COVER SHEET FOR PROPOSAL TO THE NATIONAL SCIENCE FOUNDATION

PROGRAM ANNOUNCEMENT/SOLICITATION NO./CLOSING DATE/if not in response to a program announcement/solicitation enter NSF 00-2

NSF 00-89 **07/25/00**

FOR CONSIDERATION BY NSF ORGANIZATION UNIT(S) (Indicate the most specific unit known, i.e. program, division, etc.)

CCR - COMMUNICATIONS RESEARCHCCR - THEORY OF COMPUTING

FOR NSF USE ONLY

NSF PROPOSAL NUMBER

0093140

DATE RECEIVED	NUMBER OF COPIES	DIVISION ASSIGNED	FUND CODE	DUNS# (Data Universal Numbering System)	FILE LOCATION
				047120084	

EMPLOYER IDENTIFICATION NUMBER (EIN) OR TAXPAYER IDENTIFICATION NUMBER (TIN)

946036494

SHOW PREVIOUS AWARD NO. IF THIS IS
☐ A RENEWAL
☐ AN ACCOMPLISHMENT-BASED RENEWAL

IS THIS PROPOSAL BEING SUBMITTED TO ANOTHER FEDERAL AGENCY? YES ☐ NO ☒ IF YES, LIST ACRONYMS(S)

NAME OF ORGANIZATION TO WHICH AWARD SHOULD BE MADE

University of California-Davis

AWARDEE ORGANIZATION CODE (IF KNOWN)

0013136000

ADDRESS OF AWARDEE ORGANIZATION, INCLUDING 9 DIGIT ZIP CODE

Ofc of the Vice Chancellor for Research
1 Shield Avenue, 410 Mrak Hall
Davis, CA. 95616

NAME OF PERFORMING ORGANIZATION, IF DIFFERENT FROM ABOVE

PERFORMING ORGANIZATION CODE (IF KNOWN)

ADDRESS OF PERFORMING ORGANIZATION, IF DIFFERENT, INCLUDING 9 DIGIT ZIP CODE

IS AWARDEE ORGANIZATION (Check All That Apply)
(See GPG II.D.1 For Definitions) ☐ FOR-PROFIT ORGANIZATION ☐ SMALL BUSINESS ☐ MINORITY BUSINESS ☐ WOMAN-OWNED BUSINESS

TITLE OF PROPOSED PROJECT **New Directions in Cryptography for Electronic Commerce**

REQUESTED AMOUNT	PROPOSED DURATION (1-60 MONTHS)	REQUESTED STARTING DATE	SHOW RELATED PREPROPOSAL NO., IF APPLICABLE
$ **259,930**	**60** months	**07/01/01**	

CHECK APPROPRIATE BOX(ES) IF THIS PROPOSAL INCLUDES ANY OF THE ITEMS LISTED BELOW

☐ BEGINNING INVESTIGATOR (GPG 1.A.3)
☐ DISCLOSURE OF LOBBYING ACTIVITIES (GPG II.D.1)
☐ PROPRIETARY & PRIVILEGED INFORMATION (GPG II.D.10)
☐ NATIONAL ENVIRONMENTAL POLICY ACT (GPG II.D.10)
☐ HISTORIC PLACES (GPG II.D.10)
☐ SMALL GRANT FOR EXPLOR. RESEARCH (SGER) (GPG II.D.12)
☐ VERTEBRATE ANIMALS (GPG II.D.12) IACUC App. Date _____
☐ HUMAN SUBJECTS (GPG II.D.12)
Exemption Subsection _____ or IRB App. Date _____
☐ INTERNATIONAL COOPERATIVE ACTIVITIES: COUNTRY/COUNTRIES _____
☐ FACILITATION FOR SCIENTISTS/ENGINEERS WITH DISABILITIES (GPG V.G.)
☐ RESEARCH OPPORTUNITY AWARD (GPG V.H)

PI/PD DEPARTMENT
Computer Science

PI/PD FAX NUMBER
650-812-4471

PI/PD POSTAL ADDRESS
410 Mark Hall

Davis, CA 956168671
United States

NAMES (TYPED)	High Degree	Yr of Degree	Telephone Number	Electronic Mail Address
PI/PD NAME **Matthew Franklin**	**Ph.D**	**1994**	**916-752-2075**	**franklin@parc.xerox.com**
CO-PI/PD				
CO-PI/PD				
CO-PI/PD				
CO-PI/PD				

Electronic Signature

New Directions in Cryptography for Electronic Commerce
M. Franklin

PROJECT SUMMARY

The research community has been rushing to keep up with the commercial sector in the area of electronic commerce security. We are still searching for the right formal frameworks through which the deeper questions can emerge. The future study of electronic commerce security will require new models and abstractions. Significant progress may come once we have identified important open problems and grand challenges that can inspire our next generation of computer science researchers. There is an opportunity to contribute to a true science of electronic commerce security, rather than merely a bundle of profitable business ideas.

In this proposal, I describe a five-year plan to help lay the foundation for this new science. Over those five years, I will develop undergraduate courses, graduate seminars, scientific symposia, and a comprehensive personal research program. I will help bring together both the academic and industrial dimensions of e-commerce security. I will help to train the next generation of computer professionals with those fundamentals they will need to know to flourish in an unpredictable business landscape. I will help to inspire the next generation of computer scientists with research questions that combine scientific depth with practical impact.

My personal research program will focus on four main areas: secure multi-party protocols in e-commerce, anonymity and privacy mechanisms in e-commerce, fraud detection and prevention in e-commerce, and secure content distribution mechanisms in e-commerce. I have a number of reasons for these choices. They are all areas that I believe are ripe for significant future progress. They are all areas in which I have made significant contributions, both theoretical (models, protocols, proofs) and practical (experiments, prototypes). Future progress in these areas is also likely to bridge theory and practice. Lastly, I believe that there are deeper connections to be found through cross-fertilization and combining of ideas among them.

TABLE OF CONTENTS

For font size and page formatting specifications, see GPG section II.C.

Section		Total No. of Pages in Section	Page No.* (Optional)*
Cover Sheet (NSF Form 1207) (Submit Page 2 with original proposal only)			
A	Project Summary (not to exceed 1 page)	1	
B	Table of Contents (NSF Form 1359)	1	
C	Project Description (plus Results from Prior NSF Support) (not to exceed 15 pages) **(Exceed only if allowed by a specific program announcement/solicitation or if approved in advance by the appropriate NSF Assistant Director or designee)**	15	
D	References Cited	3	
E	Biographical Sketches (Not to exceed 2 pages each)	2	
F	Budget (NSF Form 1030, plus up to 3 pages of budget justification)	6	
G	Current and Pending Support (NSF Form 1239)	1	
H	Facilities, Equipment and Other Resources (NSF Form 1363)	1	
I	Special Information/Supplementary Documentation	1	
J	Appendix (List below.) **(Include only if allowed by a specific program announcement/ solicitation or if approved in advance by the appropriate NSF Assistant Director or designee)**		
	Appendix Items:		

*Proposers may select any numbering mechanism for the proposal. The entire proposal however, must be paginated. Complete both columns only if the proposal is numbered consecutively.

New Directions in Cryptography for Electronic Commerce
M. Franklin

PROJECT DESCRIPTION

1. Objectives and Significance

One of the main objectives of this proposal is to help advance our state of scientific knowledge for e-commerce security. This objective is of course directly linked to my personal research agenda. What is equally clear to me is that this objective is crucial to my educational agenda as well. I feel that there are tremendous pressures these days to commercialize any good idea – and many mediocre ones -- in e-commerce security. As a consequence, many promising research results never appear in scientific conferences or journals. Many good students are lost before they finish their degrees, or never bother to enroll. Part of the problem is the lure of industry, but there is a corresponding failure of the universities to provide a sufficiently attractive alternative. A science of e-commerce security, rather than a mere collection of profitable business ideas, may contribute towards such an alternative. If there is more of a solid foundation to the area, then more students may decide that their best long-term strategy is to ground themselves thoroughly in this new knowledge.

E-commerce will be a dominant force in our economy over the next decade. How can we ensure that security will be handled properly, or that privacy concerns will be addressed suitably? Perhaps the best insurance is to see that the right ways of thinking about these problems are inculcated in the widest possible manner to our newest computer scientists and software engineers. Important cryptographic techniques and security ideas must not be left in the hands of a small group of researchers and consultants or they may not be deployed appropriately. When the ethical dimensions of privacy technology are factored in, then the urgency of this educational task becomes even clearer. It is my desire to help instill in the next generation of computer professionals what they need to know to make e-commerce a success, commercially and culturally.

I hope to bridge a gap between academia and industry through my proposed activities. I feel that I am uniquely qualified to do this, since I was at several first-rate industrial research labs for many years, and since my work in secure e-commerce spans the theoretical (models and proofs) and the practical (experiments and prototypes). Through research collaborations, and the development of symposia, I will help to improve the lines of communication with industry. This will have many positive benefits, because it will feed back on the quality of the research problems that I work on with my students, and because it will directly impact the development of my course curricula. I have often found my industrial research colleagues eager to find good graduate students that they can influence with the research questions that have arisen through their practically motivated work. This will help my industry-bound graduate students by guiding them to fruitful problems that will be considered practically significant as well as scientifically sound.

I also expect this plan to have significant impact internationally through collaboration with foreign researchers. For example, I have recently joined in a proposal to the South Korean Information Technology Research Center to study secure protocols for e-commerce with Professor Kunsoo Park at Seoul National University. If that proposal is accepted, then the cost of some visits and seminars in South Korea will be subsidized by the ITRC That would dovetail very naturally with the 5-year plan that I outline here. I expect to make similar connections with my current and future collaborators around the world.

2. Relation to Current State of Knowledge

There are a number of researchers now working on problems that I consider related to secure e-commerce. However, as I have stated above, the aggregate looks more like a bundle of clever and profitable ideas than a true scientific discipline. This is not a criticism of how the research community has proceeded so far, but rather a realistic reflection of the current state of knowledge. The purpose of my five-year plan is to help lay the groundwork for the field to mature into a science. By helping to train the next generation of researchers, and by working on topics where deeper connections might be found, I propose to help move the field toward this goal.

There are by now a number of university courses in cryptography and security (see, e.g., http://avirubin.com/courses.html for a recent compilation). There is also an emerging collection of university courses in e-commerce, offered primarily by Computer Science Departments and Business Schools. However, there are relatively few courses that focus specifically on security for e-commerce. My proposed curriculum development will help meet this need.

My proposed symposia will address the lack of specialized meetings for researchers in the area of secure e-commerce. Some of this research gets reported at more general conferences and workshops for cryptography (e.g., Crypto, Eurocrypt, Asiacrypt, Financial Crypto), security (e.g., IEEE Oakland, ACM Computer and Communication Security), or e-commerce (e.g., ACM E-Commerce Conference). There have been occasional workshops on topics related to security in e-commerce, e.g., an upcoming one-day workshop in Greece in November 2000. There have also been occasional invited talks and panels on e-commerce security at other conferences. However, there is much work to be done to create the right scientific meeting grounds for stimulating future development. My symposia will contribute to this field-building process, by offering sharply focused agendas that will draw together like-minded researchers.

There are some interesting start-up companies working on some aspects of the problems that I will be considering, e.g., Zero Knowledge Systems, E-Cash Technologies, VoteHere.net, and Intertrust, to name a few. Some of these start-ups are doing exciting cutting-edge work. However, many of the underlying cryptographic ideas that are being implemented were first conceived at least ten years ago. I hope to establish collaborative ties and mutually profitable dialogues with relevant start-ups whenever appropriate.

3. Outline of Plan of Work

	Year 1	Year 2	Year 3	Year 4	Year 5
Graduate seminar	**X**		**X**		
Undergrad lecture class		**X**		**X**	
Scientific symposia		**X**		**X**	
Research and collaborations	**X**	**X**	**X**	**X**	**X**

I plan to create and teach graduate seminars at U. C. Davis on security in e-commerce that will focus on new research topics. The goal will be to lead graduate students as quickly as possible to the frontiers of our knowledge, and help guide the search for possible thesis directions. I also plan to create and teach undergraduate courses that survey a broad range of topics related to e-commerce security, both theoretical and practical. The idea is to give a familiarity with a wide variety of tools and ideas.

I plan to organize and chair two scientific symposia. These will be half-day or full-day programs of talks from leading researchers in the field of secure e-commerce. I will model these on the symposium that I am chairing for the AAAS Annual Meeting (San Francisco, February 2001 on "Mathematical aspects of intellectual property management on the Internet. My future symposia will focus on other topics in secure e-commerce that deserve a closer look by the research community and the broader public.

Throughout the five years, I plan to conduct my own research agenda in secure e-commerce. The research will proceed with students and colleagues at U.C. Davis, as well as with students and colleagues at other universities and industrial research labs. The end products of this research will include papers for recognized scientific conferences and journals, and invited talks when appropriate to announce new results.

My research will also culminate in new experiments, prototypes and implementations. In my research to date, I have tried to include this practical dimension whenever possible. I have found it to be an excellent communication tool, as well as a means to probe deeper into a problem space. Secure e-commerce research lends itself to this practical dimension quite well. In the Summary of Prior Research, I discuss a number of my results in the area of secure e-commerce that benefited in this way.

The rest of this plan of work will discuss the four main areas on which my research will focus: secure multi-party protocols in e-commerce, anonymity and privacy mechanisms in e-commerce, fraud detection and prevention in e-commerce, and secure content distribution mechanisms in e-commerce. I have several reasons for this selection. First, they are all areas in which I have already made significant contributions, as discussed in the section on Prior Research. Second they are all areas, which I believe are ripe for

future progress. Third, I believe there are deeper connections to be found by combining ideas from these areas

3.1 Plan of Work for Secure Multi-Party Protocols in E-Commerce

The idea of secure multi-party protocols (or secure distributed computation) is an important cryptographic notion that has emerged over the past fifteen years. Powerful completeness theorems developed in the late 1980's [GMW87, BGW88, CCD88] showed how any function can be cooperatively computed when the input is divided among mutually mistrustful parties. If there were a fully trusted neutral party, then all of the mutually mistrustful parties could simply give their secret inputs to the neutral party to compute on their behalf. Thus these completeness theorems can be viewed as providing a multi-party protocol that in some sense simulates a fully trusted neutral party.

There are two main fault models (also called "adversary settings") that are considered. In the "passive fault" setting (also called "honest-but-curious"), all parties follow the protocol faithfully, but later some subset of the parties pool their information (private inputs, local calculations, transcript of incoming messages) in an attempt to learn something new about the other parties' private inputs. In the "active" fault setting (also called "Byzantine"), some subset of the parties deviate from the protocol in an arbitrarily malicious and coordinated manner, in an attempt either to learn something new about the other parties' private inputs, or to prevent the other parties from computing the function correctly.

The maximum possible fault tolerance achievable through these completeness theorems depend on the adversary setting and on the communication model for the participants. There are a few main communication models that have been considered. For example, in one important setting, each pair of parties is connected by a private and authenticated channel. In this setting, less than one-half of the parties may be passive faults, or less than one-third may be active faults. If all of the parties also share an authenticated broadcast channel, then less than one-half of the parties may be active faults. These particular results are sometimes called "unconditional" or "non-cryptographic" because the protocols make no cryptographic hardness assumption (encompassing such an assumption in the private channels model of communication).

Although quite powerful, these completeness theorems can be somewhat inefficient to use in practice. The protocols are in the form of "meta-protocols" that work from a circuit-level description of the function to be computed. Here the basic gates of the circuit may be arithmetic (arbitrary fan-in addition and 2-ary multiplication over a finite field) or Boolean (NOT gates and 2-ary OR). The bit complexity of the resulting protocol is at best proportional to the number of basic gates in the circuit, while the round complexity is at best proportional to the depth of the circuit. This is unwieldy for many functions of practical importance. For example, imagine the number of basic gates in a circuit to compute an RSA key (for distributed key generation).

Fortunately, we do not always have to rely on the meta-protocols directly. For example, I have found an especially efficient secure multi-party protocol for computing an RSA key. This protocol is based in part on ideas and techniques from the completeness theorems, but it also introduces new ideas to achieve its speed. This work is described in more detail in the Summary of Prior Research.

I feel that there is still a lot for us to learn about the proper application of these general completeness theorems. In particular, we should continue to look for efficient special-purpose protocols for functions of practical importance. This has been successful for a number of specific functions of importance to e-commerce, including secure auctions, key escrow agencies, certification authorities, fair exchange protocols, and secret ballot elections. I list some of my contributions to these areas in the Summary of Prior Research.

One exciting area for future investigation is to consider variations on the standard communication model. The great success of threshold cryptography [Des94] rests in part on the efficiency of the "combiner model" of communication. For example, to sign a message, each key-share holder simply sends one message to a neutral combiner who can then compute the signature while learning nothing useful about the key-shares. A related model for general secure computation in a three-party scenario is described by [FKN94]. It is interesting to explore communication patterns and trust assumptions that can lead to efficient protocols for specific functions of importance to e-commerce. This becomes especially intriguing if the messages could be piggybacked on preexisting protocols with matching communication patterns that would be executing anyway (e.g., SSL, or various payment schemes).

One important new application area for future research is the design of secure agents for autonomous e-commerce. In principle, an agent could be programmed on your behalf with all of your consumer preferences, negotiating strategies, and payment methods. This agent could then go out and shop on your behalf. In the process, it might interact with a number of other agents acting on the behalf of businesses and organizations. It might enter into alliances with other consumer agents to negotiate group discounts. There are a variety of privacy and security issues here. These kinds of interactions can be modeled as secure multi-party protocols. Theoretically, then, these agent interactions could be implemented using the general completeness results, but the result would be far too inefficient. Some progress towards more efficient solutions has been made by others (e.g., [ST98, CCKM2000]), but much remains to be done.

Another important direction is the search for new adversarial models that are relevant for secure e-commerce. Relatively unexplored adversarial models might need to be considered in greater depth, e.g., faulty parties that are "malicious but rational" [Nis99, MT99], or "malicious but uncoordinated" [BFG+99] or "malicious but undetectable" [CO99].

1. Can agent-based autonomous e-commerce be realized as efficient special-purpose secure multi-party protocols?

2. What other new applications of e-commerce can be realized as efficient special-purpose secure multi-party protocols?
3. What abstractions and models for e-commerce will lead to new completeness theorems for secure multi-party protocols?

3.2 Plan of Work for Anonymity and Privacy Mechanisms in E-Commerce

It is common for a security application to be a protocol among different kinds of parties with different security needs. In a secret ballot election protocol, for example, there might be voters and official talliers and independent observers. The security requirements for the voters are quite different from the security requirements for the other kinds of parties. In particular, only the voters have a true privacy requirement, i.e., their individual votes must be protected from disclosure. Of course, the talliers and observers have an indirect privacy requirement, in the sense that their actions must not disclose the secret votes. That is an obligation imposed on them by the true privacy requirement of the voters.

Many security applications for e-commerce have this flavor. The privacy concerns of ordinary consumers are by now well documented. Consumers are placed in a vulnerable position on the Web, faced with the disclosure of all kinds of sensitive information: their credit card numbers, buying habits, browsing patterns, and other vital statistics. By default, without an intelligent security design, sensitive information would flow directly to the consumer's ISP, the merchant's web server, or other data aggregation points.

The solutions being proposed at the moment for this problem are changes in policy and law. Certain kinds of data aggregation and data selling would become illegal, and data collection policies would have to be disclosed to consumers. This is an excellent first step to try to deal with a very difficult problem. In the long run, however, we will have to do better. Violations of these sorts of laws are difficult to identify, and difficult to prosecute. Violators may hide across unfriendly national borders, or disappear and reappear in the guise of a new business ("boiler-room" operations). It will always be difficult to prove that data was mishandled. The law might be exercised occasionally, e.g., for sting operations, but the limited resources of law enforcement may not be able to keep up with the data thieves.

Of course, it is possible to imagine the *automated* investigation and prosecution of data laws. This is an intriguing research direction, which might yield payoffs in the near term. There was recent progress along these lines by Narayanan Shivakumar, who designed copy detection systems for text, audio, and video in his Stanford Ph.D. thesis.

However, there is another approach, which yields a more solid kind of protection for consumers. If sensitive data is never disclosed in the first place, then there is no need to worry about how that data is being used. We use the term "privacy mechanisms" to refer to cryptographic protocols that offer this kind of protection for sensitive data. We use the term "anonymity mechanism" when the sensitive data is the very identity of the participant.

Anonymity and privacy mechanisms may be unconditional, in the sense that there are no circumstances under which the information could be revealed without the explicit cooperation of the participant. There are also conditional mechanisms. Some are conditional due to a limitation in the design methodology, e.g., a secret vote might be revealed if two out of three of the tallying servers collude. Some are conditional by design, so as to offer a balance between the needs of society and the individual. Key escrow mechanisms fall into this category, as do variants more closely related to e-commerce scenarios (e-cash escrow, identity escrow, etc.). Other relevant mechanisms include e-cash [Chaum82], group signature schemes [CvH91], anonymizing mixes and remailers [Chaum85], and zero-knowledge proof techniques [GMR85].

Perhaps the quintessential unconditional anonymity mechanism is "Chaumian e-cash" in all its variations. This is not the direction that most Internet payment schemes have taken, for a variety of reasons – technical, economic, political. Given the growing public concerns on privacy, it is possible that these kinds of mechanisms are worth a closer look. Of course, it is possible to borrow from the spirit of Chaum's pioneering work without requiring unconditional anonymity or unconditional privacy. Mentioned above are the so-called "escrow" mechanisms, where anonymity is completely preserved until completely revoked by an authority. By combining ideas from secure multi-party computation, the escrow authority can be converted into a distributed escrow service for which a quorum of authorities is needed. These kinds of balanced mechanisms are of great potential value. It is an important research problem to identify new kinds of balances which would have societal benefit, and for which efficient mechanisms can be constructed. For example, there might be partial escrow mechanisms with subtle layers or aspects of revocation requiring different trapdoor keys to expose.

I have become interested recently in "deniable payment mechanisms". This is a kind of "receipt-free" payment mechanism. The idea is to allow payments of any amount, but to do so in such a way that the payer can never prove that a payment was made. This is a new idea that first arose in a radical proposal for campaign finance reform [AB98], i.e., to disrupt the market for political influence by severing the connection between donor and donation. Note that this is not an anonymity mechanism, and in fact anonymity and deniability are orthogonal properties for a payment scheme. The proper modeling and design of cryptographically strong deniable payment schemes turns out to be a fascinating question that can be attacked using existing privacy mechanisms such as efficient zero-knowledge proofs. Some progress has been made (in joint work with Tomas Sander), but much remains to be discovered here.

There are new public key encryption schemes of Paillier and others with novel homomorphic properties [Pai99]. That is, some kinds of computations can be performed on encrypted data without decrypting the data, simply by performing arithmetic operations on the ciphertexts themselves. In the past, homomorphic encryption schemes have led to new designs for many anonymity and privacy mechanisms. It is likely that these new kinds of schemes, based on new trapdoors for discrete log, will turn out to be even more useful. It would be interesting to explore e-commerce applications of these

new encryption schemes. More abstractly, it might be possible to find a general classification of homomorphic cryptographic primitives, and find general theorems for reductions among such primitives, and general constructions for anonymity and privacy mechanisms built from them. In the past, this line of research made use of ideas and techniques from secure multi-party computation. I expect those connections to deepen.

It was stated earlier that the cryptographic approach could offer stronger privacy guarantees to consumers than an approach based only on laws and policies. While this is true, there is an intriguing research question that arises when considering the weaker kind of privacy guarantee. Is there a way to store sensitive data so that "legitimate" database queries can be efficiently performed, while unauthorized "data mining" queries are provably inefficient. For example, a collection of customer transaction records might be artificially expanded somehow into a massive dataset. If done cleverly, it might still be possible to perform lookups on individual transaction records without much of a loss of efficiency, say by probing some constant number of locations in the massive dataset. Then it might be possible to prove that a typical data mining operation, such as linking two or more records from the same customer, would provably require streaming through most or all of the massive dataset. Of course, this is far from an unconditional mechanism. One must still trust that the data is truly stored in this form, and not copied elsewhere in a more manageable form. One must also believe that streaming through a massive dataset is enough of a disincentive to protect the individual. But this is just one variation of a problem within a rich problem space, so it might prove to be relevant in other related guises. Given the plummeting costs of digital storage, this problem space seems ripe for exploration.

1. What new mechanisms for anonymity and privacy will help enable future e-commerce?
2. What new balances between protection for individuals and society can be found?
3. What are the new directions, applications and abstractions for homomorphic public key encryption schemes?
4. What are the new directions for databases that provably resist data mining?

3.3 Plan of Work for Fraud Detection and Prevention in E-Commerce

Much of the e-commerce currently being conducted over the Internet uses credit cards for purchases. This may be adequate for higher priced items, but the overhead involved in a single credit card purchase makes it completely inappropriate for small-valued purchases. One of the technical directions for small-valued purchases is to have purchases be less closely audited for authenticity. This immediately introduces the prospect of fraud, and raises the question of how much fraud a given system design can tolerate.

There is a growing awareness of the need for a more formal treatment of large-scale fraud. This is a topic that has been touched upon by some individual researchers, but no satisfactory treatment has emerged. To attack it properly may require a synthesis of ideas from diverse areas. Yacobi [Yac99] has developed a calculus of fraud analysis of a wide range of behavior for a population with partially audited payment devices. While

intriguing and ambitious, it may not be complete in its current form. Jarecki and Odlyzko [JO97] have a more complete treatment of a narrower fraud scenario involving partially audited payments. They analyze a randomized auditing strategy where the probability of checking up on a payment is roughly inversely proportional to the purchase price. The result is an attractive micropayment scheme.

Another direction for fraud prevention is the use of a lightweight "cost function". This was originally introduced by Dwork and Naor to discourage junk email (spam) [DN92]. Their idea was to introduce a function that was more difficult to compute than to verify, but without the kind of exponential gap in effort that is typically desired for strong signature or encryption schemes. Each piece of email needs to have a lightweight "stamp" for delivery to be accepted, which puts a sizable computational burden on the junk emailer.

As discussed in the section on Prior Research, I have applied lightweight cost functions to the problem of detecting and preventing fraud in the visit logs of web servers. There may be other applications of lightweight cost functions to e-commerce scenarios. There may also be intriguing connections between fraud resistance mechanisms and the ideas discussed in an earlier section about resistance to data mining through massive datasets.

The treatment of fraud becomes even more challenging for scenarios that allow different flavors of anonymity for participants. I expect there to be interesting connections between my study of fraud and my study of anonymity and privacy mechanisms.

The treatment of fraud may have interesting connections to my research on secure multi-party protocols, especially in light of new adversary models such as "malicious but rational" or "malicious but uncoordinated" or "malicious but undetectable". The kinds of misbehavior that are expected in fraud scenarios may fall into one or more of these categories.

More generally, it is intriguing to speculate on the possibility of a general theory of large-scale fraud detection and prevention. It is likely that ideas from cryptography would play a role, but other disciplines might be needed as well. Economics and statistics are obvious candidates. Large-scale dynamical systems and even biological systems may be useful, if only as metaphors and guiding examples. Other topics from computer science might be useful in a more direct sense. For example, there is a branch of algorithmic theory devoted to the competitive analysis of on-line algorithms. This theory seeks to bound the worst-case performance of an algorithm over time in the presence of a scheduling adversary that controls some of the inputs. The competitive analysis refers to a measure of performance as a ratio between actual results and ideal (omniscient) results. It may be possible to express a general class of fraud scenarios in this framework.

1. Can we reach a new understanding of fraud in e-commerce by considering new adversarial models for multiparty protocols?
2. How do ideas from anonymity and privacy mechanisms impact the analysis of fraud scenarios?

3. Can we find new uses for lightweight cost functions?
4. Can we move towards a general theory of large-scale fraud detection and prevention?

3.4 Plan of Work for Secure Content Distribution Mechanisms in E-Commerce

The World Wide Web is an excellent medium for delivering information and entertainment to consumers. Unfortunately it can also be a hostile environment for the protection of intellectual property. Whenever a digital work is rendered, its owners have the right to expect appropriate attribution and compensation. If unauthorized copying and modification cannot be prevented, then the full potential of modern digital delivery systems will never be met. The task of intellectual property management is especially difficult because significant technological, legal and culture obstacles stand in the way. A number of cryptographic techniques have already been developed for dealing with the technological aspects of the problem, including the following mechanisms for the secure distribution of digital content:

Watermarking, in which images (or documents, or software) are surreptitiously and unobtrusively altered to produce a common mark of ownership that could survive copying (or even modification), to help resolve ownership disputes.

Fingerprinting, which is similar to watermarking, except that each mark is different to help trace illegal copying back to its source.

Broadcast Encryption, in which digital goods can reach a large, targeted audience with privacy and authenticity and efficiency, to help in subscriber-based business models such as pay-per-view.

Traitor Tracing, in which cryptographic keys are given unique fingerprints to help trace illegal cloning of decryption devices (piracy) [CFN94]. The idea is to encrypt data so that there are many decryption keys that are functionally equivalent but structurally distinct. The motivating application is for broadcasting encrypted content to subscribers. Each legitimate subscriber would have a set-top box with a unique decryption key in it. If a subscriber became a "traitor" and sold clones of his set-top box, then her identity could be traced by examining the decryption key in any clone.

I believe that the connections between anonymity and privacy mechanisms and secure content distribution mechanisms have not been adequately explored. The work of Pfitzmann and others on anonymous fingerprinting schemes is an example of this kind of connection (e.g., [PS99]. Another example is very recent work by Glenn Durfee and me on the application of zero-knowledge proof techniques to a new security problem that will arise in future business-to-business e-commerce scenarios [DF2000]. I will now describe this work in a little more detail.

When distributing digital content, commercial solutions often begin with the notion of a "digital contract" attached to a "self-protecting document". The idea is that the digital

contract expresses the terms and conditions under which a document may be viewed (or printed, or otherwise rendered), and the self-protection elements help to enforce the contract. Many attacks on such systems focus on weaknesses of the self-protecting document, showing how contracts can be modified or severed from the content. We stipulate that self-protecting documents are possible, and focus on a different security issue: How will contracts for digital content get negotiated between middlemen in a distribution chain?

These middlemen may be re-packaging or enhancing a single digital work, or bundling together several digital works. There is a natural privacy requirement at work here, because a businessman negotiating with a buyer will not always want to expose the deals that he has already made with his suppliers. If all of these earlier negotiated terms are revealed, then the businessman is at a disadvantage in the new negotiations. Worse, if even the identities of suppliers are revealed, the businessman might find that he has been "disintermediated" by his buyer, i.e., cut out of the chain altogether. There is also a natural integrity requirement in these distribution chain scenarios. Terms that are negotiated into new contracts must remain faithful to restrictions and obligations of earlier contracts. For example, expiration dates on a digital work should not get moved ahead, and relevant payments and royalties should be honored.

Very efficient zero-knowledge proof techniques can be used to prove that a certain "fair contract relation" always holds. This approach balances the privacy and integrity requirements of distribution chain security. For efficiency, when the distribution chains are long, we use neutral entities called "contract certifiers" that can verify these zero-knowledge proofs without learning any sensitive terms of the contracts themselves. This is the first step in a research program that will find other applications of anonymity and privacy mechanisms to secure e-commerce scenarios.

The area of secure content distribution is a tricky one to navigate, because some of the claims are difficult to verify. For example, there have been a lot of claims (and a number of commercial products) for digital watermarking that can resist the attempts of a malicious party that is attempting to remove it. However, there is no credible scheme in the literature for which such a claim can be demonstrated. The status of so-called self-protecting documents is similarly unresolved. If we are to arrive at a science of secure content distribution, we must separate out what is truly achievable from what is merely fanciful. This is made more difficult by the fact that a lot of potentially good ideas may be hidden in the form of proprietary data and patent submissions.

Another complicating factor is that it may be difficult to specify the actual goals of the participants in a secure content distribution scenario. For example, a content publisher may sometimes want to tolerate or encourage small-scale piracy (beyond the "fair use" bounds), for reasons of publicity or goodwill. At the same time, a publisher might want to maintain the ability to crack down on piracy large or small, to set an example or thwart a serious threat. This suggests a deeper connection between secure content distribution and fraud detection and prevention.

1. What new mechanisms for secure content distribution will help enable future e-commerce?
2. What new synergies can be found by bringing anonymity and privacy mechanisms to content distribution scenarios?
3. What is the foundation of the science of secure content distribution?

4. Relation to Career Goals and Job Responsibilities

As a Computer Science professor at U. C. Davis, I will be responsible for developing curricula for undergraduate courses and graduate seminars. I will teach courses that are based on ideas from e-commerce security. I believe that these courses would be quite popular with a wide variety of students at Davis. Teaching them would be rewarding for at least two reasons. I have always found it satisfying to teach courses that had practical impact as well as intrinsic interest. I have also found that developing and teaching courses, even at a basic level, has stimulated my research in exciting new directions.

The research symposia are not part of my job responsibilities in the narrowest sense. Nevertheless, these activities fit in well with my professional goals. I want to emerge as a leader in this new field of e-commerce security, so that I can help it grow and develop in a scientifically meaningful manner. I have had some experience in this direction already. I have already organized one symposium on e-commerce security (more specifically, on mathematical aspects of intellectual property management on the Internet), to be held this coming February at the AAAS Annual Meeting in San Francisco. I have also helped to launch and expand a series of conferences in Financial Cryptography, serving as Program Committee member, Co-Chair, and Chair. This has been a successful series of meetings among scientists, academics, bankers, lawyers, and privacy advocates.

It is also important for my professional goals to have a strong research program on a topic that is important and exciting. The cryptographic aspects of e-commerce security that I have described in this proposal are a good fit with that goal. Thus this proposed plan of work is closely related to my goals and responsibilities. However, there is something about this five-year plan that strengthens all of these activities through a conceptual integration. By pursuing this plan, I will have the chance to ally my personal career goals and job responsibilities in the service of the greater goal of forwarding a science of e-commerce security.

5. Summary of Prior Research and Education

I received a B.A. in Mathematics from Pomona College in May 1983, and an M.A. in Mathematics from U. C. Berkeley in May 1985. After four years in industry, I returned to Columbia University, where I received a Ph.D. in Computer Science in February 1994. My Ph.D. thesis was on the “Efficiency and security of distributed protocols”.

I will summarize my research contributions to secure e-commerce in the four main technical areas that I have already discussed: secure multi-party protocols, privacy and anonymity mechanisms, fraud detection and prevention, content distribution mechanisms:

5.1 My Prior Research in Secure Multi-Party Protocols in E-Commerce

Sealed Bid Auctions: My work with Mike Reiter introduced the area of auctions to the security community [FR96]. We modeled the problem of conducting a secure sealed-bid auction as a distributed multi-party protocol among bidding agents and auctioneer agents. Our security model included threats against the bidders, such as disclosing bids improperly, misplacing bids, declaring the wrong winner, and so forth. We also addressed threats against the auction house, in particular the threat that the winning bidder would default and refuse to pay. Our solution defended against all of these threats with a novel blend of known and new cryptographic techniques. To solve the winning bidder default problem, we devised a scheme for the distributed escrow of digital cash, so that every valid bid had to "show the money up front". To demonstrate the practicality of this approach, we prototyped the system and took precise timing measurements. This work was begun in the Fall 1994, and first presented in May 1995 (at the IEEE Oakland Security Conference), well before auctioning on the Internet was established.

Threshold CA: Mike Reiter, Jack Lacy and Rebecca Wright and I gave the first implementation of a distributed certification authority and escrow service [RFLW96]. We combined ideas from threshold cryptography in particular and secure multi-party protocols in general to achieve a design with strong security guarantees. User keys were escrowed as threshold shares among separate servers. Users had the option of recovering their key directly, or having the escrow service use the keys on their behalf on a per-signature or per-decryption basis. Once a user had escrowed a key with the service, the service would issue a public key certificate to the user. This also used threshold cryptography, to protect the highly sensitive root signing key. The design was highly tuned for maximum efficiency while resisting coordinated malicious attacks by users or certification servers. The public key for the Omega certification service was installed and widely deployed in the first commercially available browser to support outside keys (Netscape 1.2).

Distributed RSA Generation: Dan Boneh and I showed how three or more parties could efficiently generate a shared RSA key without trusting each other [BF97]. This solved an open problem that goes back to Yao 1986 [Yao86]. Prior to our work, any system that relied on threshold sharing to protect sensitive RSA keys (such as a distributed certification authority) had to rely on a trusted dealer to initialize the system. Our protocol for shared RSA key generation gives an alternative approach for handling highly sensitive RSA keys, so that throughout their lifetime there is no single point of vulnerability to attack. Timing experiments have demonstrated the practicality of this approach: A 1024-bit RSA can be generated in less than 91 seconds by three Sun workstations across a local area network [MWB99].

Fair Exchange: Together with Mike Reiter, I introduced a new approach to the problem of fair exchange between two mutually suspicious parties [FR97]. We devised the use of a third party that was "semi-trusted", in the sense that it might misbehave on its own but would never collude with either of the two main parties. This enabled us to find extremely efficient and secure three-party protocols for fair exchange, which had previously required either a very costly two-party protocol, or a three-party protocol with weaker security guarantees. This work was a steppingstone for the security community to the powerful notion of "optimistic" fair exchange, where the third party is only needed to resolve disputes. The recent work on fair exchange is an example of new adversary models leading to breakthroughs in efficiency for an important security task.

Secret Ballot Election: Ronald Cramer, Berry Schoenmakers, and Moti Yung and I presented new secure multi-party protocols for conducting a large-scale secret ballot election [CFSY96]. This is a difficult problem, because it blends privacy concerns for the voter (to keep his vote secret), with reliability concerns for everyone (to ensure that the tally is accurate). Our approach was a significant improvement over the most efficient election protocols known at that time. The scheme was implemented independently at several universities and research labs. Although later schemes have improved on our results, they continue to incorporate key features of our design.

Conspiracy Start-Up: My work with Harry Buhrman et al. investigated one aspect of the "malicious-but-uncoordinated" adversary setting for secure multi-party protocols [BFG99+]. Specifically, we considered the "conspiracy start-up" problem that arises when malicious but uncoordinated faults attempt to find one another surreptitiously.

5.2 My Prior Research in Anonymity and Privacy Mechanisms in E-Commerce

Offline E-Cash: Moti Yung and I developed new directions for efficient "off-line" Chaumian e-cash [FY93]. A digital coin scheme is off-line if only the customer and the vendor need to participate in the purchase protocol, but not the bank or any other parties. The concept and first constructions were due to Fiat, Chaum, and Naor [FCN88]. One drawback of these early constructions was that the purchase protocol required a costly cut-and-choose step, and the size of the coin was proportional to the cut-and-choose security parameter. Our work showed how to streamline the construction with a "single-term" coin and a simplified purchase protocol. We also gave the first formal definitions for electronic cash, which was cited as a foundational contribution by Goldreich [Gol98].

Anonymous Authentication: Dan Boneh and I suggested a new approach to anonymous authentication and group signature schemes [BF99b]. This is a mechanism for proving membership in a group without revealing which group member it is. The exact identity of the group member can only be revealed with the use of a secret trapdoor key (e.g., known to law enforcement). This mechanism has been called "identity escrow" to emphasize its close relation to key escrow. This is a good example of an anonymity mechanism that blends some protection for the individual with some protection for society.

Recommendation Systems: My work with Bernardo Huberman and Tad Hogg showed how existing anonymity and privacy mechanisms could be applied to enhance the power of online recommendation systems [HFH99]. Individuals are often reluctant to reveal their true preferences for a variety of reasons, e.g., fear of liability, litigation, embarrassment, or reprisal. Cryptographic techniques such as deniable signatures and secure function evaluation can help individuals overcome their reluctance. One new scheme for "community discovery" adapted the cryptographic primitive of non-interactive oblivious transfer to let individuals efficiently distribute secret keys according to the results of a survey. Some of these ideas were prototyped at Xerox PARC for inclusion in a "shared bookmarks" platform for web browsing.

5.3 My Prior Research in Fraud Detection and Prevention

Auditable Metering: Dahlia Malkhi and I worked on the problem of fraud prevention for web sites [FM98]. We started with the observation that visit logs for web sites were stored insecurely at the web sites themselves. Since advertisers were beginning to pay fees based on the number of hits, there seemed to be a great incentive for web sites to tamper with the visit logs. We devised a solution that did not require any change in the existing infrastructure, and in particular used no cryptographic keys at all. Our approach was to discourage large-scale fraud without preventing abuse on a smaller scale, a type of security that had already been introduced for combating junk mail and for micropayment schemes. A simple java applet downloaded to the user's machine when she visited a web site, and returned the result of a special computation when she clicked away. The duration of visits could be estimated accurately from these results, and forgery in large quantities required massive computational resources. We prototyped our scheme to demonstrate its effectiveness.

5.4 My Prior Research in Content Distribution Mechanisms in E-Commerce

Traitor Tracing: Previous approaches to traitor tracing were combinatorial and symmetric key, i.e., a number of simple symmetric key encryption schemes were combined and each user was given a particular subset of the keys. In recent work with Dan Boneh [BF99a], I helped develop a new approach that was algebraic and public key. That is, we devised a new public key scheme with one encryption key and many decryption keys, based on the hardness of the Decision Diffie-Hellman problem (a well-known hardness assumption related to the discrete log problem). By assigning decryption keys to users according to an underlying Reed-Solomon error correcting code, the ability to trace a traitor is guaranteed. Even if many traitors collude, tracing is guaranteed as long as the number of traitors is below a threshold design parameter.

Distribution Chain Security: Glenn Durfee and I introduced the problem of distribution chain security [DF2000] that was described in some detail in the Outline of Plan of Work. This is an application of very efficient zero-knowledge proof techniques to a new security problem that will arise in business-to-business content distribution scenarios. We have prototyped these ideas to demonstrate their efficiency.

New Directions in Cryptography for Electronic Commerce
M. Franklin

References Cited

[AB98] I. Ayres and J. Bulow, "The donation booth: Mandating donor anonymity to disrupt the market for political influence", *Stanford Law Review* 50 (1998).

[BGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic falut-tolerant distributed computation", *Proc. ACM Symposium on Theory of Computing* (STOC), 1988, 1—9.

[BF97] D. Boneh and M. Franklin, "Efficient generation of shared RSA keys", *Proc. Advances in Cryptology -- Crypto '97*, 1997, 425—439.

[BF99a] D. Boneh and M. Franklin, "An efficient public key traitor tracing scheme", *Proc. Advances in Cryptology -- Crypto '99*, 1999, 338—353.

[BF99b] D. Boneh and M. Franklin, "Anonymous authentication with subset queries", *Proc. ACM Conference on Computer and Communications Security*, 1999, 113—119.

[BFG+99] H. Buhrman, M. Franklin, J. Garay, J. Hoepman, J. Tromp, and P. Vitanyi, "Mutual Search", Journal of the ACM 46(1999), 517—536.

[CCKM2000] C. Cachin, J. Camenisch, J. Kilian, and J. Müller, "One-round secure computation and secure autonomous mobile agents", *Proc. 27th International Colloquium on Automata, Languages and Programming (ICALP), Geneva*, July 2000.

[CO99] R. Canetti and R. Ostrovsky, "Secure computation with honest-looking parties: what if nobody is truly honest?", *Proc. ACM Symposium Theory of Computing* (STOC), 1999, 255—264.

[Cha82] D. Chaum, "Blind signature for untraceable payments", *Proc. Advances in Cryptology -- Crypto '82*, 1982, Springer-Verlag, 199—203.

[Cha85] D. Chaum, "Security without identification: transaction systems to make big brother obsolete", *Communications of the ACM* 28 (1985), 1030—1044.

[CCD88] D. Chaum, C. Crepeau, and I. Damgard, "Multiparty unconditionally secure protocols, *Proc. ACM Symposium on Theory of Computing* (STOC), 1988, 11—19.

[CFN88] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash", *Proc. Advances in Cryptology -- Crypto '88*, 1988, Springer-Verlag, 319—327.

[CFN94] B. Chor, A. Fiat, and M. Naor, "Tracing traitors", *Proc. Advances in Cryptology -- Crypto '94*, 1994, Springer-Verlag, 257—270.

[CvH91] D. Chaum and E. van Heyst, "Group signatures", *Proc. Advances in Cryptology -- Eurocrypt '91*, 1991, Springer-Verlag, 257—265.

[CFSY96] . R. Cramer, M. Franklin, B. Schoenmakers, M. Yung, "Multi-authority secret ballot elections with linear work", *Proc. Advances in Cryptology -- Eurocrypt '96*, 1996, 72—83.

[Des94] Y. Desmedt, "Threshold cryptography", European Transactions on Telecommunications 5 (1994), 449—457.

[DF2000] G. Durfee and M. Franklin, "Distribution chain security", *Proc. ACM Conference on Computer and Communication Security, 2000* (to appear). Earlier version presented at DIMACS Workshop on Protection of Intellectual Property, Rutgers University, April 2000.

[DN92] C. Dwork and M. Naor, "Pricing via processing or combating junk mail", *Proc. Advances in Cryptology -- Crypto '92*, 1992, Springer-Verlag, 139—147.

[FKN94] U. Feige, J. Kilian and M. Naor, "A minimal model for secure computation", Proc. ACM Symposium on Theory of Computing, 1994, 554—563.

[FM98] M. Franklin and D. Malkhi, "Auditable metering with lightweight security", *Journal of Computer Security* 6(4), 1998.

[FR96] M. Franklin and M. Reiter, "The design and implementation of a secure auction service", *IEEE Transactions on Software Engineering*, 22(5):302--312, 1996.

[FR97] M. Franklin and M. Reiter, "Fair exchange with a semi-trusted third party", *Proc. ACM Conference on Computer and Communications Security*, 1997, 1—7.

[FY93] M. Franklin and M. Yung, "Secure and efficient off-line digital money", *Proc. 20th International Colloquium on Automata, Languages and Programming* (ICALP), 1993, 265—276.

[Gol99] O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, Springer-Verlag, 1999.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game", *Proc. ACM Symposium on Theory of Computing* (STOC), 1987, 218—229.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems, *SIAM Journal on Computing* 18 (1989), 186—208.

[HFH99] B. Huberman, M. Franklin, and T. Hogg, "Enhancing privacy and trust in electronic communities," *Proc. ACM Conference in Electronic Commerce*, 1999, 78—86.

[JO97] S. Jarecki and A. Odlyzko, "An efficient micropayment system based on probabilistic polling", *Proc. Financial Cryptography*, 1997, Springer-Verlag, 173—192.

[MWB99] M. Malkin, T. Wu, and D. Boneh, "Experimenting with shared generation of RSA keys", *Proc. Internet Society's Symposium on Network and Distributed System Security* (NDSS), 1999, 43—56.

[MT99] D. Monderer and M. Tennenholtz, "Distributed games: from mechanisms to protocols", *Proc. 16th Natl. Conf. Artificial Intelligence*, 1999, The MIT Press, 32—37.

[Nis99] N. Nisan, "Algorithmic mechanism design", *Proc. ACM Symposium on Theory of Computing* (STOC '99), 1999, 129—140.

[Pai99] P. Paillier, "Public-key cryptosystems based on composite degree residue classes", *Proc. Advances in Cryptology – Eurocrypt '99*, 1999, 223—238.

[PS99] B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting", *Proc. Advances in Cryptology -- Eurocrypt '99*, 1999, Springer-Verlag, 150—164.

[RFWL96] ,M. Reiter, M. Franklin, R. Wright, and J. Lacy, "Key management in the Omega system", *Journal of Computer Security* 4(4):267--287, 1996.

[ST98] T. Sander and C. Tschudin, "On software protection via function hiding", *Proc. 2nd Workshop on Information Hiding*, Springer-Verlag, 1998, 113—125.

[Yac99] Y. Yacobi, "Risk management for e-cash systems with partial real-time audit", *Proc. Financial Cryptography*, 1999, Springer-Verlag, 62—71.

New Directions in Cryptography for Electronic Commerce
M. Franklin

Biographical Sketch of Principal Investigator

EDUCATION

Feb 1994 Ph.D. in Computer Science, Columbia University, New York, NY.
Thesis Advisors: Zvi Galil, Moti Yung.
Thesis Title: "Efficiency and Security of Distributed Protocols".

May 1985 M.A. in Mathematics, University of California, Berkeley, CA.

May 1983 B.A. in Mathematics, Pomona College, Claremont, CA.

PROFESSIONAL EXPERIENCE

August 1998 - present Xerox PARC, Palo Alto, CA.
Member of Research Staff, Secure Document Systems Group.

July 1994 - July 1998 AT&T Research, Florham Park, NJ.
(formerly AT&T Bell Labs, Murray Hill, NJ.)
Principal Technical Staff Member, Secure Systems Research Department.

1987-1989 Thomson-CSF, Inc., Palo Alto, CA.

1985-1987 Lockheed Software Technology Center, Palo Alto, CA.

VISITS AND INTERNSHIPS

Jan-June 1994: Center for Mathematics and Computer Science (C.W.I.), Amsterdam.

Summer 1993: IBM Research Division, T.J. Watson Center, Yorktown, NY.

Summer 1992: Bellcore, Morristown, NJ.

Summer 1991: AT&T Bell Laboratories, Murray Hill, NJ.

PROFESSIONAL HONORS AND ASSOCIATIONS

Editorial Board, Journal of Cryptology (starting January 2001).

Board of Directors, International Association for Cryptologic Research, 1999-2000.

AT&T Bell Laboratories Ph.D. Scholar, 1990-94.

TEACHING EXPERIENCE

Stanford, Fall 1999: Freshman Seminar on Computer Security (with D. Boneh).

Columbia, Spring 1998: Graduate Crypto Seminar (with M. Yung, S. Haber).

NYU, Spring 1997: Design and Analysis of Crypto Protocols (with A. Rubin).

NYU, Fall 1996: Design and Analysis of Crypto Protocols (with A. Rubin).

Columbia, Fall 1995: Graduate Crypto Seminar (with M. Yung, S. Haber).

CONFERENCE ACTIVITIES

Eurocrypt: Program Committee (2001)
Crypto: General Chair (2000), Program Committee (1998)
Financial Crypto: Program Committee (2001, 1997), Co-Chair (1998), Chair (1999)
ACM Security: Program Committee (1999,1996), Tutorials (2001), Publication (1999)
Computer Security Foundations Workshop: Program Committee (2000)

PUBLICATIONS

Proceedings

M. Franklin (editor), *Proc. Financial Cryptography '99*, Springer-Verlag, Lecture Notes in Computer Science, vol. 1648, 1999.

Patents

U.S. Patent #6055518, "Secure auction systems", April 25, 2000.

Refereed Journal Publications

M. Franklin, M. Yung, "Privacy from partial broadcast," *SIAM J. Discrete Math*, in review.

D. Boneh and M. Franklin, "Efficient generation of shared RSA keys," *Journal of the ACM*, accepted with minor revisions.

M. Franklin, Z. Galil, M. Yung, "Eavesdropping games," *Journal of the ACM* 47(2000):225—243.

H. Buhrman, M. Franklin, J. Garay, J. Hoepman, J. Tromp, P. Vitanyi, "Mutual search," *Journal of the ACM*, 46(4):517--536, 1999.

M. Franklin and R. Wright, "Secure communication in minimal connectivity models," *Journal of Cryptology*, 13(1):9--30, 2000. (Special Issue on General Secure Multiparty Computation).

A. Beimel and M. Franklin, "Reliable communication over partially authenticated networks," *Theoretical Computer Science*, 220(1)185--210, 1999, Special Issue on Distributed Algorithms.

M. Franklin and D. Malkhi, "Auditable metering with lightweight security," *Journal of Computer Security* 6(4), 1998.

M. Reiter, M. Franklin, R. Wright, and J. Lacy, "Key management in the Omega system," *Journal of Computer Security* 4(4):267--287, 1996.

M. Franklin, M. Reiter, "The design and implementation of a secure auction service," *IEEE Transactions on Software Engineering*, 22(5):302--312, 1996.

M. Franklin, S. Haber, "Joint encryption and message-efficient secure computation," *Journal of Cryptology* 9(4):217--232, 1996.

A. Gabrielian, M. Franklin, "Multi-level specification and verification of real-time software," *Communications of the ACM* 34(5):50--60, 1991. Invited from earlier version in *Proc. 12th International Conference on Software Engineering*, Nice, France, 1990.

Refereed Conference Publications

Omitted twenty-four references due to space limitations.

SUMMARY PROPOSAL BUDGET

YEAR 1

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION
University of California-Davis

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Matthew Franklin

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Matthew Franklin - Acting Associate Professor**	**0.00**	**0.00**	**1.00**	$ **8,715**	$
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**1.00**	**8,715**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**1**) GRADUATE STUDENTS				**11,075**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**1**) OTHER				**1,785**	
TOTAL SALARIES AND WAGES (A + B)				**21,575**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**1,715**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**23,290**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.) **See Budget Justification** $ **2,000**					
TOTAL EQUIPMENT				**2,000**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**2,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**1,300**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**4,965**	
TOTAL OTHER DIRECT COSTS				**6,765**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**34,055**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **MTDC (Rate: 48.0000, Base: 27090)**					
TOTAL INDIRECT COSTS (F&A)				**13,003**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**47,058**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.D.7.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **47,058**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI / PD TYPED NAME & SIGNATURE*	DATE	FOR NSF USE ONLY
Matthew Franklin		INDIRECT COST RATE VERIFICATION
ORG. REP. TYPED NAME & SIGNATURE*	DATE	Date Checked / Date Of Rate Sheet / Initials - ORG

SUMMARY PROPOSAL BUDGET YEAR 2

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION: **University of California-Davis**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **Matthew Franklin**

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Matthew Franklin - Acting Associate Professor**	**0.00**	**0.00**	**1.00**	$ **9,608**	$
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**1.00**	**9,608**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**1**) GRADUATE STUDENTS				**11,629**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**1**) OTHER				**1,874**	
TOTAL SALARIES AND WAGES (A + B)				**23,111**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**1,853**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**24,964**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.) **See Budget Justification** $ **2,000**					
TOTAL EQUIPMENT				**2,000**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**2,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**1,300**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**5,213**	
TOTAL OTHER DIRECT COSTS				**7,013**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**35,977**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **MTDC (Rate: 48.5000, Base: 28764)**					
TOTAL INDIRECT COSTS (F&A)				**13,950**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**49,927**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.D.7.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **49,927**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI / PD TYPED NAME & SIGNATURE*	DATE	FOR NSF USE ONLY
Matthew Franklin		INDIRECT COST RATE VERIFICATION
ORG. REP. TYPED NAME & SIGNATURE*	DATE	Date Checked / Date Of Rate Sheet / Initials - ORG

SUMMARY PROPOSAL BUDGET YEAR 3

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION: **University of California-Davis**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **Matthew Franklin**

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Matthew Franklin - Acting Associate Professor**	**0.00**	**0.00**	**1.00**	$ **10,089**	$
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**1.00**	**10,089**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**1**) GRADUATE STUDENTS				**12,211**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**1**) OTHER				**1,968**	
TOTAL SALARIES AND WAGES (A + B)				**24,268**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**1,955**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**26,223**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.) **See Budget Justification** $ **2,000**					
TOTAL EQUIPMENT				**2,000**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**2,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**1,300**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**5,474**	
TOTAL OTHER DIRECT COSTS				**7,274**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**37,497**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **MTDC (Rate: 48.5000, Base: 30023)**					
TOTAL INDIRECT COSTS (F&A)				**14,561**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**52,058**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.D.7.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **52,058**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI / PD TYPED NAME & SIGNATURE*	DATE	FOR NSF USE ONLY
Matthew Franklin		INDIRECT COST RATE VERIFICATION
ORG. REP. TYPED NAME & SIGNATURE*	DATE	Date Checked / Date Of Rate Sheet / Initials - ORG

SUMMARY PROPOSAL BUDGET

YEAR 4

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION
University of California-Davis

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Matthew Franklin

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Matthew Franklin - Acting Associate Professor**	**0.00**	**0.00**	**1.00**	$ **10,593**	$
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**1.00**	**10,593**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**1**) GRADUATE STUDENTS				**12,821**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**1**) OTHER				**2,066**	
TOTAL SALARIES AND WAGES (A + B)				**25,480**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**2,053**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**27,533**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.) **See Budget Justification** $ **2,000**					
TOTAL EQUIPMENT				**2,000**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**2,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**1,300**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**5,748**	
TOTAL OTHER DIRECT COSTS				**7,548**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**39,081**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **MTDC (Rate: 48.5000, Base: 31333)**					
TOTAL INDIRECT COSTS (F&A)				**15,196**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**54,277**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.D.7.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **54,277**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI / PD TYPED NAME & SIGNATURE*	DATE	FOR NSF USE ONLY
Matthew Franklin		INDIRECT COST RATE VERIFICATION
ORG. REP. TYPED NAME & SIGNATURE*	DATE	Date Checked / Date Of Rate Sheet / Initials - ORG

SUMMARY PROPOSAL BUDGET

YEAR 5

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION
University of California-Davis

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Matthew Franklin

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Matthew Franklin - Acting Associate Professor**	**0.00**	**0.00**	**1.00**	$ **11,123**	$
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**1.00**	**11,123**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**1**) GRADUATE STUDENTS				**13,462**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**1**) OTHER				**2,170**	
TOTAL SALARIES AND WAGES (A + B)				**26,755**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**2,155**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**28,910**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.) **See Budget Justification** **$ 2,000**					
TOTAL EQUIPMENT				**2,000**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**2,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**0**	
4. COMPUTER SERVICES				**1,300**	
5. SUBAWARDS				**0**	
6. OTHER				**6,035**	
TOTAL OTHER DIRECT COSTS				**7,835**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**40,745**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **MTDC (Rate: 48.5000, Base: 32710)**					
TOTAL INDIRECT COSTS (F&A)				**15,864**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**56,609**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.D.7.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **56,609**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI / PD TYPED NAME & SIGNATURE*	DATE	FOR NSF USE ONLY
Matthew Franklin		INDIRECT COST RATE VERIFICATION
ORG. REP. TYPED NAME & SIGNATURE*	DATE	Date Checked / Date Of Rate Sheet / Initials - ORG

SUMMARY PROPOSAL BUDGET

Cumulative

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION: **University of California-Davis**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **Matthew Franklin**

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Matthew Franklin - Acting Associate Professor**	**0.00**	**0.00**	**5.00**	$ **50,128**	$
2.					
3.					
4.					
5.					
6. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**5.00**	**50,128**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**5**) GRADUATE STUDENTS				**61,198**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**5**) OTHER				**9,863**	
TOTAL SALARIES AND WAGES (A + B)				**121,189**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**9,731**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**130,920**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.) $ **10,000**					
TOTAL EQUIPMENT				**10,000**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**10,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**2,500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**5,200**	
4. COMPUTER SERVICES				**1,300**	
5. SUBAWARDS				**0**	
6. OTHER				**27,435**	
TOTAL OTHER DIRECT COSTS				**36,435**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**187,355**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE)					
TOTAL INDIRECT COSTS (F&A)				**72,575**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**259,930**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.D.7.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **259,930**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI / PD TYPED NAME & SIGNATURE*: **Matthew Franklin** DATE

ORG. REP. TYPED NAME & SIGNATURE* DATE

FOR NSF USE ONLY

INDIRECT COST RATE VERIFICATION

Date Checked	Date Of Rate Sheet	Initials - ORG

NSF Form 1030 (10/99) Supersedes all previous editions

C***SIGNATURES REQUIRED ONLY FOR REVISED BUDGET (GPG III.B)**

New Directions in Cryptography for Electronic Commerce
M. Franklin

Current and Pending Support

1. DARPA Grant #N66001-00-1-8921
   "Secure Group Communications for Large Dynamic Coalitions"
   Principal Investigator: Matt Franklin
   Issuing Office: Space and Naval Warfare Systems Center, San Diego
   Funding Amount from DARPA: $807,467.00
   Matching Amount from Xerox: $807,467.00
   Grant Term: April 19, 2000 – April 18, 2002

Note: I do not plan to continue as P.I. on this grant after September 2000. I am currently discussing the possibility of continuing in some other capacity, e.g., as a consultant or sub-contractor.

FACILITIES, EQUIPMENT & OTHER RESOURCES

FACILITIES: Identify the facilities to be used at each performance site listed and, as appropriate, indicate their capacities, pertinent capabilities, relative proximity, and extent of availability to the project. Use "Other" to describe the facilities at any other performance sites listed and at sites for field studies. USE additional pages as necessary.

Laboratory: **There is ample space available for this proposed project. No special facilities, other than computer workstations, are necessary. The Department will provide Dr. Franklin with a faculty office, as well as research space for his students in the Computer Science Theory Lab (Room 2235, Engineering II) or the Computer Science Security**

Clinical:

Animal:

Computer:

Office:

Other: _____

MAJOR EQUIPMENT: List the most important items available for this project and, as appropriate identifying the location and pertinent capabilities of each.

OTHER RESOURCES: Provide any information describing the other resources available for the project. Identify support services such as consultant, secretarial, machine shop, and electronics shop, and the extent to which they will be available for the project. Include an explanation of any consortium/contractual arrangements with other organizations.

Continuation Page:

LABORATORY FACILITIES (continued):

Research Lab (Rooms 2244 and 2245, EII). Existing workstations in those labs are available for the project, in addition to workstations that will be bought with Dr. Franklin's new faculty start-up funds.

UNIVERSITY OF CALIFORNIA, DAVIS

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

COLLEGE OF ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE
(530) 752-7004
FAX: (530) 752-4767

ONE SHIELDS AVENUE
DAVIS, CALIFORNIA 95616-8562

gusfield@cs.ucdavis.edu
(530) 754-8016

I am delighted to write a supporting letter for Professor Matthew K. Franklin. Professor Franklin has an exceptional record in cryptography, computer security and efficient computer algorithms. Professor Franklin received his Ph.D. in Computer Science from Columbia University in February 1994 and has been working in industrial research labs since then (A.T.T. Research Labs and Xerox PARC.) He comes to us from the Secure Documents Systems Group at Xerox Palo Alto Research Center (PARC). His work has paid particular attention to security issues in electronic commerce, blending theory and practice. His background in cryptography, combined with his industrial experience in security, make him uniquely talented to address many of the most difficult and nationally important issues of secure computing, e-commerce and secure computing/communication infrastructure. Security is one of the major growth areas in computer science, and central in our academic plan, written in 1998. The security group at UC Davis is already strong and nationally recognized. Professor Franklin's Career Development Plan fits perfectly with the overall educational and research plans of the department and the university.

Professor Franklin has been very active professionally. One of his most prestigious activities is serving as General Chair of this year's CRYPTO conference, which is the most important conference in his field. Last year, Professor Franklin served as the Program Chair of the Financial Crypto conference, another important distinction. In addition to his superb research and professional record, Professor Franklin has taught or co-taught five courses at Stanford University, Columbia University and New York University. We are quite impressed by Professor Franklin's activities in teaching, while a member of industrial research labs.

Because of Professor Franklin's accomplishments and potential, the Department of Computer Science and the College of Engineering are committed to helping him further his successful research program, and to develop his teaching program at Davis. In addition to paying his full academic year salary, he has been given a generous startup package. This consists of $40,000 of equipment funds; $25,000 in equipment matching funds; $6,000 in travel and moving expenses; support for one graduate student for one year under a GAANN fellowship; support for one graduate student for one year of non-resident tuition fellowship; a reduction of one course for the 2000-01 academic year.

Overall, we are excited about having Professor Franklin as a member of our faculty. His proposed research has the potential to achieve significant advances in cryptography and secure e-commerce.

The applicant received his Ph.D. in February, 1994. The official effective date of the applicant's first tenure-track appointment was July 1, 2000. The applicant does not hold tenure at University of California, Davis. I have read and I endorse this Career Development Plan.

Dan Gusfield
Professor and Chair
Department of Computer Science
University of California, Davis
July 17, 2000