

Kryptologie und Computer in der Arbeit der NSA / USA

Dieser Artikel wurde aus alten Pdf – Dateien übersetzt, die Verstümmelungen des Textes bitten wir zu entschuldigen.

Die Originalseiten dieser Information finden Sie unter : [2006 Schlüsselrolle der NSA bei wichtigen Entwicklungen in der Informatik \(Teile 1 & 2\)](#)

(U) **NSA**s Schlüsselrolle in größeren Entwicklungen in Computer Science Teil eins

(U) Kryptologie hat historisch eine intensive Bewerbung der Arbeit mit sich gebracht. Aber seit der Mitte des letzten Jahrhunderts ist Automatisierung als Art verwendet worden, die Herstellung und den Bruch von Codes sehr zu mildern. Die Formung und Reifung von der Staatssicherheitsagentur (**NSA**) und der Evolution ihrer Aufträge glichen in Großteil dem Aufkommen des Computerzeitalters. *Ein* Folge, das **NSA** und *seine* Vorgängeragenturen sind historisch *an der ersten Stelle* von Computerentwicklung in den *Vereinigten Staaten gewesen*.

{U), aber die Verwendung von Computermaschinen in amerikanischer Kryptologie ging der offiziellen Geburt **ofNSA** lang voraus. Während Weltkriegs integrierte ich, das Militär Verwendung der Verschlüsselungsausrüstung. Während der 1930er erwarben sowohl die Armee als auch marineblaue **cryptologic** Bestandteile Geräte von International Business Machines { IBM), welches ermöglichte, dass sie große Datenmengen sortierten. Zur Zeit, als der zweite Weltkrieg ausgebrochen war, besaßen alle größeren Kombattanten hoch entwickelte Ziffernmaschinen für meiste ihrer Datenübertragungserzeugung und Sicherheitsprogramme.

{U) As der Krieg schritt voran, die US-Wehrdienste stellten viele elektronische Buchungsmaschinen auf das Feld, um einen breiten Bereich von feindlichen Signalen zu verarbeiten. Die Dienste entwickelten Beziehungen zu Industrie - Bell Laboratories and Teletype Corporation im Falle von der Armee, und IBM, Eastman Kodak und nationale Registrierkasse (NCR) im Falle von der Marine. Ein Paradebeispiel von den Nutzen von solchen Beziehungen war der Bau vom **cryptanalytic** der Marine "**Bombe**" (*die erste Maschine wurde von britischen Forschern , A. Turing und Team entwickelt*) eine Maschine, die von NCR gebaut ist, um Nachrichten von der deutschen Rätselmaschine zu entziffern. Die Armee und das **Nary** entwickelten auch Geräte von wachsenden Macht und Kapazität während des Kriegs. Die Maschinen konnten Mitteilungstexte zusammenstellen und vergleichen, nach Krippen suchen oder statistische Zufälle suchen. Die farbigen Laufwerkkenzeichnungen von diesen Maschinen schlossen Drachen, Mokassinschlange, **RATI'LER**, Mamba, **DUENNA**, Madame X und **SUPERSCRITCHER** ein. Keine von diesen waren tatsächliche Computer, *da* ihnen Gedächtnis oder die Fähigkeit dazu, zu leisten, Außenseite ihrer bestimmten Rechenfunktionen fehlte.

{U) Großbritannien und die Vereinigten Staaten wurden nahe Partner, in **cryptanalysis** und da eine Folge Maschinen aus wachsenden Macht und Komplexität baute, um die Schlüsselssysteme ihrer Feinde zu lösen. Nahe dem Kriegsende entwickelte die britische Regierung ein Gerät, das als der erste wahre Computer gekennzeichnet werden konnte. Für rasche Ausnutzung der als Thunfisch (*Enigma*) bekannt deutschen Verschlüsselungsmaschine erfanden britische Ingenieure den Koloss, den gehabte viele Merkmale jetzt mit Modemcomputern verbanden. Fast zur gleichen Zeit hatten amerikanische Ingenieure an der Universität von Pennsylvania auch einen Computer ENIAC gebaut, um Artillerieballistiktabellen zu generieren.

Stelit ich)) iIEL t 6 03 t. Ich t §, CJ t! ICH. 8!ttt. lth (U) auf diese Art, vom Ende des Kriegs US-Anny und marineblaue Kryptologen hatten beträchtliche Erfahrung mit Spezialgeräten und sogar den britischen proto Computer. Diese beiden Diensten klar gemachte Erfahrung, dass rasche Datenverarbeitung zukünftig für amerikanische Kryptologie wichtig wäre. Die Herausforderung *sollte* ihr schwer gewonnenes Wissen von Spezialmaschinen auf das Design eines zu mehrfachen Bewerbungen fähigen Universalrechners übertragen. Obwohl breit anerkannt dass die Vereinigten Staaten rasche Datenverarbeitung für ihre cryptologic Ausnutzungsbemühungen brauchten, Budgets leider fielen, viel technische Experten Staatsdienst ließen, und industrielle Verträge erloschen während der unmittelbaren Nachkriegsära. Das am besten, dass das durch betriebsinterne Forschung getan werden konnte, war Produktion von als rasche analytische Maschinen bekannt cryptanalytic Geräten, die gegen je nur ein ausländisches System funktionierten. Diese Geräte enthielten ALCATRAZ, O'MAU.EY, Zauberer, HECATE und Schlitten.

(U/; ' JiQTTi ~ von Mittel-1946 neuen Fortschritten trat in Datenverarbeitung auf. Programmiersprachen, gesteigertes Gedächtnis und neue Prozessoren wurden vorgestellt, und discussed. an führender Hochschulforschung zentriert. Besonders führten zwei Zivilforscher James Pendergrass für die Marine und Samuel Snyder für die Armee der Weg in kritischen Bewerbungen von Fortschritten in kommerzieller Datenverarbeitung für militärische Kryptologie. Bis 1947 beschlossen die beiden Anny und marineblaue cryptologic Organisationen, Computer zu erwerben.

(U/; ' fiUi'~ in 1950, der Marineblauen und Industrie arbeitenden, produzierte zusammen den ersten wirklichen Universalrechner für die Regierung. Gebaut von elektronischen wissenschaftlichen Mitarbeitern (Ära), eine geleitete Gesellschaft von Howard Engstrom, der selbst am marineblauen Bombe während des Kriegs gearbeitet hatte, sie hieß ATIAS. Diese Maschine kostete ne.a.rly \$ eine Million, verwendete 2,700 Vakuumröhren und hing von Trommelspeichertechnik ab. Atlas würde gut im anschließenden Jahrzehnt zur Unterstützung von cryptanalysis arbeiten, wobei er verwendet wurde. One of A TLAS's greatest assignments was to attack isologs in messages codenamed VENONA, intercepts of Soviet espionage communications during the height of World War II.

~ Atlas war vom marineblauen verwendenden Outsourcing gebaut worden, aber das Anny hing stattdessen von betriebsinterner Arbeit für seine eigenen Computerforschung und Entwicklung ab. Der Armeesicherheitsdienst (ASA) beschäftigte mit beträchtlicher Entwicklungsarbeit für seinen eigenen Computer, aber geübte nicht begonnene tatsächliche Produktion zur Zeit die Bewaffneten bricht Sicherheitsdienst (AFSA) auf

wurde im Mai 1949 gegründet. Viele cryptologic Forschungsfunktionen, Datenverarbeitung einschließend, waren fundiert unter AFSA, und der Ausbruch des Koreakriegs lieferte den Anreiz für mehr rasche Entwicklung. Da sich konventionelles Mittel als zu langsam darin erwies, US-Verschlüsselungstabellen zum Kriegsgebrauch durch amerikanische Streitkräfte auszuwerten, bevollmächtigte AFSA Produktion von .ASAs Computerentwicklung. Das Ergebnis, beendet im Jahr 1952 unter einem ASA Vertrag, war ABNER, ein allgemein verwendbarer analytischer Computer. ABNER bestand aus Vakuumröhren und hielt auch nur 16. drückt in seiner Erinnerung aus, aber beigetragen mächtig dazu, Berechnungsgeschwindigkeit zu reduzieren.

Sie zentrieren für Cryptologic Geschichte

YUP tiEIJRliiF; Vi8f lliifiF; ' Alii U UO: ;; tUJ, schlechtes Übel 88 R, IJEE

(U) **NSA*s** Schlüsselrolle in größeren Entwicklungen in Computer Science

TEIL ZWEI

(8 #81es ' bald nach seiner Formung am 24. Oktober 1952 **NSA** stieß auf eine andere Möglichkeit dazu, elektronische Datenverarbeitung zu verwenden. Während der Mitte -1950er schickten Standorte rund um die Welt jeden Monat 37 Tonnen von Abschnitten nach **NSA**, und konventionelle Maschinen waren der Aufgabe zu sortieren nicht gleich, als sie standardisierten, das und das Vertreiben dieses Betrags. Um von diesem Volumen zu handeln, gab **NSA** mehr als \$ 3 Millionen Dollars für einen Vertrag aus, Nomaden zu entwickeln. Dieses Gerät, entworfen dafür, Rechnerspeicher exponentiell zu steigern, versäumte, adäquat von der ständig sich ausdehnenden Menge des eingehenden Materials zu handeln.

(ich ': ' lili) wenn der Ausfall des Nomaden werden offensichtlich, **NSA** entwickelte eine Anzahl von Spezialgeräten, um die notwendigen Daten auszuführen, die zurechtkommen und verarbeiten, die Nomade zusammengestaucht worden war zu tun. Die vielen Auftragsanforderungen erfüllen, mit denen sie während der Höhe des kalten Kriegs beschäftigt worden waren, **NSA** war unter den ersten Organisationen, um Gebrauch von Systemen zu machen, die innovative Zufuhrtechniken und Speichervorrichtungen integrierten, als sie Trommellagerung, Bandlaufwerke, entfernten Arbeitszugang einschlossen und Computerchiptechnik. Solo, ein in die Mitte -1950er eingebauter Computer wurde die erste Maschine, um Vakuumröhren durch Transistoren zu ersetzen. Spezialcomputer wurden für **cryptanalysis**, aber auch nicht nur dafür entworfen, Kommunikationssicherheits- (COMSEC) Material für Schutz der US-Kommunikation zu generieren. Ein anderes System benannte **BOGART**., entworfen ursprünglich dafür, Nomaden zu unterstützen, verwendete feste Staatstechnik zum ersten Mal für langfristige Datenspeicherung und nutzte neue Bandlaufwerke für sie aus. **BOGART** diente auch als der Zentralrechner für rauben **ROY**. eins die ersten entfernten Jobeintragungssysteme. Von verwandter Bedeutung kam Gauner zu dieser Zeit als der erste entfernte Arbeitszugangscomputer heraus.

('1' 8; '; 181) durch die Späten 1950er, die höchste Priorität waren zu **cryptanalytically** Angriffssowjet verschlüsseln Systeme. Eine größere Studie, bei der der Vorsitz von Expräsident Herbert Hoover geführt ist, empfahl einem totalen widerwärtigen Programm gegen sowjetischen Schlüsselsystem ~, das dem Projekt, das die Atombombe entwickelt hatte, in Umfang ähnlich war. Der erste Direktor. **NSA** (DIRNSA). Generalleutnant (LTG) Ralph Canine, der in Howard Engstrom gebracht ist, um Forschungsaufwände dazu zu führen, dieses Problem zu lösen. **Engstrom**, wer würde später **NSAs** Abgeordneter werden, in den **director**. Ideen von **NSA** Wissenschaftlern und Kryptoanalytikern sortierte, die beide langfristige Forschung betrachten, super-schnelle Computer und Beurteilungen von sowjetischen Schlüsselsystemen. Seine Befunde entwickelten sich schließlich zu einem Vorschlag zu als Projekt bekannt Schnellcomputerbau freihändig. Eine untergeordnete Anstrengung, unterstützende Metallwaren zu entwickeln, wurde als der Projektblitz bekannt.

(8: ': ' 8 "allgemeiner Hund wollte, dass die Pläne begonnen wurden, bevor er sich zurückzog, und es ihm gelang, höhere Finanzierung und Unterstützung zu bekommen, für Projekt freihändig. In eine Besprechung mit)

Declassified und gebilligt für Freigabe von **NSA** auf 07-19-2011 entsprechend E .Os.

13526 : BVORFRMNN -101721

: Der Nachfolger des Hundes, **LTG** John Samford, Präsident Dwight Eisenhower tat es formell: //approve// der Projektblitz. Howard Campaigne became the LIGHTNING program : manager and was charged with developing a super-fast computer to meet the country's : national security needs. Verwandte Fortschritte, die sich aus diesen **NSA** Projekten ergaben, beinhalteten: die Entwicklung der Kryotron, um Computerbetriebstemperaturen, Bestandteil zu senken: Miniaturisierung, das und das schnell Tauschen von Geräten mit Hilfe der Tunnelodiode.

▪

FE // "" zur gleichen Zeit der Blitz begann, die IBM Corporation schlug vor ein: **paraJlel** erforschen als Ernte **Notably**. sowohl **Engstrom** als auch Snyder bekannt Spur; war gegen das **concept.**, das behauptete, dass die eingeschlossene Technik nicht so fortschrittlich wie war: brauchte, und diese Finanzierungsernte würde sich in Projekt **FREEHAND**. einmischen: Jedoch General **Samford** genehmigte den Vorschlag mit Ernte, IBM, eingeführt, ein: neu neuester zweite Erzeugungsgemein verwendbarer Prozessor.

(1' "EI) To be successful, HARVEST had to have a super-high-speed memory : and high-speed tape drives beyond anything then in existence, Developed over five : years, the most innovative component was TRACTOR, a high-speed tape drive system. Es: war das erste vollständig automatisierte Lagerung und Retrieval-System und ein Vorgänger zu Strom? Speichersysteme. Aber Ernte war auf höhere Kosten hereingekommen, als hervorgeragt, bewiesen: sehr schwierig zu verwenden und langsamer gehabt Durchsatz als geplant. While NSA : personnel wrote innovative programs for it that extended its applications, HARVEST ; never achieved the goal of multiprogramming. Dennoch blieb Ernte in: Dienst von 1962 bis 1976.

(TI "" EI) schon durch die Frühen 1960er, Automatisierung völlig überschatteten: Handbuch verarbeiten. In der Mitte dieses Jahrzehnts beginnend, begann **NSA** zu kaufen: geschäftlich entwickelte Computer zusätzlich zu dem Bauen seiner eigenen Einheiten. Agentur: Programmierer schrieben oft spezialisierte Software, die die **cryptologic** Fähigkeiten erweiterte: von diesen auf dem Brett Systeme. Der Computer von Wahlmöglichkeit war die IBM 7010. NSA also : used the minicomputers PDP-1 and PDP-10 as well as the UNIVAC 490, along with a : software developed at NSA known as RYE. The Honeywell Corporation also developed : the Honeywell 316 to accept manual Morse data from 128 different sources ; simultaneously and record it directly onto magnetic tape. Auch, Sammelsysteme: sogar in ferne Standorte wurden digital basiert. Weiterhin berücksichtigten Computer auch die Sammlung von einer größeren Vielfalt von Signalen, als sie beinhalteten

Ich an 1968 NSA hatte über 100 Computer, organisiert in Komplexen entsprechend der Art der ausgeführten Verarbeitung. NSAs fünf Morgen Ausrüstung wurden die größte Sammlung von modernen Computern in den Vereinigten Staaten und wahrscheinlich in der Welt.

das **Aufkommen der Ernte hatte die Vorherrschaft markiert, durch große Zentralrechner zu berechnen, NSA hatte sechs Komplexe dieser Zentralrechner entwickelt**, gewidmet je einem Sonderzweck. UNIVAC und Honeywell Computer verarbeiteten *inc, ~ ing*

da ~ al strömt am Datenübertragungskomplex. Fünf IBM -370er führte Stapeljobs der Roggenkomplex unterstützte gegenwärtige Operationen, ein Paar von UNIVAC 1108er führte p ein! *n ab.* Control Data Corporation (**CDC**, der Nachfolger in Ära) Computer verarbeiteten elektronische Intelligenz. Die Größten von diesen sechs Komplexen *waren cryptanal ~* gewidmet ist.

(U "FQ! Ui ") an den 1980ern, NSAs Zentralrechnern war, überfüllt zu werden, und die Agentur bewegte sich in Richtung Einsatzes von Personalcomputern (PCs). Während der Mittelstimme des Jahrzehnts wurde der IBM PC XT der Standard für Benutzerschnittstelle, und AT&T stellte das Netz für sie auf zur Zeit für das dominierende Betriebssystem, Unix. Auch während dieser Zeit führte NSA zwei wichtige Zentren, eins, für Supercomputerforschung und den Anderen für Rechnersicherheit ein.

(U: 'F9U' i) **obwohl, wie Zeit verging, Entwicklungen in der Computerindustrie verloren hatten das früher Querverbindung zur ständig wachsenden Komplexität der Kryptologie, die Agentur fuhr fort, an der ersten Stelle von größerem Fortschritt zu bleiben.** In der Tat wurden einige der frühesten Supercomputer für NSA gestaltet und gebaut. Bis zu den frühen 1970ern war die Agentur in die Ära des Supercomputers Hals über Kopf mit dem Kauf von **CDC 6600** bewegend und später das **CDC 7700**. In 1972 früherem **CDC Angestelltem** bildete Seymour **Cray** seine eigene Gesellschaft und begann, seine Supercomputermarke zu gestalten. NSA . kaufte das erste eines seiner Produkte, Cray ich im Jahr 1976. Im Jahr 1983 war Crays **XMP -22** der erste Supercomputer, den Cray jemals tatsächlich einer Kundenseite lieferte. Sie wurde bald zu einem **XMP -24** befördert, wohl leistungsfähigster Computer in der Welt, wenn sie, kam online. Das **XMP -24** verwendete die serielle Verarbeitung, um 420 Millionen Operationen pro **second.** zu führen, und blieb in Betrieb von 1983 bis 1993.

(U: '; 'f81 "8) die **zweite Generation** Cray, das **YMP -90** **ersetzte die ältere Version im Jahr 1993.** Es hatte eine 32 Gigabytespeicherkapazität, ein 2,000 mal dem Speicher der besseren Personalcomputer von dieser Zeit. Das **YMP -90** verwendete die Vektorverarbeitung, eine mit Parallelverarbeitung verbundene sehr mächtige Form zu überlappen, um 2,67 Milliarden Operationen pro Sekunde zu führen. Arbeiten so rasch dass es **itself.** schmelzen konnte der Designer hatte ein Kühlsystem installiert, das Gebrauch von **Flourinert** machte, gepumpt durch Röhren, die durch die Leiterplatten gehen. The YMP-90, called "Barney" due to its sharing of the purple color belonging to a contemporary popular children's television character, was decommissioned at decade's end.

("EI) es gab andere wichtige ComputerfIRSTen bei NSA. Ein anderer

Supercomputer wurde von der Thinking Machine Corporation entwickelt. Dieser Computer wurde als der cm -5 oder **FROSTBURG** bekannt. Gebaut zu Kosten von \$ 25 Millionen, hatte der cm -5 eine Lagerkapazität von 500 **gigawords** und konnte 65 Milliarden Berechnungen pro Sekunde ausführen. Entworfen dafür, höher mathematikgebundene Fragen anzugehen, war **FROSTBURG** einer der ersten wahren Parallelverarbeitungscomputer. Auch Wert, erwähnend, wenn **instajjed** der Schritt 10 war der erste analoge Tischcomputer in Verwendung bei **NSA**. Dieser Computer benötigte die elektrischen Handleitungen von verschiedenen Tafeln, dass jede Art mathematischer Berechnung ausgeführt wird. Von weiterer Notiz entwickelte **NSA** viele einzigartige und Pioniersoftwaresysteme und Datenbanken wie SOLIS, die alle **NSA** Elektronikartikelberichte hielt.

(**UNF8t98**) **NSA produzierte** auch Computer für **Telemetrierverarbeitungssysteme**. Wie **ofNSA** zu teilen, signalisiert Intelligenz (**SIGINn** Auftrag, Telemetrie signalisiert, dass von verschiedenen Bühnen gesammelt wurde. Magnetbandaufnahmen der abgefangenen Signale wurden damals zu **NSAs** nationalem Telemetrierverarbeitungszentrum für das Verarbeiten geschickt. Diese Messungen wurden damals in der Form des Computerbands in Analysezentren gesendet das identifizierte das

Funktion der verschiedener Umformer und schließlich entwickelter Leistungsschätzungen. **TELLMAN**, das **NSA** ist erster Telemetrieprozessor, um extensive Verwendung von einem Universalrechner zu machen, wird im Jahr 1969 betriebsbereit. In den frühen 1980ern war **TELLMAN** . ersetzt durch **RISSMAN**, welches verarbeitete eine größere Vielfalt von Signalen mit höherem System · Zuverlässigkeit und niedrigere Instandhaltungskosten.**RISSMANs** kundenspezifische Metallwaren verwendeten · drei Intel 8086 Mikrocomputer, um Echtzeitprozess auszuführen, den **control. whiJe** digitale · VAX -11 Computer Daten **demultiplexing**. lieferten, Datendateilagerung, Benutzerschnittstelle. Lokaler Bereich · Netzzugriff, digitale Banderzeugung und Qualitätskontrolle, die Dienste aushecken. '**RISSMAN** war in täglicher Verwendung, als es Bänder oft rund um die Uhr vom Datum seiner Lieferung durch das Ende des kalten Kriegs verarbeitete.

(U: ': ' **FSt!JS**), die geschaffenen Daten zu speichern, war ein anderes Problem, dass **NSA** mit Außenhilfe löste. Frühe Bemühungen schlossen ein Photo, das digitaler Prozess von IBM entwickelte, und ein Bandspeichersystem von **AMPEX** ein. More recently. the Storage Technology (Storage Tek)

: Corporation hat viel von **NSAs** Aufzeichnungsmedien produziert Lagerbibliotheken. Lagerung **Tek**: gestaltete ein automatisiertes Bandkassettesystem für die Großen, Komplexen und Hohen-: Leistungsumgebung von **NSA**.Es besaß ausreichende Kapazität für 6,000 Band: Kassetten, die je 50 Gigabyte Daten hielten.Das Benutzen eines Roboterarms, des StorageTeks: Maschine ist dazu fähig, 175 Kassetten pro Stunde zu tauschen.Das ganze System kann halten; 3 0 Terabytes von Daten.

. (U: ': ' **I?8 Isllii**), da sie die Welt besitzt, ist größte Supercomputing-Einrichtung an sein · headQuarters, NSA therefore has a great demand for microchips. I

(**UNF!iIslllich** } in letzte Jahre, Bericht und Analyse bewegte sich zu einer Onlinebasis, um rasche Verbreitung zu erleichtern. Während der 1990er stellte die Agentur

das NSA Netz (NSANet) auf . ein internes klassifiziertes Netz. Konnektivität zum Rest des Ic wurde vornehmlich durch das Gemeinschaftsweltweite Intelligenzkommunikationssystem (JWICS) eingeführt . ein Rückgratsnetz, das alle Mitglieder der DoDintelligenzinformationssystem- (DODIIS) Gemeinschaft verbindet, die Militärkommandos und der Ic. Intelink t (die der General NSA Population als einfaches "Intelink" bekannt sind) ist die t/SI/Tkbewertete USA-nur Netz, das auf JWICS reitet, um den leichten Informationsaustausch innen zu erleichtern der Ic. Das Intelink S (für Geheimnis) Netz reitet auf dem geheimen Internetprotokollkopplernetz (SIPRNet) ., aber es gibt keine physische Verbindung zwischen NSANet und SIPRNet. Diese und die anderen Mitglieder der Intelink Familie werden von dem Intelink Verwaltungsbüro (IMO), einer Iorganisation geleitet, die bei NSA präsentiert ist.

(U; ' ; ' fiWI!lich), um an der Vorhut von den Letzten zu bleiben, Fortschritte, NSA haben versucht, immer zur Privatsektorforschung hinauszureichen und bestimmte Gemeinschaft zu entwickeln, Die Hauptforschungsgebiete bestehen A.T.photonik andl elektronische Bewerbungen, Magnetisierung, thermische management. Material und Gerätefertigung, optische gemeinsame Zitate und Mikroelektronik einschließlich der Erkundung vom Verarbeitungspotential von Quantenphänomenen.

(U; ' /F@~@) die Entwicklung von Computern für cryptologic Anwendungen geschah nicht glatt oder direkt. Auf bestimmte Probleme, und wie man sie lösen kann, nicht abstraktes theory. und dort gerichtete NSA Forschung war viele Ausfälle und Fehlsowohl Anfänge als auch Erfolge. Jedes neue System gab jedoch NSAs Analytikern verbesserte Fähigkeiten und in irgendwelchen lieferte jenen, die mit Grundlagenforschung verbunden waren, Fall eine ausgezeichnete Lernerfahrung. Es ging NSAs Computern fast immer gut vor Datenverarbeitungsanlage irgendwo anders. In Verbindung mit ihren Partnern in Industrie und Akademikerwelt, NSA fährt fort, ein Vorreiter bei Forschung und Entwicklung von Computertechniken zu sein, und ist ein einzigartiger Pionier auf den Grenzgebieten von Informatik und Elektrotechnik gewesen.

Diese Publikation ist sehr empfehlenswert :

(U) für weiteres reading. sehen: (U) Bamford, James, Körper von Geheimnissen: *Anatomie des extremen Geheimnisses Staatssicherheitsagentur* (Doubleday: 2001).

(U) Boak, David G., A Geschichte von US-Kommunikationssicherheit (NSA: 1973) . (U) Burke, Colin B., sie war nicht ganz MA CIC: *Der frühe Kampf, um Cryptanalysis zu automatisieren, (zentrieren für Cryptologic Geschichte (CCH): 2002).*

(U; ' ; ' f8-W8) Johnson, Thomas R., *amerikanische Kryptologie während des kalten Kriegs, 1945-1989 (CCH: 1995- 1999).*

<https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/nsa-early-computer-history/6586785-nsa-key-role-in-major-developments-in-computer-science.pdf>

Weitere Quellen siehe Originalpublikation