Accountable Privacy

Mike Burmester[1], Yvo Desmedt[1], Rebecca N. Wright[2], and Alec Yasinsac[1]

[1] Department of Computer Science, Florida State University, Tallahassee, FL, 32306–4530, USA
[2] Department of Computer Science, Stevens Institute of Technology, Hoboken, NJ, 07030, USA

Abstract. As the Internet has gained widespread use, and advanced technologies such as high-speed multi-media technologies and automated digital monitoring have become a reality, privacy is at the greatest risk of all time. At the same time, sophisticated threats from hackers, terrorists, thieves, and others that would abuse privacy highlight the need to find technologies that provide some accountability. However, the goals of accountability and of privacy appear to be in contradiction: accountability tends to be about determining which entities committed which actions, while privacy seeks to hide this information.
In this paper, we discuss the apparent conflict that exists between privacy and accountability. We survey some of the issues in privacy and in accountability and highlight research directions for balancing the needs of both.

1 Introduction

As more of our daily activities are conducted on networked computers, privacy has become harder to maintain. Advances in networking, data storage, and data processing make it easier for information to be retained and accessed. Privacy is an important issue to many people, businesses, and governments, though different entities may not even agree on what privacy is. Loosely speaking, privacy is the ability to control private information, including identity and identifiers, sensitive information such as medical or financial records, and information about certain kinds of personal, corporate, or government activity. The kind of privacy usually desired in the real world is not hiding all information from all parties, but rather having the ability to disclose selected information to selected parties under certain circumstances, while preventing other disclosure.

At the same time as technological advances have made it easier to store and access data, the value of such data has often increased. For example, widespread use of personal data for authentication purposes makes personal data an increasingly attractive target for potential criminals. Governments and businesses wish to carry out data mining for security or marketing purposes, often to an extent that many individuals find uncomfortably privacy-invasive. Governments and businesses themselves also have privacy concerns regarding their own sensitive or proprietary information, as well as wanting to avoid poor public relations associated with mishandling of their citizens' or customers' private information.

To appear in *Proceedings of the Twelfth International Workshop on Security Protocols, Cambridge, England, 26–28 April 2004.*

Although many think privacy is important, few would advocate a society in which no data is collected and no collected data is ever used. There are legitimate needs and desires for using collected data, including uses as varied as providing customers with their desired services, detection of terrorist or criminal plots or attacks underway, identification of terrorists, criminals, and hackers, and medical research. The goal, then, is to develop and deploy technologies and policies that satisfy both legitimate privacy needs and legitimate accountability needs, and that balance the sometimes conflicting desires of individuals and society. We start by discussing privacy and accountability separately, in Sections 2 and 3, and then discuss them in relation to each other in Section 4.

2 Privacy Issues and Abuses

Users often desire to hide their activities on the network. For example, a user may desire to access Internet services without allowing anyone to know (or preventing specific parties from knowing) that she accessed the service. Legitimate instances where users may desire anonymity include:

- a potential customer would like to "window shop" electronically without the shop knowing, e.g., the information he has gathered about competing products,
- an employee may not want her boss to know that she has been accessing employment services web sites (see e.g. [41]), and
- decision-making processes where ideas are intended to be judged based on their merits rather than on their originators.

On the other hand, undesirable uses of anonymity include sending threatening e-mail, money laundering, denial of service attacks, and spam, see e.g. [40, 14].

As discussed above, being able to identify oneself is a matter of authentication, while preventing others from accessing one's data is a matter of privacy. However, because knowledge of personal data is often used as a means of authentication, and because some means of authentication is often required in order to enforce limits on information access, the two are inextricably linked.

Some of the basic privacy issues are given in Figure 1. We note that some of the described "benefits" of privacy are very similar to some of the described "abuses." The difference is in the content and intention of the action, according to value judgments imposed by the owners of the network, the relevant laws, and/or social conventions. This makes a general purpose solution elusive, and suggests that legal and public policy issues must always remain part of any solution.

3 Accountability

Accountability hinges on the ability to attribute actions to the entity that caused those actions. It seems only possible if entities can be accurately identified, either

Controlling Privacy

1. Personal information
   - Identity and anonymity: I may or may not be X
   - Speech: I may or may not have said X
   - Activity: I may or may not have done X
   - Location: I may or may not have been at X
   - Knowledge: I may or may not have known X
2. Privacy with partial disclosure
   - Identity: I am not saying who I am, but I am not X or one in a list Y
   - Speech: I am not divulging what I said, but I never said X
   - Activity: I am not divulging what I did, but I never did X
   - Location: I am not saying where I am or was, but I was not at place X during time Y
   - Knowledge: I am not saying what I know, but I did not know X before time Y

   Partial disclosure can be useful, for example, for showing that you are not a member of some undesirable set, such as persons on a terrorist watchlist, without disclosing your identity.
3. Privacy benefits
   - Prevents fear of retribution and enables:
     - freedom through anonymity
     - freedom of speech, activity, movement and thought
   - Protects property rights for:
     - identity, activities, location and thoughts
4. Privacy abuses
   - Total anonymity precludes verification and lawful retribution
     - Freedom from personal retribution of malicious acts
     - Freedom from legal deterrence
     - Freedom from legal attribution
   - Emboldens malicious parties
   - Facilitates cover-up

Fig. 1.

individually or as part of a group [3]. Entity authentication [26] has been the topic of extensive research, mostly focused on cryptography as the enabling technology. Passwords and personal identification numbers (PINs) are the de facto authentication standards, though they provide only weak guarantees of authentication. While cryptography has broad power and flexibility in solving multiple security problems, its application to the accountability problem requires a trust infrastructure such as a public key infrastructure.

Beyond identification of entities, accountability also requires the ability to enact particular consequences for particular actions. Methods of accountability without authentication are also possible, if consequences can be enforced anonymously. For example, one might use anonymous digital cash to ensure that appropriate payments are made if and only if certain events occur, without requiring explicit authentication of those involved.

Accountability is presently accomplished by a combination of: entity and message authentication, action/event binding, monitoring, and trust infrastructures, each of which we elaborate on.

Entity and Message Authentication Methods. Identity may be traced [38] from an IP address, to a pseudonym [9], to an account name, to the registered name at the ISP, and often through other identifying stages, eventually, to some fundamental identifying information such as a social security number, a finger print, or possibly a DNA match. An important characteristic of authentication is the degree of confidence that can be achieved. Traditional methods depend on both rigor and heuristics to show that authenticated mappings are accurate. Another research direction addresses authentication methods based on interactive zero-knowledge proofs [20] .

Binding Actions to Events. Few mechanisms for binding actions to events have been proposed, and indeed, when such mechanisms have been engineered into the infrastructure, public outrage has purged them from the marketplace, e.g. Carnivore and Clipper [34]. On the other hand, many commercial and public domain mechanisms were developed using operational information (for example information included in a message that allows a response) to trace events to the action that caused the event, and to bind the root actions to an end user. Tools for cyberforensics have come a long way in the past five years. However, there is still more to be done, particularly to find tools that properly balance accountability with privacy.

Monitoring. To ensure accountability, monitoring must be feasible and effective. Tracing all packets on the Internet leads to massive data volumes that challenge even the most sophisticated data mining techniques to analyze. On the other hand, tracing too little activity leads to insufficient information to identify and prove the guilt of attackers, since large efforts are sometimes required to know the identity of a message originator. Despite the fact that legal actions have sometimes been taken, hackers have not been sufficiently deterred. The amount of effort required to trace perpetrators, plus the effect on the efficiency of the network, must be weighed against the effectiveness of doing so.

Trust Infrastructures. Public Key Infrastructures (PKIs) have been proposed and partially deployed as a method for managing trust in security protocols. However, there have also been advisories issued about the weaknesses of such infrastructures, particularly when they are improperly used [18]. Nonetheless, because of their architectural position between the end user and the actions taken by, and on the behalf of, the users, PKIs and related security protocol infrastructures offer an excellent environment that can balance accountability and privacy concerns when properly implemented. An important focus is to develop cryptographic infrastructure models, techniques, principles, and tools to facilitate accurate, efficient, privacy-balanced accountability.

To complement authentication methods, efforts must be made to investigate policies, tools, and techniques that facilitate accountability during system operation. Authentication in itself does not ensure accountability. Results must be traceable to action originators when necessary as a response to particular events. Traceability can either be triggered through policies that allow access under certain circumstances (along with necessary auditing or other mechanisms to ensure that these privileges are not abused), or more elegantly, through the existence of such events themselves. The classical example of the latter is Chaum's e-cash [8], in which it is the information contained in the double-spending of a coin that allows the traceability of the double spender. More recently, Jarecki and Shmatikov [28] extend this idea to releasing escrow after a pre-specified threshold of activity is reached.

In Figure 2, we highlight several issues related to accountability.

Managing Accountability

1. Binding identities to entities
   - Certificates, Tokens, Registration authorities
2. Associating actions with entities
   - Bind actions to identities to the following extent(s) and no more:
     - They can be successfully prosecuted
     - Victims can recoup losses
     - The extent of damage can be verified
   - Malicious parties can be found, but only when triggering events occur and/or when approved by proper authority
     - Federal Communication Commission E-911 Technology
   - Non-repudiation without unreasonable search
3. Associating (Intellectual) Property to Entities

Fig. 2.

4 Balancing Privacy and Accountability (Responsible Privacy)

Two canonical examples of situations in which demands of accountability must be balanced with demands of privacy are electronic voting and digital cash. Keeping a balance between the conflicting rights of different parties seems almost impossible. However, early work on electronic voting (e.g. [24, 23, 27, 37]) and digital cash showed that some balance is possible. Additionally, research on some forms of key escrow (e.g. [2, 29, 34, 16, 15]) has suggested that it is possible to deal with conflicting requirements in a "fair" or "equitable" way using cryptographic techniques.

We note that it is not the case that privacy is necessarily the realm of the individual, nor accountability of society. As discussed before, business and governments also have privacy needs. Conversely, individuals are often well-served by a system of accountability so that they know there will be consequences for others if individuals' data is abused, as well as a deterrence effect of such consequences. In particular, a necessary component for preserving privacy in a system that allows some traceability is accountability of those that are sometimes allowed to violate privacy so that they do not routinely abuse this ability.

To properly analyze the requirements of accountability and privacy, one must understand and balance a number of potentially conflicting desires. In particular, it is important to consider the conflicts between:

- Anonymity and identification
- Confidentiality and required information disclosure
- Freedom of action balanced with attribution of action
- Cyber-privacy and cyber-forensics
- Free speech and liability/copyright

We address these tradeoff issues in more detail in the following subsections, as well as discussing some potential directions for solutions.

4.1 Anonymity balanced with identification

Identity protection is commonly accomplished through anonymity. Unfortunately, anonymity may be abused, and used to undermine the protection goal of accountability [14]. In particular, malice accomplished anonymously cannot be deterred by retribution. On the other hand, as we discussed before, there are scenarios where anonymity is desirable or even necessary. Clearly, anonymity and identification both have an important role to play in security and balancing their conflicting characteristics will require significant effort.

We recognize a natural conflict between allowing free speech and enforcing liability and copyright laws. For example, the owner of a Web page wants freedom to post arbitrary information, but should be liable for the content. In some countries, such as Germany and Britain, Internet Service Providers have decided unilaterally to censor controversial Web pages, an overly simplistic solution to solving this accountability problem (by removing content that might need its originators identified) that unnecessarily restricts freedom of speech.

Findings of a National Security Council study reflect similar tradeoffs between confidentiality and authentication [39], (p. 214):

> The committee emphasized the importance of authentication (over confidentiality) for both technical and policy reasons. The technical reason is that authentication is the first line of defense against the most serious threats to NISs [Network Information Systems] for critical infrastructures—intruders attempting to deny the benefits of using NISs to authorized users.

A Toy Example: Balancing Free Speech with Liability

A speaker, Alice, distributes shares of a message to Bob and Carol. The message is a binary string m. Bob's share is a random binary string m_1 which has the same length as m, and Carol's share is m_2, where $m_2 = m_1 \oplus m$ (so $m = m_1 \oplus m_2$). Bob and Carol together can compute the message m, but separately they get no information about m. This is a 2-out-of-2 secret sharing scheme, but the shares are not linked to Alice, so Alice is not liable (accountable) for the content of m.

Next, suppose that Alice appends to each share m_i her digital signature. This enables accountability, but results in loss of anonymity. For anonymity, Alice may encrypt her signatures with the public key of a trusted friend, Justice, who will only reveal Alice's signatures when compelled by a legitimate authority.

However, this toy solution does not really solve the problem unless everyone trusts Justice and agrees on the conditions under which the signatures should be revealed. Clearly Alice's privacy is dependent on Justice. If Justice is untrustworthy or may be subjected to too much pressure from others, or if Justice's computer systems are not sufficiently well-protected from outside attack, then Alice's privacy is at risk. Privacy also requires trust on the part of Bob and Carol who may not know Justice. Similarly, accountability requires that Justice will in fact reveal the signatures under the appropriate conditions. If Justice is really working for Alice and will not reveal the information, or if Justice accidentally misplaces the relevant files, then accountability will not be properly served.

Since such mutually trusted parties do not usually exist, it become necessary to have a complex system of checks and balances to prevent and/or detect misuse. One component of such a solution is to share the signature among many justices using robust threshold techniques, so multiple justices must collaborate to reveal the signatures, and a few malicious justices cannot prevent such revelation.

Fig. 3.

As we discussed before, often the only difference between desirable and undesirable uses of anonymity may be in the content and intention of the action, according to some kind of social assessment. For example, the U.S. Constitution provides for freedom of speech, but there are some exceptions, such as malicious, slanderous, or threatening speech. On the other hand, political speech has special protections: Supreme court ruling precludes laws requiring identity on political flyers.

Several cryptographic models will support the security tradeoff issue of anonymity and identification. For example, pseudonym models, blind cryptography [8, 11, 10], e-commerce, e-auctions, and, of course, e-voting models.

4.2 Confidentiality balanced with required information disclosure

Another easily recognizable conflict is between confidentiality and authentication. Once the identity of the origin is divulged for authentication, the ability of entities to control all aspects of their privacy is significantly reduced. One option to protect confidentiality is to refuse to be authenticated or prove your identity. Unfortunately, authentication is a fundamental element of many security and network activities. Access control typically requires some form of identification. This opens the problem of authenticated all-or-nothing-disclosure-of-secrets (ANDOS) [6]. In ANDOS, the client privacy is protected, but without access control. We envision authenticated ANDOS will protect access control, while the server does not know which files the client has access to or those the client has accessed.

Similarly, if an entity wants to store information on a network and to protect that information from general access or manipulation, he must be able to distinguish himself as the information owner, or at the very least present some credential indicating authority to access the information. A similar conflict occurs with voting systems and auction systems.

Several cryptographic models address this security tradeoff. These employ fair [33] or equitable [7] public key encryption schemes in which the secret key is escrowed.

4.3 Freedom of action balanced with attribution of action

Privacy includes prevention of knowledge being gained by others of one's actions. This may be accomplished by either conducting activities in an undetectable or untraceable way. Unfortunately, such actions may be used to undermine accountability. In particular, bad acts accomplished anonymously cannot be deterred by fear of punishment.

To balance freedom of action and accountability, mechanisms may be devised that will attribute the action. Several distinct cryptographic tracing models can support this security tradeoff issue. For example, the broadcast encryption model can provide evidence of service theft by using tracing mechanisms [13, 30, 5, 31]. Additionally, digital fingerprinting models can be used to deter disclosure of secrets by trusted parties, through traitor tracing mechanisms. Watermarking is another cryptographic model. Another model involves privacy-preserving database queries, which we discuss in Section 4.7.

4.4 Privacy balanced with Cyber-forensics

Cyber-forensics techniques are frequently at odds with privacy considerations. At the core of cyber-forensics techniques is finding the identities of those responsible for actions. Moreover, it is also important to identify exactly when an action occurred, why it was taken, what the goal of the action was, and so on. A cyber-forensics expert seeks to know every detail about every aspect of every principal under investigation. Thus, the goals of privacy are apparently in direct conflict with the goals of cyber-forensics.

Current research on cyber-forensics focuses on how to use current and emerging technologies to track, examine, and correlate information, e.g. by wiretapping, confiscating computers, and using hysteresis properties of magnetism to recover erased data. One should explore before-the-fact policies and procedures that will facilitate after-the-fact system analysis. Techniques perfected for forensics applications must be combined with management policies and practices to give a level of accountability and a manner of situational awareness to privacy issues that are not presently possible by addressing operational policies and their impact on cyber-forensic efforts.

Cryptographic methods can also be used to extend cyber-forensic capabilities by assisting investigators at reconstructing elements of an intrusion, while protecting such information in the typical, non-intrusion case. This technology is based on research on copyright techniques that focus on using special encoding (as encryption) to enhance tracing of copyright violators.

Several cryptographic models address this security tradeoff. These include targeted/limited/controlled forensics tools. Of particular interest are privacy-preserving database queries (see Section 4.7).

4.5 Freedom of movement balanced with location tracking

One approach to balancing freedom of movement with location tracking is to reveal one's location only if unauthorized movement occurs. Closed circuit television, global positioning systems [42], and RFID tags can reveal location. Information release should be controlled by appropriate policy implemented by escrow or other security mechanisms. An alternative approach is to employ group identification (group entity authentication) where one identifies oneself as belonging anonymously to a group where anonymity is escrowed [17].

4.6 Bonded Privacy

In this approach, abuse of privacy forfeits the e-bond. The cryptographic model that addresses this tradeoff issue involves an anonymous entity, a Service Provider

(SP), a Trusted Arbiter(s) (TA), cryptographically verifiable transactions, and e-bonds. If the anonymous entity authorizes an illegal transaction, as adjudicated by the TA, the e-bond is forfeited and a payment is made to the SP.

4.7 Privacy-preserving database queries

Privacy-preserving database queries and privacy-preserving data mining seek to allow the computation of certain information, while protecting other information. For example, the simplest case of symmetrically private information retrieval allows a client to access an individual database record without learning anything else about the database, and without the database learning which record the client accessed. Many software vendors do not reveal the source code. If the source code is private then one cannot verify correctness, check for Trojan horses, etc. Worse, if source code development is outsourced to third parties, the issue of correctness becomes even more problematic, as trust is implicitly extended to the third party even if the existence of this party is unknown to the software consumer.

An approach that could be followed is to use a layered design and ramp schemes [4]. (A ramp scheme is a secret sharing scheme in which parties may learn some, but not all information.) In this approach the designer will give to each entity:

- the logical layout of the subroutines, and
- the source code of a subroutine,

such that no entity has access to more than one block (a block being the logical layout or a source code subroutine). Each entity will verify the correctness of the block and if correct certify it.

Although this approach may seem valid, it is easy to construct a counterexample, as shown in the following example.

> Suppose a corporation wants to design a secret block cipher algorithm. To prevent it to become public, it splits the algorithm in two and reveals to different experts half the scheme. Each expert group can now analyze each part and certify it is a block cipher. However, if the second part is the inverse function of the first, then the total is not a secure block cipher!

So the certification of each part is not sufficient. One needs extra information about their inter-operability. The question then is how to guarantee this while maintaining as much privacy as possible.

A question is whether the work on privacy-preserving database queries can help address this issue. One solution is to use general secure distributed computation [25], which allows splitting the problem without the need to reveal even a single line of source code. However this solution is completely impractical for realistic program sizes.

Privacy-preserving computation on large databases is a new and exciting area that shows a lot of promise in helping to balance privacy with information disclosure [32, 1]. However, much work remains to be done, such as understanding how to integrate query restriction [12] with privacy-preserving computation and how to combine provably private cryptographic methods [32, 21, 22] with very efficient randomization methods [1].

4.8 Emerging Approaches: New Models for Accountable Privacy

Good models are important tools for describing problems and their solutions formally. For each of the accountable privacy tradeoffs discussed above, a model is necessary. For some properties, such as privacy, we already have a model: Shannon's secrecy model, which is based on probability theory. Other models are based on computational complexity or economics. Although early research with computational complexity models led mainly to impractical schemes, recently several practical protocols have been proposed. One should, therefore investigate models based on probabilistic and computational complexity approaches. However, not all properties of accountable privacy have been formally modeled as yet. The work of Millen and Wright [35] may be a useful starting point for addressing liability.

Models for Accountable Privacy

1. e-Bay Model
   - Weakly authenticated accounts
   - Trust based on ongoing trust ratings
2. Business Model
   - Weakly authenticated accounts
   - Security is based on profit, i.e. it is more profitable to adhere to the rules
3. Insurance Model
   - Weakly authenticated accounts
   - Liability covered by third party insurance
4. Credit Card [Accountability Partner] Model
   - Weakly authenticated accounts
   - Institution or a groups of trusted users vouch for the protected entities
5. Deposit-Based Model
   - Weakly authenticated accounts
   - Entity provides deposit to guarantee liability in lieu of insurance

Fig. 4.

We propose that the overarching goal for addressing the conflicting requirements of privacy and accountability must be to: (a) identify the guilty and, (b) protect the innocent. We posit that it should be possible to enable entities to maintain a "reasonable level" of privacy as long as they do not abuse the privilege. Specifically, we seek tools that allow decision makers to evaluate the quantitative meaning of the reasonable level of privacy and what constitutes abuse. There is extensive existing research in security, cryptography, and trust infrastructures that, when coupled with new models, methods, and techniques can provide adequate accountability while concurrently balancing security with needs for privacy. Several emerging technologies offer attractive prospects for accountable privacy. We conclude this paper by listing some basic, emerging technology models in Figure 4.

References

1. R. Agrawal and R. Srikant, "Privacy-preserving data mining", *Proceedings of the 19th International Conference on Management of Data*, ACM Press, 2000, pp. 439–450.
2. M. Bellare and S. Goldwasser, "Verifiable partial key escrow", *Proceedings of the 4th ACM Conference on Computer and Communications Security*, 1997, pp. 78–91.
3. T. Beth, "Zur Sicherheit der Informationstechnik", *Informatik-Spektrum*, Vol. 13, Springer-Verlag, 1990, pp. 204-15 (in German).
4. G. R. Blakley and C. Meadows, "Security of Ramp Schemes", *Advances in Cryptology, CRYPTO 1984*, Springer-Verlag, 1984, pp. 242-68.
5. D. Boneh and M. Franklin. An efficient public key traitor tracing scheme. In *Advances in Cryptology — Crypto '99, (LNCS 1666)*, pages 338–353. Springer-Verlag, 1999.
6. G. Brassard, C. Crepeau, and J.-M. Roberts, "All-or-Nothing Disclosure of Secrets," *Advances in Cryptology: Crypto '86*, Springer-Verlag, LNCS 263, 1987, pp. 234-238.
7. M. Burmester, Y. Desmedt and J. Seberry, "Equitable Key Escrow with Limited Time Span". *Advances in Cryptology - Asiacrypt '98* LNCS 1514, Springer-Verlag, 1998, pp. 380-391.
8. David Chaum, "Blind Signatures for untraceable payments", *Crypto '82*, Plenum Press, New York, 1983, pp. 199–203.
9. David Chaum, "Security without identification: transaction systems to make big brother obsolete", *Communications of the ACM*, Vol. 28, No. 10, 1985, pp. 1030–1044.
10. David Chaum, "Showing Credentials without Identification: Transferring Signatures between Unconditionally Unthinkable Pseudonyms", *Auscrypt '90*, LNCS 453, Springer-Verlag, 1990, pp. 246–264.
11. David Chaum and Torben P. Pedersen, "Wallet Databases with Observers", *Crypto '92*, LNCS 740, Springer-Verlag, 1993, pp. 89–105.
12. F. Chin and G. Ozsoyoglu, "Auditing and inference control in statistical databases", *IEEE Transactions on Software Eng.*, Vol. 8, No. 6, April 1982, pp. 113–139.
13. B. Chor, A. Fiat, and M. Naor. Tracing traitors. In *Crypto '94, (LNCS 839)*, pages 257–270. Springer-Verlag, 1994.
14. David Davenport, "Anonymity on the Internet: why the price may be too high", *Communications of the ACM*, Vol. 45, No. 4, April 2002, pp. 33-35.

15. D. E. Denning and D. K. Branstad, "A Taxonomy of key escrow encryption systems", *Communications of the ACM*, Vol. 39, No. 3, 1996, pp. 34-40.
16. Y. Desmedt, "Securing Traceability of Ciphertexts—Towards a Secure Software Key Escrow System", *Advances in Cryptology—Eurocrypt '95*, LNCS, Springer-Verlag, 1995, pp. 147-57.
17. Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous identification in ad hoc groups. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 609–626. Springer, 2004.
18. Carl Ellison and Bruce Schneier, "Ten Risks of PKI, What You Are Not Being Told About PKI", *Computer Security Journal* , Vol. XVI, No. 1, 2000, pp. 1–7.
19. A. Fiat and M. Naor, "Broadcast Encryption", *Advances in Cryptology–Crypto '93*, LNCS 773, Springer-Verlag, pp. 480–491, 1994.
20. Uriel Feige, Amos Fiat, and Adi Shamir, "Zero-knowledge proofs of identity, *Journal of Cryptology,* , Vol. 1, No. 2, pp. 77–94, 1988.
21. J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. Strauss, and R. N. Wright, "Secure multiparty computation of approximations", *Proceedings of 28th International Colloquium on Automata, Languages and Programming*, LNCS 2076, Springer, 2001, pp. 927–938.
22. M. Freedman, K. Nissim, and B. Pinkas, "Efficient Private Matching and Set Intersection", *Proceedings of Eurocrypt 2004*, LNCS 3027, Springer, 2004, pp. 1–19.
23. A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Election", *Advances in Cryptology-Auscrypt '92*, LNCS 718, Springer-Verlag, 1992, pp. 248–59.
24. J. Furukawa, H. Miyauchi, K. Mori, S. Obana, and K. Sako", "An Implementation of a Universally Verifiable Electronic Voting Scheme based on Shuffling", *Financial Cryptography 2002, 6th International Conference*, LNCS 2357, Springer-Verlag, 2003 pp. 16–30.
25. O. Goldreich, S. Micali, and A. Wigderson, "How to Play Any Mental Game", *Proc. of 19th STOC*, pp. 218-229, 1987.
26. D. Gollmann. "What do we mean by Entity Authentication?" *In Proceedings of the 15th IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, 1996, pp. 46–54.
27. M. Hirt and K. Sako, "Efficient Receipt-Free Voting Based on Homomorphic Encryption", *Advances in Cryptology—Eurocrypt 2000*, LNCS 1807, Springer-Verlag, 2000, pp. 539–556.
28. S. Jarecki and V. Shmatikov, "Handcuffing Big Brother: an Abuse-Resilient Transaction Escrow Scheme", *Advances in Cryptology—Eurocrypt 2004*, LNCS 3027, Springer-Verlag, 2004, pp. 590–608.
29. L. R. Knudsen and T. P. Pedersen, "On the difficulty of software key escrow", *Advances in Cryptology—Eurocrypt '96*, LNCS 1070, Springer-Verlag, 1996, pp. 237–44.
30. K. Kurosawa and Y. Desmedt. Optimum traitor tracing and asymmetric schemes. In *Eurocrypt '98, (LNCS 1403)*, pages 145–157. Springer-Verlag, 1998.
31. Kaoru Kurosawa and Takuya Yoshida. Linear code implies public-key traitor tracing. In *Public Key Cryptography*, volume 2274 of *LNCS*, pages 172–187. Springer, 2002.
32. Y. Lindell and B. Pinkas, "Privacy preserving data mining", *J. Cryptology*, Vol. 15, No. 3, 2002, pp. 177–206. An earlier version appeared in *Crypto 2000*.
33. S. Micali, "Fair Cryptosystems", *Advances in Cryptology, Proceedings of Crypto' 92*, LNCS 740, Springer-Verlag, 1992, pp. 113–138.

34. S. Micali and R. Sidney, "A simple method for generating and sharing pseudo-random, with applications to Clipper-like key escrow systems", *Advances in Cryptology—Crypto '95*, LNCS 963, Springer-Verlag, 1995, pp. 185–196.
35. J. K. Millen and R. N. Wright. "Reasoning about Trust and Insurance in a Public Key Infrastructure," *Proceedings of 13th IEEE Computer Security Foundations Workshop*, IEEE Computer Society, July 2000, pp. 16–22.
36. Donald Rumsfeld. US Secretary of State, Comments to the press, Sept 12, 2001, `http://www.defenselink.mil/transcripts/2001/t09122001_t0912sd.html`.
37. K. Sako and J. Kilian, "Receipt-free mix-type voting scheme", *Advances in Cryptology—Eurocrypt '95*, LNCS 921, Springer-Verlag, 1995, pp. 393–403.
38. Didier Samfat, Refik Molva, N. Asokan, "Untraceability in mobile networks", *Proceedings of the 1st annual international conference on Mobile computing and networking*, Berkeley, California, 1995, pp. 26-36.
39. Fred B. Schneider. *Trust in Cyberspace*, National Academy Press, 1999.
40. B. von Solms and D. Naccache. On blind signatures and perfect crimes. *Computers and Security*, 11(6):581–583, October 1992.
41. Gene Spafford, "Protecting Personal Information in Academia," *Computing Research News*, May 2001, pp. 3, 4, 12. `http://www.cra.org/CRN/articles/may01/spafford.html`.
42. Mike Spreitzer and Marvin Theimer, "Providing location information in a ubiquitous computing environment" (panel session), *December 1993 ACM SIGOPS Operating Systems Review, Proceedings of the fourteenth ACM symposium on Operating systems principles,* Vol. 27, No. 5, 1993, pp. 270–283.