience of a well-kept and well-publicized public file; that is, they could not call up anyone they want and have a secret conversation with her. They thus would need alternative, cumbersome, and secretive methods to exchange their own keys.

In other words, it is one thing that criminals go out of their way to avoid being controlled by the Government in presenc of a court order, and a *very different thing* that the Government goes out of their way to provide criminals with this capability by setting up an ordinary PKC on a grand scale!

2) Besides difficulty in key distribution, criminals will have no convenient access to "alternative" cryptographic *products* which use their keys.

In fact, most products whose usefulness may be greatly enhanced by public-key cryptography --such as "secure" phones, "secure" faxes, etc.-- could become reasonably available, economic, reliable, and compatible, only if *mass produced;* that is, only after intensive engineering effort and big initial investments. Thus, if essentially only the criminals were to use non-fair cryptography, industry would not have sufficient interest in developing products incorporating such technology. (Else, the "criminal market" should have grown so much that we would have nothing more to worry about: civil society as we know it would have already ceased to exist.) Also, big and reputable companies would refrain anyway from manufacturing "questionable" products. Finally, even if a company were willing to manufacture products utilizing non-Fair PKCs, the list of its customers or any record of its sales would be excellent tips for the Police.

3) In an ordinary PKC, the Government is in a difficult position. Since it cannot understand any conversation at all, it has no way to distinguish even potential criminals from non-criminals (setting aside what criminals are saying). In a Fair PKC, instead, the Government can at least make this distinction. Assume that a Fair PKC is standardized, X is one of its users, and a court order authorizes the Government to listen to all messages addressed to X. If the Government is still unable to understand these calls, it means that X really uses a different cryptosystem, and thus intends not to be understood by the Government even in case of a court order. This may be crucial information, and information not available in an ordinary PKC.

4) If all commercially available cryptographic products (e.g., "secure" phones) were based on Fair-PKCs, there would be several advantages. True: a powerful criminal organization could succeed in having designed and produced phones made secure by a non-Fair PKC. This would, however, be less easy for isolated criminals; moreover, it would be most inconvenient for two or three people to get hold of "alternative" products just to discuss their FIRST crime. *At least,* Fair PKC-based products prevent their initially (but no longer) honest buyers from conveniently and undetectably shift to illegal communications.

5) In any case, punishing *abuse* is secondary with respect to enabling *legitimate use.*

Q: *Fair PKCs may strike a good balance between the needs of the Government and those of the citizens in a democratic country, but: is there any use of Fair PKCs for "less democratic" settings?*

A: Yes. Consider the case of a large organization, say a private company, where there is a need for privacy, there is an established "superior" --say, a president,-- but not all employees can be trusted since there are too many of them. The need for privacy requires the use of encryption. Since not all employees can be trusted, using a single encryption key for the whole company is unthinkable. So is using lots of single-key cryptosystems, since this would generate enormous key-distribution problems. Having each employee use his own double-key system is also dangerous, since he might conspire against the company with great secrecy, impunity, and convenience. Obliging every employee to surrender his decryption key to the president is certainly more possible than in the public sector, since a private company need not to be too democratic an organization. But *it may not be a good idea* for many reasons, two of which are the following. First, the identity of the president may change, and change quite often, but an employee should not change his keys for every new president. Second, a storage device containing all or many of the decryption keys would require to be overwhelmingly guarded.

Even in this context Fair PKCs may be of help. Again, key distribution will not be a problem. Each employee will be in charge of choosing his own keys, which makes the system more distributed and agile. While enjoying the advantages of a more distributed procedure, the company will retain an absolute control, since the president is guaranteed to be able to decrypt every employee's communications when necessary. There is no need to change keys when the president does, since the trustees need not to be changed. The trustees' storage places need less surveillance, since only compromising all of them will give an adversary any advantage.

Finally, Fair PKCs can be used as better secret sharing, since one has the guarantee that the secret will be reconstructed if all pieces (or the majority of them, depending on the implementation) will be made available.

5. A Concrete But Impractical Construction of Fair PKCs

We now show that any ordinary PKC can actually be made fair along the lines of the abstract construction of Section 3. The construction below, though concrete, is however too general for being practical, and thus more direct solutions are described in the next two sections for making fair the most popular, ordinary PKCs. The practically-oriented reader may thus prefere to procede directly to those sections.

5.1 A Sketch For The Expert

The expert in secure protocol theory may be satisfied with the following sketch.
Cuttng corners, each user should (1) come up with a pair of matching public and private keys and give the trustees his chosen public key, (2) encrypt (by a different cryptosystem, even one based on a one-way function) his chosen private key, (3) give the trustees the just computed ciphertext and a zero-knowledge proof that the corresponding "decryption" really consists of the private key corresponding to the given public key, and (4) give the trustees shares of this decryption by means of a proper Verifiable Secret Sharing protocol.

5.2 A More Informative Discussion

In expanding the above sketch for the non-expert in protocol design, we feel important to illustrate both similarities and differences between Fair PKCs and other related prior notions.

SECRET SHARING
As independently put forward by Shamir [Sh] and Blakley [Bl], secret sharing (with parameters n,T,t) is a cryptographic scheme consisting of two phases: in phase 1, a secret value chosen by a distinguished person, the *dealer*, is put in "safe storage" with n people or computers, the *trustees*, by giving each one of them a piece of information, a *share*, of the secret value. In phase 2, when the trustees pool together the information in their possession, the secret is recovered . In a secret sharing, this storage is *safe* only in two senses:

1 *Redundancy*.
Not all trustees need to reveal their shares in phase 2: it is enough that T of them do. (Thus the system tolerates that some of the trustees "die" or accidentally destroy the shares in their possession)

2 *Privacy.*
If less than t of the trustees accidentally or even intentionally divulge the information in their possession to each other or to an outside party, the secret remains unpredictable until phase 2 occurs.

Secret sharing suffers, though, of a main problem: *Assumed honesty*; namely,

> Secret sharing presupposes that the dealer gives the trustees correct "shares" (pieces of information) about his secret value. This is so because each trustee cannot verify that he has received a meaningful share of anything. A dishonest dealer may thus give "junk" shares in phase 1, so that, when in phase 2 the trustees pool together the shares in their possession, there is no secret to be reconstructed.

EXAMPLE (Shamir)
The following is a secret sharing scheme with parameters n=2t+1 and T=t+1.

> Let p be a prime >n, and let S belong to the interval [0,p-1]. Choose a polynomial P(x) of degree t by choosing at random each of its coefficients in [0,p-1], except for the last one which is taken to be equal to S , that is, P(0)=S. Then the n shares are so computed: S1=P(1),...,Sn=P(n). *Redundancy* holds since the polynomial P(x) can be interpolated from its value at any t+1 distinct points. (This, in turn, allows the computation of P(0) and thus of the secret.) *Privacy* holds since P(0) is totally undetermined by the value of P at any t points X1 ... Xt different from 0 (in fact, any value v for P(0), together with the value of P at points X1 ... Xt uniquely determines a polynomial).

As it can be easily seen, if the dealer is dishonest, he may give each trustee a random number mod p. If this is the case, then (a) each trustee cannot tell that he has a junk share, and (b) in phase 2 there will be no secret to reconstruct. The consequence of this is that secret sharing is more useful in those occasions in which the dealer is certainly honest, for instance, because being honest is *in his own interest.* (A user that encrypts his own files with a secret key has a big interest in properly secret sharing his key with, say, a group of colleagues: if he accidentally looses it, he needs to reconstruct it!) Secret sharing alone, instead, cannot be too useful for building Fair Cryptosystems: we cannot expect that a criminal give proper shares of his secret key to some federal judges when the only purpose of his doing this is allowing the authorities, under a court order, to understand his communications!

VERIFIABLE SECRET SHARING
A closer connection exists between Fair PKCs and verifiable secret sharing (VSS) protocols. While the two concepts are not identical, a special type of VSS can be used to build Fair PKCs. As put forward by Awerbuch, Chor, Goldwasser, and Micali [CGMA], a verifiable secret sharing (VSS) scheme is a scheme that, while guaranteeing both the redundancy and the privacy property, overcomes the "honesty problem." In fact, in a VSS scheme each trustee can *verify* that the share given to him is genuine *without knowing at all the shares of other trustees or the secret itself.* That is, he can verify that, if T verified shares are revealed in phase 2, the original secret will be reconstructed, no matter what the dealer or dishonest trustees might do.

EXAMPLE (Goldreich, Micali, and Wigderson [GMW1])

Assume that a PKC is in place and let Ei be the public encryption function of trustee i. Then, as in Shamir's scheme, the dealer selects a random polynomial P of degree t such that P(0)=the secret, and gives each trustee the n-vector of encryptions E1(P(1)) E2(P(2))...En(P(n)). Trustee i will therefore properly decode P(i), but has no idea about the value of the other shares, and, consequently, whether these shares "define" a unique t-degree polynomial passing through them. The dealer thus proves to each trustee that the following sentence is true "*if you were so lucky to guess all decryption keys, you could easily verify that there exists a unique t-degree polynomial interpolating the encrypted shares.*" Since easily verifying something after a lucky guess corresponds to NP, the above is an "NP sentence." Since, further, the whole of NP is in zero-knowledge [GMW1], the dealer proves the correctness of the sentence, in zero knowledge, to every trustee. This guarantees each trustee that he has a legitimate share of the secret, since he has a legitimate share of P, but does not enable him (or him and other t-1 trustees) to guess what the secret is before phase 2.

VSS AND FAIR PKCs

Assume that each user chooses a secret/public key pair, and then VSS shares his secret key with some federal judges. Does this constitute a Fair PKC? Not necessarily. In a VSS scheme, in fact, the secret may be *unstructured*. That is, each trustee can only verify that he got a genuine share of some secret value, but this value can be "anything." For instance, if the dealer promises that his secret value is a prime number, in an unstructured VSS a trustee can verify that he got a genuine share of some number, but has no assurances that this number is prime.

Unstructured VSS is not enough for Fair PKCs. In fact, the trustees should not stop at verifying that they possess a legitimate share of a "generic" secret number: they should verify that the number they have a share of actually is the decryption key of a given public key! The GMW scheme, as described above, is an unstructured VSS, and thus unsuitable for directly building Fair PKCs. The same is true for other VSS schemes (e.g. the ones of Ben-Or, Goldwasser and Wigderson [BeGoWi]; of Chaum, Crepeau and Damgard [ChCrDa]; and of Rabin and Ben-Or [RaBe], just to mention a few).

Some VSS schemes are *structured*, that is each trustee can further verify that the secret value of which he possesses a genuine share satisfies some additional property. What this property is depends on the VSS scheme used. For instance, Feldman proposes a VSS in which, given an RSA modulus N and an RSA ciphertext E(m)= m^e mod N (of some cleartext message m), the trustees can verify that they do possess genuine shares of the decryption of E(m) (i.e., of m). This scheme is attractive in that it is "non-interactive," but *cannot* be used to hand out in a verifiable way shares of the decryption key of a given public key. In fact,

the trustees have no guarantee that the decryption of E(m) actually consists of N's factorization.

In other words, the trustees can verify that they have genuine shares of the decryption (m) of a ciphertext E(m), but m is *unstructured* (with respect to N's factorization and anything else).

CONSTRUCTING FAIR PKCs WITH A GENERIC VSS

Can a generic VSS scheme be transformed so as to yield Fair PKCs? The answer is YES, but at a formidable cost. All of the above mentioned VSS protocols can be "structured" so that the extra property verifiable by the trustees is that the dealer's secret actually is the decryption key of a given public key. In fact, this can be achieved as an instance of *secure function evaluation* between many parties as introduced by Goldreich, Micali, and Wigderson in a second paper [GoMiWib]. Such secure evaluation protocols are possible, though, more in theory than in practice in light of the complexity of the particular functions involved. In the case of the GMW VSS scheme, since the encryption of all the shares is publicly known, the transformation can actually be achieved by a simpler machinery: an additional zero-knowledge proof. But even in this case the computational effort involved is formidable. Essentially, one has to encode the right statement (i.e., the secret, whose proper shares are the decodings of these public ciphertexts, is the decryption key of this given public key) as a VERY BIG graph, 3-colorable if and only if the statement is true, and then prove, in zero-knowledge, that indeed the graph is 3-colorable. Not only are these transformations of a generic VSS to one with the right property computationally expensive, but they require INTERACTION (on top, if any, of the interaction required by the VSS scheme itself)! All these considerations may rule out constructing Fair PKCs this way in practice. Thus CUSTOM-TAILORED methods should be sought, whenever possible, to transform ordinary PKCs to Fair ones. This is our next goal.

6. Making Fair the Diffie-Hellman Scheme

Let us now exhibit concrete and efficient methods for turning two popular PKCs into Fair ones. We start by making Fair the scheme of Diffie and Hellman, since this is the simplest of the two.

Recall that, a bit differently than in other systems, in Diffie-Hellman's scheme each pair of users X and Y succeeds, without any interaction, in agreeing upon a common, secret key S_{xy} to be used as a conventional single-key cryptosystem. Here is how.

The Ordinary Diffie-Hellman PKC

There are a *prime p* and a *generator* (or high-order element) *g* common to all users. User X *secretly* selects a random integer *Sx* in the interval *[1,p-1]* as his private key and publicly announces the integer $Px=g^{Sx}$ *mod p* as his public key. Another user, Y, will similarly select *Sy* as his private key and announce $Py=g^{Sy}$ *mod p* as his public key. The value of this key is determined as $S_{xy}=g^{Sx.Sy}$ mod p. User X computes Sxy by raising Y's public key to his secret key mod p; user Y by raising X's public key to his secret key mod p. In fact

$$(g^{Sx})^{Sy}=g^{Sx.Sy}=Sxy=g^{Sy.Sx}=(g^{Sy})^{Sx}= \ mod\ p.$$

While it is easy, given *g*, *p*, and *x*, to compute $y=g^x$ *mod p*, no efficient algorithm is known for computing, given *y* and *p*, *x* such that $g^x=y$ mod *p* when *g* has high enough order. This is, in fact, the famous *discrete logarithm problem*. This problem has been used as the basis of security in many cryptosystems, and in the recently proposed U.S. standard for digital signatures. We now transform Diffie and Hellman's PKC into a fair one. Again, to keep things as simple as possible we imagine that there are 5 trustees and that ALL of them should cooperate to reconstruct a secret key, that is, that ALL shares are needed to reconstruct a secret key. Relaxing this condition involves another idea and will be dealt with in section 5.

A Fair Diffie-Hellman Scheme
(All-Shares Case)

Instructions for the users
Each user X randomly chooses 5 integers *Sx1,...,Sx5* in the interval *[1,p-1]* and lets *Sx* be their sum *mod p*. From here on, it will be understood that all operations are modulo *p*. He then computes the numbers

$$t1=g^{Sx1},...,t5=g^{Sx5} \text{ and } Px=g^{Sx}.$$

Px will be user X's public key and *Sx* his private key. The *ti*'s will be referred to as the *public pieces* of *Px*, and the *Sxi*'s as its *private pieces*. Notice that the product of the public pieces equals the public key Px. In fact,

$$t1\cdot ... \cdot t5=g^{Sx1}\cdot ... \cdot g^{Sx5}=g^{(Sx1+...+Sx5)}=g^{Sx}.$$

Let T1,...,T5 be the five trustees. User X now gives *Px* and pieces *t1* and *Sx1* to trustee T1, *t2* and *Sx2* to T2, and so on. It is important that piece *Sxi* be privately given to trustee T_i.

Instructions for the trustees
Upon receiving public and private pieces *ti* and *Sxi*, trustee Ti verifies whether $g^{Sxi}=ti$. If so, it stores the pair *(Px,Sxi)*, signs the pair *(Px,ti)*, and gives the signed pair to the key-management center. (Or to user X, who will then give all of the signed public pieces at once to the key-management center.)
Instructions for the key-management center
Upon receiving all the signed public pieces, *t1...t5*, relative to a given public key *Px*, the center verifies that the product of the public pieces indeed equals *Px*. If so, it approves *Px* as a public key, and distributes it as in the original scheme (e.g., signs it and gives it to user X.)

This ends the instructions relative to the keys of the Fair PKC. The encryption and decryption instructions for any pair of users X and Y are exactly as in the Diffie and Hellman scheme (i.e., with common, secret key *Sxy*). It should be noticed that, like the ordinary Diffie-Hellman, the Fair Diffie-Hellman scheme does not require any special hardware and is actually easily to implement in software.

Why does this work?
First, the privacy of communication offered by the system is the same as in the Diffie and Hellman scheme. In fact, the validation of a public key *does not compromise at all* the corresponding private key. Each trustee Ti receives, as a special piece, the discrete logarithm, *Sxi*, of a *random number*, *ti*. This information is clearly irrelevant for computing the discrete logarithm of *Px*! The same is actually true for any 4 of the trustees taken together, since any four special pieces are independent of the private decryption key *Sx*. Also the key-management center does not possess any information relevant to the private key; that is, the discrete logarithm of *Px*. All it has are the public pieces signed by the trustees. (The public pieces simply are 5 random numbers whose product is *Px*. This type of information is irrelevant for computing the discrete logarithm of *Px;* in fact, any one could choose four integers at random and set the fifth to be *Px* divided by the product of the first four[1]. As for a trustee's signature, this just represents the promise that *someone else* has a secret piece. As a matter of fact, even the information in the hands of the center together with any four of the trustees is irrelevant for computing the private key *Sx*.) Thus, not only is the user guaranteed that the validation procedure will not betray his private key, but he also knows that this procedure has been properly followed because he himself has computed his own keys and the pieces of his private one!

Second, if the key-management center validates the public key *Px*, then the corresponding private key is guaranteed to be reconstructible by the Government in case of a court order.

[1] The result would be integral because division is modulo p.

In fact, the center receives all 5 public pieces of *Px*, each signed by the proper trustee. These signatures testify that trustee Ti possesses the discrete logarithm of public piece *ti*. Since the center verifies that the product of the public pieces equals *Px*, it also knows that the sum of the secret pieces in storage with the trustees equals the discrete logarithm of *Px*; that is, user X's private key. Thus the center knows that, if a court order is issued requesting the private key of X, by summing the values received by the trustees, *the Government is guaranteed* to obtain the needed private key.

It should be noticed that, for efficiency considerations, we split the verification of the structure of the secret among trustees and key-management center. In fact a trustee verifying that Sxi is the discrete log of ti cannot possibly verify that Sxi is a share of the secret key of public key Px, since he has never seen Px! (If we wanted we could have defined the public key to consist of Px t1 t2 t3 t4 t5. In this case giving trustee Ti the entire public key and the private piece (share) Sxi, we would have enabled him to verify the structure of the secret as well.)

7. Making Fair the RSA Scheme

Let us now just OUTLINE a custom-tailored method to make the RSA Fair. We will be more precise in the final paper. Our method, while simple algorithmically, does require some more knowledge of number theory. (We wish to note that our effort could be consirerably simplified if we were willing to make Fair not the basic RSA scheme, but some variants of its that essentially exhibit its same security.)

In the basic RSA PKC, the public key consists of an integer N product of two primes and one exponent e (relatively prime with f(N), where f is Euler's totient function). No matter what the exponent, the private key may always be chosen to be N's factorization. Before we show how to make a Fair PKC out of RSA we need to recall some facts from number theory.

Fact 1. Let Z_N^* denote the multiplicative group of the integers between 1 and N which are relatively prime with N. If N is the product of two primes N=pq (or two prime powers: $N=p^ap^b$), then

* a number s in Z_N^* is a square mod N if and only if it has four distinct square-roots mod N: x, -x mod N, y, and -y mod N. (That is, $x^2=y^2=s$ mod N.) Moreover, from the greatest common divisor of +-x+-y and N, one easily computes the factorization of N. Also,

* one in four of the numbers in Z_N^* is a square mod N.

Fact 2. Among the integers in Z_N^* is defined a function easy to evaluate, the Jacobi symbol, that evaluates to either 1 or -1. The Jacobi symbol of x is denoted by (x/N). The Jacobi symbol is multiplicative; that is, (x/N)(y/N)=(xy/N). If N is the product of two primes N=pq (or two prime powers: $N=p^ap^b$), and p and q are congruent to 3 mod 4, then, letting x, -x, y, and -y mod N be the four square roots of a square mod n, (x/N)=(-x/N)=+1 and (y/N)=(-y/N)=-1. Thus, because of fact 1, if one is given a Jacobi symbol 1 root and a Jacobi symbol -1 root of any square, he can easily factor N.

We are now ready to describe how the RSA cryptosystem can be made fair in a simple way. For simplicity we again assume that we have 5 trustees and that *all* of them must collaborate to reconstruct a secret key, while no 4 of them can even predict it.

A Fair RSA Scheme
(All-Shares Case)

Instructions for the user
A user chooses P and Q primes and congruent to 3 mod 4 as his private key, and N=PQ as his public key. Then he chooses 5 Jacobi 1 integers X_1 X_2 X_3 X_4 and X_5 at random in Z_N^* and computes their product, X, and X_i^2 mod N for all i=1,...,5. The product of these 5 squares, Z, is itself a square. One square root of Z mod N is X, which has Jacobi symbol equal to 1 (since the Jacobi symbol is multiplicative). The user thus computes Y one of the Jacobi -1 roots mod N. X_1...X_5 will be the public pieces of public key N, and the X_is its private pieces. The user gives trustee T_i private piece X_i (and possibly the public piece).

Instructions for the trustees
Trustee Ti checks that X_i has Jacobi symbol 1 mod N, then he squares X_i mod N, gives the key-management center his signature of X_i^2 mod N, and stores X_i and X_i^2 (or X_i and N).

Instructions for the key-management center
The center first checks that (-1/N)=1, that is, that for all x: (x/N)=(-x/N); which is partial evidence that N is of the right form. Upon receiving the valid signature of the public pieces of N and the Jacobi -1 value Y from the user, the center checks whether, mod N, the square of Y equals the product of the 5 public pieces. If so, the center is now guaranteed that it has a *split* of N. To make sure that it actually has the *complete factorization* of N, it must now perform the *missing procedure* (i.e., a procedure whose description we temporarily postpone) to check that N is the product of two prime powers. If this is the case, it *approves* N.

Again, it should be noticed that the Fair RSA scheme can be conveniently implemented in software.

Why does this work?
The reasoning behind the scheme is the following. The trustees' signatures of the X_i^2's (mod N) guarantee the center that every trustee Ti has stored a Jacobi symbol 1 root of X_i^2 mod N. Thus, in case of a court order, all these Jacobi symbol 1 roots can be retrieved. Their product mod N will also have Jacobi symbol 1, since this function is multiplicative, and will be a root of X^2 mod N. But since the center has verified that $Y^2 = X^2$ mod N, one would have two roots X and Y of a common square mod N; moreover, Y is different from X since it has a different Jacobi symbol, and is also different from -x, since (-x/N)=(x/N); in fact: (a) (-1/N) has been checked to be 1 and (b) the Jacobi symbol is multiplicative. Possession of such square roots, by Facts 1 and 2, is equivalent to having the factorization of N, *provided that N is a product of at most two prime powers*. That's why this last property has also been checked by the center before it approved N.

The reason that 4 (or less) trustees cannot factor N with the information in their possession is similar to the one of the discrete log scheme. Namely, the information in their possession solely consists of 4 random squares and their square roots mod N. This cannot be of any help in factoring N, since anybody could randomly choose 4 integers in Z_N^* and square them mod N.

The missing procedure
The center can easily verify that N is not prime. It can also easily verify that N is not a prime power by checking that N is not of the form x^y, for x and y positive integers, y>1. In fact, for each fixed y one can perform a binary search for x, and there are at most $\log_2(N)$ y's to check, since x must be at least 2 if N>1. It is thus now sufficient to check that N is the product of at most 2 prime powers. Since no efficient algorithm is known for this task when N's factorization is not known, any such check must involve the user who chose N, since he will be the only one to know N's factorization. In the spirit of what we have done so far, we seek a verification method that is (1) *simple*, (2) *non-interactive*, and (3) *provably safe*. The key to this is the older idea of Goldwasser and Micali of counting the number of prime divisors of N by estimating the number of quadratic residues in Z_N^*. In fact, if N is the product of no more than two prime powers, at least one number in four is a square mod N, otherwise at most 1 in 8 is. Thus the user can demonstrate that N has at most two different prime divisors by computing and sending to the center a square root mod N for at least, say, 3/16 of the elements of a prescribed list of numbers that are guaranteed to be randomly chosen. This list may be taken to be part of the system. Requiring the user to give the square roots of those numbers in such a random sequence that are squares mod N does not enable the center --or anybody else for that matter-- to easily factor N. To make this idea viable one would need some additional details. For instance, the trustees may be involved in choosing this public sequence so as to guarantee to all users the randomness of their elements; also the sequence should be quite long, else a user may "shop around" for a number N' that, though product of --say-- 3 prime powers, is such that at least 3/16 of the numbers in the sequence are squares modulo it; and so on. In "practice" this idea can be put to work quite efficiently by one-way hashing the user's chosen N to a small "random" number H(N), where H is a publicly known one-way hash function, and then generating a sufficiently long sequence of integers S(N) by giving H(m) as a seed to a reasonable pseudo-random number generator. This way, the number sequence may be assumed to be random enough by everybody, since the user cannot really control the seed of the generator. Moreover, the sequence changes with N, and thus a dishonest user cannot shop around for a tricky N as he might when the sequence is chosen before hand. Thus, the sequence chosen may be much shorter than before. If a dishonest user has chosen his N to be the product of three or more prime powers, then it would be foolish for him to hope that roughly 1/4 of the integers in the sequence are squares mod N. The scheme is of course non-interactive, since the user can compute on his own H(N), the number sequence S(N), and the square roots mod N of those elements in S(N) that are quadratic residues, and then sends the center only N and the computed square roots. Given N, the center will compute on its own the same value H(N) and thus the same sequence S(N). Then, without involving the user at all, it will check that, by squaring mod N the received square roots, it obtains a sufficiently high number of elements in S(N).

8. Basic Variants of the Basic Notion

Independent of the underlying PKC, several variants of the notion of a Fair PKC are possible, each, of course, possessing its own advantages and disadvantages, either in efficiency or fairness. Here, let us briefly discuss two important variants and then just mention a few others.

8.1 Relying on Fewer Shares

The schemes developed so far are robust only in the sense that some trustees, accidentally or maliciously, may reveal the shares in their possession without compromising the security of the system. However, our schemes so far rely on the fact that the trustees will collaborate during the recovering stage. In fact, we insisted that all of the shares should be needed for recovering a secret key. This may be disadvantageous, either because some trustees may after all be untrustworthy and refuse to give the Government the key in their possession, or because, despite all file back-ups, they may have genuinely lost the information in their possession. Whatever the reason, in this circumstance the reconstruction of a secret key will be prevented. Since VSS protocols exist (such as the GMW one) which tolerate any minorities of trustees to be bad, this problem can, in principle, be solved. However, the cost to be paid would be very very high, *independently of whether or not the number of trustees is small.* Thus, once again, one should resort to direct constructions. The ones discussed below have been selected because of their *simplicity*, their being quite practical whenever the number of trustees is small (in particualr they continue to be non-interactive), and their sufficient generality (though they will be illustrated only in the context of a single PKC). Slicker solutions can be obtained, but at the expense of greater complications. (One such method has been recently developed by Sidney based on a previous construction of Feldman [Fe87].)

THE SUBSET METHOD.
Each Fair PKC described so far is based on a (properly structured, non-interactive) VSS scheme with parameters n=5, T=5 and t=4. It may be preferable to have different values for our parameters; for instance, n=5, T=3, and t=2. That is, any majority of the trustees can recover a secret key, while no minority of trustees can predict it at all. This is achieved as follows (and it is easily generalized to any desired values of n,T and t in which T>t). We confine ourselves to exemplifying our method in conjunction with the Diffie-Hellman scheme. The same method essentially works for the RSA case as well.

The Subset Method for the Diffie-Hellman scheme

After choosing a secret key Sx in [1,p-1], user X computes his public key $Px=g^{Sx}$ mod p. (All computations from now on will be mod p.) User X now considers all triplets of numbers between 1 and 5: (1,2,3), (2,3,4), etc.
For each triplet (a,b,c), he randomly chooses *3* integers *S1abc,...,S3abc* in the interval *[1,p-1]* so that their sum *mod p* equals Sx. Then he computes the 3 numbers

$$t1abc=g^{S1abc},\ t2abc=g^{S2abc},\ t3abc=g^{S3abc}$$

The *tiabc*'s will be referred to as *public pieces* of *Px*, and the *Sxiabc*'s as *private pieces.* Again, the product of the public pieces equals the public key Px. In fact,

$$t1abc \cdot t2abc \cdot t3abc = g^{S1abc}\cdot g^{S2abc}\cdot g^{S3abc} = \\ = g^{(S1abc+S2abc+S3abc)} = g^{Sx} = Px$$

User X then gives trustee Ta *t1abc* and *S1abc*, trustee Tb *t2abc* and *S2abc*, and trustee Tc *t3abc* and *S3abc*, always specifying the triplet in question.

Upon receiving these quantities, trustee Ta (all other trustees do something similar) verifies that $t1abc=g^{S1abc}$, signs the value *(Px,t1abc,*(a,b,c)) and gives the signature to the key management center.

The key-management center, for each triple (a,b,c), retrieves the values *t1abc t2abc* and *t3abc* from the signed information received from trustees Ta, Tb and Tb. If the product of these three values equals Px and the signatures are valid, it approves Px as a public key.

The reason the scheme works, assuming that at most 2 trustees are bad, is that all secret pieces of a triple are needed for computing (or predicting) a secret key. Thus no secret key in the system can be retrieved by any 2 trustees. On the other hand, when after a court order, at least 3 trustees reveal all the secret pieces in their possession about a given public key, the Government has all the necessary secret pieces for at least one triple, and thus can compute easily the desired secret key.

THE SHARE REPLICATION METHOD.
In this solution, each of the 5 trustees is replaced by a group of new trustees. For instance, instead of a single trustee T_1, there may be 3 trustees, $T_1{}^1$ $T_2{}^1$ $T_3{}^1$; each of these trustees will receive and check the same share of trustee T_1. Thus, it is going to be very unlikely that all 3 trustees will refuse to surrender their copy of the first share. This scheme is a bit "trustee-wasteful" since it requires 15 trustees while it is enough that an adversary corrupts 5 of them to defeat the scheme. (However, one should appreciate that defeating the share-replication scheme is not as easy as corrupting any 5 trustees out of 15, since it must be true that a trustee is corrupted in each group.) The scheme has, nonetheless, two strong advantages: (1) *Scalability*: denoting by n the number of trustee groups, the computational effort of the scheme grows polynomially in n, no matter what the group size is, and thus -- if desired-- one can choose a large value for n; (2) *Repetitiveness*: if there are n trustee groups of size k each, one should only perform n "operations," in fact, each member of a trustee group gets a "xerox copy" of the same computation.

In the final paper we shall demonstrate that both methods can be optimized, but here let us instead move on to consider a far more important problem than efficiency.

8.2 Making Trustees Oblivious

There is another point that requires attention. Namely, a trustee requested by a court order to surrender his share of a given secret key may alert the owner of that key that his communications are going to be monitored. This serious problem can be attacked by a general-purpose machinery, yielding a purely theoretical solution. But, here, let us outline a simple and practical one, available when the cryptosystem used by the trustees possesses a nice algebraic property (essentially, *random self-reducibility* as introduced by Blum and Micali [BlMi]). This practical strategy is exemplified below by making oblivious (and Fair) the Diffie-Hellman scheme for the "all-shares" case, but also works for the RSA scheme and for fewer shares.

Oblivious and Fair Diffie-Hellman Scheme
(All-Shares Case)

The trustees' encryption algorithms
Since RSA itself possesses a sufficient algebraic property, let us assume that all trustees use *deterministic* RSA for receiving private messages. Thus, let Ni be the public RSA modulus of trustee Ti and ei his encryption exponent (i.e., to send Ti a message m in encrypted form, one would send m^{ei}mod Ni.)

Instructions for user U
User U prepares his public and secret key, respectively Px and Sx (thus Px = g^{Sx} mod p), as well as his public and secret pieces of the secret key, respectively ti and Sxi's (thus Px= t1· t2· ... ·t5 mod p and ti = g^{Sxi} mod p for all i). Then he gives to the key-management center Px, all of the ti's and the n values Ui=$(Sxi)^3$ mod Ni; that is, he encrypts the i-th share with the public key of trustee Ti.

(Comment: Since the center does not know the factorization of the Ni's this is no useful information to predict Sx, nor can it verify that the decryption of the n ciphertexts are proper shares of Sx. For this, the center will seek the cooperation of the n trustees, but without informing them of the identity of the user.)

Instructions for the center/trustees
The center stores the values tj's and Uj's relative to user U and then forwards Ui and ti to trustee Ti. If every trustee Ti responds to have verified that the decryption of Ui is a proper private piece relative to ti, the center approves Px.

Instructions in case of a court order
To lawfully reconstruct secret key Sx without leaking to a trustee the identity of the suspected user U, a judge (or another authorized representative) randomly selects a number Ri mod Ni and computes $yi = Ri^{ei}$ mod Ni. Then, he sends trustee Ti the value $zi = Ui \cdot yi$ mod Ni, asking with a court order to compute and send back wi, the *ei*-th root of zi mod Ni. Since zi is a random number mod Ni, no matter what the value of Ui is, trustee Ti cannot guess the identity of the user U in question. Moreover, since zi is the product of Ui and yi mod Ni, the ei-th root of zi is the product mod Ni of the ei-th root of Ui (i.e., Sxi) and the ei-th root of yi (i.e., Ri). Thus, upon receiving wi, the judge divides it by yi mod Ni, thereby computing the desired Sxi. The product of these Sxi's equals the desired Sx.

8.3 Time-Bounded Court-Authorized Eavesdropping

At present the Citizens have no guarantees that an illegal wiretapping will be initiated, or that a legitimate eavesdropping will be stopped at the prescribed date --indeed, courts usually authorize line-tapping for a bounded length of time only.

Fair PKCs are preferable to the *status quo* : the users are guaranteed that no illegal wire-tapping will be initiated, because without the help of the trustees their cryptosystems are impenetrable. Fair PKCs, however, are just as "bad" as the current system with respect to the time-bound issue. In fact, once the private key of the user of a Fair PKC erroneously suspected of unlawful activities is reconstructed, thanks to the collaboration of the trustees in response to a legitimate court order, it would be very easy for the agent monitoring her conversations (say, the Police) to exceed its mandate and keep on tapping (or allow someone else to tap) her line for a longer period of time.

Because it is our goal to strike a better balance between the needs of the Government and those of the Citizens in a modern democracy, we have developed various strategies for improving on the *status quo* and removing this weakness altogether.

8.3.1 Multiple Public-Keys

A very simple way to ensure time-bounded court-authorized line tapping consists of having each user choose a sufficient amount of matching public and secret keys, say one per month. Each public key will then be publicized specifying the month to which it refers. Someone who wants to send user X a private message in March, will then encrypt it with X's public March key. If this level of granularity is acceptable, the court may then ask the trustees to reveal X's secret keys for a prescribed set of months.

The disadvantage of this approach is that it requires a rather large "total public key," and it may be totally impractical if a fine granularity is desired.

8.3.2 Tamper-Proof Chips

One simple method to ensure time-bounded court-authorized eavesdropping makes use of *secure* chips; these are special chips that cannot be "read" from the outside, and cannot be tampered with. Thus, in particular, upon receiving an input they produce a specific output. but effectively hide all intermediate results. (Such chips are central to the Clipper Chip proposal.)

Time-bounded legal eavesdropping can be achieved by having the Police use secure chips possessing an internal and thus untamperable clock, the *Polchips*, in order to monitor the communications of a suspected user. Assume that a proper court order is issued to tap the line of user X from February to April. Then, each trustee will send the Polchip a digitally signed message consisting of his own share of user X's private key (encrypted so that only the Polchip will understand it). The Polchip can now easily compute X's secret key. Thus, if the Court sends to the Polchip a signed message consisting of, say, "decode, X, February-April"[1], since the Polchip has an internal clock, it can easily decrypt all messages relative to X for the prescribed time period. Then, it will destroy X's secret key, and, in order to allow further line tapping, a new court order will be required.

A main advantage of this approach is its simplicity; it does, however, require some additional amount of trust. In fact, the citizens cannot check, but must believe, that each Polchip is manufactured so as to work as specified above.

8.3.3 Algorithmically-Chosen Session Keys

In the multiple public-key method described above, each user selected and properly shared with the Trustees a number of secret keys of a PKC equal to the number of possible transmission "dates" (in the above example, each possible month). Within each specified date, the same public-secret key pair was used for directly encrypting and decrypting any message sent or received by any user. Time-bounded Fair PKCs, however, can be more efficiently achieved by using public keys only to encrypt session keys, and session keys to encrypt real messages (by means of a conventional single-key system). This is, in fact, the most common and efficient way to proceed.

Session keys are usually unique to each pair of users and date of transmission. Indeed, if each minute or second is considered a different date, there may be a different session key for every transmission between two users. Abstractly, the date may just be any progressive number identifying the transmission, but not necessarily related to physical time.

To achieve time-bounded court-authorized line tapping, we suggest to choose session keys *algorithmically* (so that the Trustees can compute each desired session key from information received when users enter the system), but *unpredictably* (so that, though some session keys may become known --e.g., because of a given court order-- the other session keys remain unknown).

The particular mechanics to exploit this approach is, however, important, because not all schemes based on algorithmically selected session keys yield equally convenient time-bounded Fair PKCs.[2]

---

[1] Alternatively, the time interval can be specified in the message of the trustees, since they learned it from the Court anyway.

[2] For instance, a time-bounded FAIR PKC that required the Police to contact the Trustees specifying the triplet (X,Y,D) in order to understand X's communication to Y at time D (belonging to the court-authorized time interval), might be deemed inpractical. A better scheme may allow the Police to contact the Trustees only once, specifying only X, Y, and D1 and D2,

An effective method is described below, basic properties first and technical details later.

The high-level mechanics of our Suggestion
In presence of a court order to tap X's lines beween dates D1 and D2, no matter how many dates there may be between D1 and D2, our method allows the Trustees to easily compute and give the Police a small amount of information, i=i(X,D1,D2), that makes it easy to tap X's lines in the specified time interval. The method consists of using a Fair PKC **F** together with a special additional step for selecting session keys for a conventional single-key cryptosystem C. In our suggested method, call it the *(F,C) method*, for any users X and Y, and any date D, there is a session key SXDY for enabling X to send a private message to Y at time D. Each user X is asked to provide the trustees not only with proper shares of his secret key in F, but also with *additional pieces of information* that enable them, should they receive a legitimate court order for tapping X between dates D1 and D2, to compute easily i(X,D1,D2) and hand it to the Police.

While the trustees can verify that they possess correct shares of X's secret key in **F**, we do not insist that the same holds for X's session keys. This decreased amount of verifiability is not crucial in this context for the following reasons. Assume in fact that the Police, after receiving i(X,D1,D2) from the Trustees in response to a legitimate court order, is unable to reconstruct a session key of X during the given time interval. This inability proves that X did not originally give the Trustees the proper additional pieces of information about his session keys. If so, the protocol will then ask the cooperation of the Trustees so as to reconstruct X's secret key in F (which is guaranteed possible since the trustees could verified to have legitimate shares of that key). Consequently, from that point on, all messages sent to X will cease to be private. Moreover, the adoption of a proper "hand-shaking protocol" will ensure the Police to understand all messages sent by X to any user who replies to him in the (F,C) system.[1]

In sum, therefore, malicious users who want to hide their conversations from law-enforcement agents even in presence of a court order, cannot do so by taking advantage of

---

in order to understand all the communications between X and Y at any date D in the time interval (D1,D2). Since, however, there may be quite many users Y to which the suspected user X talks to, also this scheme may be considered impractical.

[1] Of course, one may object that nothing is guaranteed about conversations between two users that are both malicious, since they may be using their own, altogether-different cryptosystems. Once more, however, we should remember that this is impossible to prevent, unless use of non-government-approved cryptosystems is made illegal. It is instead important to realize that, though all good citizens can enjoy a nation-wide PKC, the Government is at least guaranteed to have done NOTHING to facilitate private communications between malicious users. In fact, they cannot use **F** to exchange session keys for the recommended conventional cryptosystem **C**, since after reconstructing the relevant secret keys of **F** the Government could reconstruct such session keys and understand what any two malicious users would be saying to each other via **C**. Nor can all malicious users use **F** for exchanging secret keys relative to a special conventional cryptosystem **C'** that is known to criminals but unknown to the Government. In fact, any conventional cryptosystem that is used by a sufficiently large group of people will eventually become known to the Government. On the other hand, if each pair of malicious users X and Y were to use a dedicated conventional cryptosystem **Cxy** to talk to each other, they would have no convenience to gain from using the society-provided public-key cryptosystem **F**! In fact, if they could establish beforehand (i.e., without using **F**) a common and secret cryptosystem **Cxy**, they might as well exchange (without using **F**) a common secret key Kxy to be to used with any conventional cryptosystem.

the convenience of a nation-wide (**F**,**C**) system. They must go back to the cumbersome practice of exchanging common secret keys before hand, outside any major communication network. It is my firm opinion that the amount of illegal business privately conducted in this cumbersome way should be estimated minuscule with the respect to the one that might be conducted via a nation-wide *ordinary* PKC.

The Specifics Of Our Suggestion

The hand-shaking protocol of our suggested (**F**,**C**) cryptosystem is the following. When X wants to initiate a secret conversation with Y at date D, she computes a secret session key SXDY and sends it to Y using the Fair PKC **F** (i.e., encrypts it with Y's public key in **F**). User Y then computes his secret session key SYDX and sends it to X after encrypting it with the received secret key SXDY (by means of the agreed-upon conventional cryptosystem **C**). User X then sends SYDX to Y by encrypting it with SXDY. Throughout the session, X sends messages to Y conventionally encrypted with SXDY, and Y sends messages to X via SYDX. (If anyone spots that the other disobeys the protocol the communication is automatically terminated, and an alarm signal may be generated.) Thus in our example, though X and Y will understand each other perfectly, they will not be using a common, conventional key. Notice that, if the Police knows SXDY (respectively, SYDX), it will also know SYDX (respectively, SXDY).

Assume now that the Court authorizes tapping the lines of user X from date D1 to date D2, and that a conversation occurs at a time D in the time interval [D1,D2] between X and Y. The idea is to make SXDY available to the Police in a convenient manner, because knowledge of this quantity will enable the Police to understand X's out-going and in-coming messages, if the hand-shaking has been performed, independently of whether X or Y initiated the call. To make SXDY conveniently available to the Police, we make sure that it is easily computable on input SXD, a master secret key that X uses for computing his own session key at date D with every other user. For instance, SXDY = H(SXD,Y), where H is a one-way (possibly hashing) function.

Since there may be many dates D in the desired interval, however, we make sure that SXD is easily computable from a short string, i(X,D1,D2), immediately computable by the Police from the information it receives from the Trustees when they are presented with the court order "tap X from D1 to D2." For instance, in a 3-out-of-3 case, if we denote by i_j(X,D1,D2) the information received by the Police from Trustee j in response to the court order, we may set

$$i(X,D1,D2)= H(\ i_1(X,D1,D2),\ i_2(X,D1,D2),\ i_3(X,D1,D2)),$$

where H is a one-way (preferably hashing) function. Now, we must specify one last thing: what should i_j(X,D1,D2) consist of? Letting $X_j$be the value originally given to Trustee j by user X when she entered the system (i.e., X gives X_j to Trustee j together with the j-th piece of her own secret key in the FAIR PKC **F**), we wish that i_j(X,D1,D2) easily depend on X_j. Let us thus describe effective choices for X_j, i_j(X,D1,D2), and SXD. Assume that there are 2^d possible dates. Imagine a binary tree with 2^d leaves, whose nodes have n-bit identifiers --where n=0,...,d. Quantity i_j(X,D1,D2)is computed from X_j by storing a value at each of the nodes of our tree. The value stored at the root, node N_e (where e is the empty word), is X_j. Then a *secure* function G is evaluated on input X_j so as to yield two values, X_j0 and X_j1. The effect of G is that the value X_j is unpredictable given X_j0 and X_j1. (For instance, X_j is a random k-bit value and G is a secure pseudo-random number generator that, using X_j as a seed, outputs 2k bits: the first k will constitute value X_j0, the second k value X_j1.) Value X_j0 is then stored in the left child of the root (i.e., it is stored in node N0) and value X_j1 is stored in the right child of the root (node N1). The values of below nodes in the tree are computed using G and the value stored in their ancestor in a similar way. Let SX_jD be the value stored in leaf D (where D is a n-bit date) and $SXD=H(SX_1D,SX_2D,SX_3D)$. If D1 < D2 are n-bit dates, say that a node N *controls* the interval [D1,D2] if every leaf in the tree that is a descendent of N belongs to [D1,D2], while no proper ancestor of N has this property. Then, if $i_j(X,D1,D2)$ consists of the (ordered) sequence of values stored in the nodes that control [D1,D2], then

I. $i_j(X,D1,D2)$ is quite short (with respect to the interval [D1,D2]), and

II. For each date D in the interval [D1,D2], the value SX_jD stored in leaf D is easily computable from $i_j(X,D1,D2)$, and

III. The value stored at any leaf not belonging to [D1,D2] is not easily predictable from $i_j(X,D1,D2)$.

Thus if each user X chooses her X_j values (sufficiently) randomly and (sufficiently) independently, the scheme has all the desired properties. In particular,

1. user X computes SXD very efficiently for every value of D.

2. When presented with a court order to tap the line of user X between dates D1 and D2, each Trustee j quickly computes $i_j(X,D1,D2)$. (In fact, he does not need to compute all values in the 2^n-node tree, but only those of the nodes that control [D1,D2].)

3. Having received $i_j(X,D1,D2)$ from every trustee j, the Police can, *very quickly* and *without further interaction with the Trustees*, compute
(3.1)SX_jD from $i_j(X,D1,D2)$ for every date D in the specified interval (in fact, its job is even easier since the SXiD's are computed in order and intermediate results can be stored)
(3.2) the master secret-session key SXD from the SX_jD's, and
(3.3) the session key SXDY from SXD from any user Y talking to X in the specified time interval.

Note, however, that no message sent or received before or after the time-interval specified by the court order will be intelligible to the Police (unless a new proper court order is issued).

9. Fair PKCs vs. the Clipper Chip

9.1 A Quick Review of the Clipper Chip

Also the Clipper Chip proposal is based on the notion of a set of trustees, but it is primarily aimed at conventional cryptosystems. Under the new proposal, users encrypt messages by means of secure chips (as defined in subsection 8.2). All these chips contain in their protected memory a common classified encryption algorithm E and possess a unique identifier. To "initialize" chip x, two Trustees A and B independently choose a secret number (call ax the secret choice of Trustee A and bx that of Trustee B), and remember which secret choice they have made relative to x. These two numbers are then given (somehow) to a chip factory that computes their exclusive-or, cx, and stores it into the protected memory of the chip. This ends the initialization of chip x. Thus after being initialized, each clipper chip possesses a secret key, whose value is at this point only known to the chip itself, though shares of it are stored with the two trustees. Since the chip is assumed to be tamper-proof, it can be handled and sold without any further precautions after being initialized. Assume now that user X has bought chip x, that user Y has bought an analogous chip y, and that the two users have *somehow* exchanged a common secret key Kxy. To privately send a message m to Y, X inputs m to chip x, which will then use the classified algorithm to (1) encrypt Kxy with key cx, and (2) encrypt message m with key Kxy, and then send both ciphertexts to Y. Y ignores the first ciphertext, but decodes the second one with the same key Kxy so as to obtain m. In case of a court order for monitoring X's conversations, the two trustees will retrieve their respective secret numbers ax and bx, and reveal them to the Police, which will then xor them so as to compute cx, decode the first ciphertext with cx so as to compute Kxy, and finally decode the second ciphertext with Kxy so as to compute m.

9.2 A Potential Weakness of the Clipper Chip

Before making any comparison with Fair PKCs, it should be noted that, in absence of a properly specified protocol, the step of having the trustees send their secret shares of the (future) secret key cx to the factory is a dangerous one. In fact, this step introduces a special party, the factory, that "single-handedly knows" the chip's secret (thus nullifying the very notion of a set of trustees), and is therefore single-handedly capable of tapping X's conversations independently of any court order. Worse, while we can hope that trustees will be chosen so as to be considered trustworthy by most people, the same trust will not presumably be enjoyed by a "factory party."

Though more inconvenient, it would thus be preferable to have trustee A itself first insert secret ax in the protected memory of chip x, and then ship chip x to trustee B so that it can directly insert its own secret bx, and then have the chip itself compute cx.

9.3 Comparison with Fair PKCs.

Though they share a common approach, we believe Fair PKCs to be superior to the Clipper Chip proposal in a variety of ways; in particular,

1. *Software versus Hardware*

   While Fair PKCs can be implemented in hardware or software, the Clipper Chip requires the use of secure hardware, and thus will drive up the cost of any devise using encryption.[1]

2. *Citizen Control*

   While in the Clipper Chip the user does not choose all keys on which her privacy depends, in a Fair PKC the user chooses all of her keys (and algorithms for that matter).

[3] It should be noted that even though in the particular implementation of time-bounded Fair PKCs of subsection 8.2 we recommend the use of secure hardware, this hardware is used by the legitimate monitoring agent, and thus it does not constitute a direct cost of the users. Moreover there will be much less monitoring agents than users.

On the other hand, the Government has at least as much control as in the Clipper Chip proposal. In either case, in fact, the Trustees have pieces that are guaranteed to be right.

3. *Flexibility*

Since in a Fair PKC the user chooses and knows all of her keys, it is easy to have the system satisfy convenient additional properties; for instance, relying on fewer shares (in the sense of section 8.1) could be a feature of crucial importance for the Government. As for another example, users may find it advantageous to use the same keys in different contexts (e.g., for their phones at work or at home) even if each of these different contexts has a different set of Trustees. This is not a problem for Fair PKCs; in fact, users, knowing all of their secret keys, can break them into a different set of proper shares, and give different set of shares to different sets of trustees, each time easily proving that they hold legitimate shares. (It should be noticed that, unless an enemy has all the shares of one set of trustees, having some of the shares of both sets is useless.).

4. *Public-Key*

If the Clipper Chip proposal wants to control crime in an effective manner, it should properly address the public-key scenario. In fact, once a nation-wide public-key distribution center is created[1] --with or without the help of the Government-- it will be easier for criminals to bypass the protection of the Clipper Chip. In fact, having one's encryption key properly publicized (e.g., by a nation-wide 411-like mechanism) may be more crucial and difficult a goal to achieve than entering in possession of a conventional cryptosystem chip. If not specifically forbidden, there will certainly be widely available "alternative" conventional-cryptosystem chips for use in conjunction with the publicly-available PKC. It is thus crucial for law-enforcement, in my opinion, to make sure that any public encryption key of a national PKC cannot be used to encrypt messages in a way that avoids court-authorized line tapping. This is the best way to extend to the field of encryption the proper system of "checks-and-balances" necessary in a democracy.

10. Final Thoughts

Fair PKCs are a new technical tool possessing the potential to improve on the *status quo*. Society must though decide which is the best way to use such a tool. Who should the Trustees be? How many should they be? For how long should line-tapping be authorized? We believe that answering questions like these requires a debate as public and wide as possible.

Acknowledgments

I wish to thank Dennis Branstad, Michael Dertouzos, John Deutch, Shafi Goldwasser, Oded Goldreich, Carl Keysen, and my wife Daniela for their comments and encouragement.

[4] A not unlikely event since it provides the most convenient way to achieve private communication.

References

[AwChGoMi] B. Awerbuch, B. Chor, S. Goldwasser and S. Micali. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. In *Proceedings of the 26th Annual IEEE Symposium of Foundations of Computer Science.* IEEE, New York, 1986, pp. 383-395.

[Be] J. Benaloh. Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret. Advances in Cryptology --Proceedings of Crypto '86. Springer Verlag, 1986.

[BeGoWi] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Fault-Tolerant Distributed Computing. In *Proceedings of the 20th ACM Symposium of Theory of Computing.* ACM, New York, 1988, pp. 1-10.

[Bl] G. Blakley. Safeguarding Cryptographic Keys. In *AFIPS - Conference Proceedings.* NCC, New Jersey, 1979, Vol. 48 (June), pp. 313-317.

[BlMi] M. Blum and S. Micali. How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. *Siam Journal on Computing,* 1984, vol. 13 (Novenber), pp. 850-863.
Proceeding Version: FOCS 1982

[ChCrDa] D. Chaum, C. Crepeau, and I. Damgard. Multi-party Unconditionally Secure Protocols. In *Proceedings of the 20th ACM Symposium of Theory of Computing.* ACM, New York, 1988, pp. 11-19.

[DiHe] W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Trans. Inform. Theory.* IT-22, 6 (Nov. 1976), IEEE, New York, pp. 644-654.

[Fe87] P. Feldman. A Practical Scheme for Non-Interactive verifiable Secret Sharing. In *Proceedings of the 28th Annual IEEE Symposium of Foundations of Computer Science.* IEEE, New York,1987, pp. 427-438.

[GoMi] S. Goldwasser and S. Micali. Probabilistic Encryption. *Journal of Computer Systems Science.* Academic Press, New York, Vol. 28 No. 2 (1984), pp. 270-299.

[GoMiWi*a*] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield Nothing but their Validity and a Methodology of Cryptographic Protocol Design. In *Proceedings of the 27th Annual IEEE Symposium of Foundations of Computer Science.* IEEE, New York,1986, pp. 174-187.

[GoMiWi*b*] O. Goldreich, S. Micali, and A. Wigderson. How To Play ANY Mental Game or A Completeness Theorem for Protocols with Honest Majority. In *Proceedings of the 19th Annual ACM Symposium of Theory of Computing.* ACM, New York, 1987, pp. 218-229.

[RaBe] T. Rabin and M. Ben-Or. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. In *Proceedings of the 21st ACM Symposium of Theory of Computing.* ACM, New York, 1989, pp. 73-85.

[RSA] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystens. Comm. ACM 21, 2 (Feb. 1978), pp. 120-126.

[Sh] A. Shamir. How to Share a Secret. *Communications of the ACM.* ACM, New York, 1979, Vol. 22, No. 11 (Nov.), pp. 612-613.