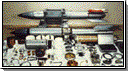
**PAL - Permissive Action Links**

[](http://www.cs.columbia.edu/~smb/nsam-160/B61clr.jpg)*"Bypassing a PAL should be, as one weapons designer graphically put it, about as complex as performing a tonsillectomy while entering the patient from the wrong end."*

**What is a PAL?**

A PAL -- a "Permissive Action Link" -- is the box that is supposed to prevent unauthorized use of a nuclear weapon. "Unauthorized" covers a wide range of sin, from terrorists who have stolen bombs to insane American military officers to our allies who may have some of their own uses for bombs that are covered by joint use agreements. It's supposed to be impossible to "hot-wire" a nuclear weapon. Is it?

There is little in the public record that discusses just how Permissive Action Links (PALs) work. This isn't surprising, of course; remarkably little has been published about most technical details of nuclear weapons design. Even so, much more has been published about the so-called "physics package" than about the control aspects. This may be because something that goes bang is sexier, of course. But it may also be because fission and fusion are natural processes that can be studied in the abstract. Someone can reinvent the atom bomb (as, indeed, many have done). A PAL is an engineering artifice, with many possible design choices. Furthermore, the design of a PAL is based on cryptography, and cryptography has always had the aura of the forbidden.

**My Motivation**

I've occasionally been asked why I compiled this page. It stemmed from my interest in the history of cryptography (see Prehistory of Public Key Cryptography for details), and for the implications of PAL design for tamper-resistant devices in general. I claim no expertise in nuclear weapons design.

**History**

PALs evolved from the need to exert greater negative control over nuclear weapons. Contrary to popular belief, the original motivation was not to guard against unauthorized actions by rogue American military officers. To be sure, this was not a negligible threat. More than one Strategic Air Command head was interested in starting World War III; one was later described this way by another general who reported to him:

I used to worry about General Power. I used to worry that General Power was not stable. I used to worry about the fact that he had control over so many weapons and weapon systems and could, under certain conditions, launch the force. Back in the days before we had real positive control [i.e., PAL locks], SAC had the power to do a lot of things, and it was in his hands, and he knew it.

A more pressing concern was foreign access. Under the auspices of NATO, assorted nuclear weapons were at least partially controlled by other nations. This was worrisome, especially to Congress, and in violation of U.S. law. Worse yet, some of our allies were seen as potentially unstable; there was considerable fear that the military in one of these countries might override even their own civilian leadership. Stein and Feaver cite France as one possible example, and possibly Germany and Turkey:

The exact details are hazy, but the broad contours are clear: the inspection team found the control of the forward-based nuclear weapons inadequate and possibly illegal. In Germany and Turkey they viewed scenes that were particularly distressing. On the runway stood a German (or Turkish) quick-reaction alert airplane (QRA) loaded with nuclear weapons and with a foreign pilot in the cockpit.

The QRA airplane was ready to take off at the earliest warning, and the nuclear weapons were fully operational. The only evidence of U.S. control was a lonely 18-year-old sentry armed with a carbine and standing on the tarmac. When the sentry at the German airfield was asked how he intended to maintain control of the nuclear weapons should the pilot suddenly decide to scramble (either through personal caprice or through an order from the German command circumventing U.S. command), the sentry replied that he would shoot the pilot; Agnew directed him to shoot the bomb.

In a discussion of the French need for PALs on their own weapons, Stein and Feaver say this:

France's history has not been characterized by the same orderliness of political succession and civil-military relations as Great Britain's. Indeed, there have even been moments of instability in the nuclear age. During the revolt of the generals against De Gaulle in 1960, for example, the government ordered the detonation of a nuclear device in Algeria so that it would not fall into the hands of the military.

For these reasons, I suspect that the "sanitized" Alternative I of NSAM 160 almost certainly calls for PAL protection only for weapons in a few specific countries, and may even cite them by name. (Another point here is that weapons that might be captured by an enemy need more protection. It wouldn't be politic to disclose that the U.S. expected certain countries to be overrun early in a war -- though of course that is to some extent obvious, especially for parts of Germany.)

The U.S. military resisted PALs for a long time. Eventually, they were persuaded because of the greater freedom it gave them: in times of tension, they could disperse nuclear weapons to block easy destruction or capture, while still retaining control over their use.

Despite that, they didn't deploy PALs that quickly. In 1974, when an armed quarrel broke out between two members of NATO (presumably Greece and Turkey, though the reference doesn't say), the Secretary of Defense learned that many tactical nukes were not equipped with PALS. Worse yet, he learned that some military commanders of these nations *wanted* those nukes.... It took two more years before PALs were completely deployed. Even then, the Pentagon dithered; at ICBM silos within the U.S., the "secret unlock code" was set to 00000000. On the other hand, some PALs were deployed by the time of the Cuban Missile Crisis, though the deployments did not yet include the Jupiter missiles in Turkey. This fact was of some concern at the time; under President Kennedy's orders, the Joint Chiefs of Staff ordered the U.S. commander in Turkey to destroy the missiles -- which, unlike their nuclear warheads, were under Turkish control -- rather than let them be launched without his explicit permission. (This might suggest that Alternative I -- presumably the highest-priority deployment -- specified Germany and/or France.)

PALs are supplemented by "coded switch systems". These are devices that prevent the release or launch of an armed nuclear weapon. For example, when B-1 bombers are on alert, the PALs in their weapons are unlocked before takeoff. But the crew can't use those weapons until they receive an authorization code. (In some planes, the crew can communicate with the PALs from the cockpit. This feature was omitted in the B-1, apparently as a cost-saving measure.)

Given this, it is not surprising that Navy weapons are not protected by PALs. In their normal environment, there is relatively little risk of capture, no foreign nationals have custody, and communications with (especially) submarines is somewhat problematic. Only when the weapons are brought ashore is a PAL activated, and then only for things like nuclear depth charges. In place of PALs, an elaborate set of procedures, involving the PA system, several different keys, and the participation of most of the crew is necessary for a nuclear submarine to launch its missiles. All that notwithstanding, a use control system, apparently similar to the coded switch systems, has recently been added to the submarine fleet. For that matter, by the early 1970s the insider threat was realized; this was the motivation for the installation of use control systems on the bombers and on the strategic missiles by 1976/7.

Several different mechanisms are used to prevent accidental detonation. First, there is the "strong link/weak link" principle. Critical elements of the detonator system are deliberately "weak", in that they will irreversibly fail if exposed to certain kinds of abnormal environments. A commonly-used example is a capacitor whose components will melt at reasonably low temperatures. The "strong" link provides electrical isolation of the detonation system; it only responds to very particular inputs. Naturally, this entire subsystem is physically packaged in such a way as to shield critical parts of the weapon from any unwanted electrical energy. A very detailed description of strong and weak links can be found in.

Bombs are also engineered to fail gracefully. For example, the high-explosive shell is closely matched to the characteristics of the fissile materials in the pit; if anything but the exact proper detonation occurs, there should be no nuclear reaction. The design goal for the safety mechanisms is a probability of less than 10-6 that an accidental detonation at one point in the explosives surrounding the core can cause a detonation equivalent to more than four pounds of TNT, and the probability of an accidental nuclear detonation due to component malfunction be less than 10-9 for normal conditions, and 10-6 for abnormal conditions.

Advances in computers have permitted the use of three-dimensional models of bomb components. These have shown that earlier two-dimensional models were dangerously misleading. Apparently, the danger was greater than had been appreciated that an accidental explosion could cause dispersal of radioactive materials or even a nuclear yield.

Coupling between at least some different stages of the detonation system is by means of a moderately complex digital signal, and not a simple contact closure. Again, the intent is to prevent accidents. It is possible that PALs function by decrypting this signal, though that by itself would not achieve the no-bypass design goal.

Bombs are also protected against accidental (and some unauthorized) detonations by "Environmental Sensing Devices" (ESDs). ESDs detect the normal physical environment expected for that weapon. For example, a nuclear warhead in a missile would experience high acceleration, a period of free fall, and then some deceleration. Its ESD is designed to detect those conditions; the warhead is not armed until they occur. Someone who stole the warhead could not detonate it unless the launch system was stolen as well. Of course, in some situations that is a risk, too.

In at least one incident, a nuclear weapon did come very close to accidental detonation. In 1961, a B-52 with two large warheads crashed near Goldsboro, North Carolina; the impact set off the conventional explosives in one of the bombs, and triggered all but one of the safety mechanisms in the other.

PALs are powered by radioisotope thermoelectric generators. An RTG provides for very long lifetime with little maintenance required. They work by alpha decay of plutonium-238, a non-fissile isotope. The limiting factor on the lifetime of an RTG is helium buildup.

**Types of PALs**

There have been a number of different types of PALs used over the years.

Combination lock

The earliest control mechanism was a three-digit combination lock. Later versions were four-digit locks designed to accommodate split-knowledge, where two different individuals could each have half the key. The combination lock can do different things. Some block the volume into which firing components must be inserted, others block electrical circuits, while still others prevent access to the fusing and arming mechanisms.

These locks were in use at least as recently as 1987. In 1981 -- almost 20 years after PALs were invented -- about half of the U.S. nuclear weapons in Europe were still protected by mechanical locks.

CAT A

CAT A PALs, intended for use on missiles, were electromechanical switches. The arming input was a 4-digit decimal number. (Some sources say it was a 5-digit number.) Crews used a portable electronic device that plugged into the weapon to arm it.

CAT B

The CAT B PAL, used on bombs, was similar in spirit to the CAT A, but used fewer wires. This permitted remote control of the PAL from an airplane cockpit. With the CAT B, it is also possible to check the code, relock the weapon, or rekey it. Later models of the CAT B included a limited-try feature, rekeying, and a code-controlled lock.

CAT C

The CAT C PAL accepts 6-digit keys. A limited-try feature disables the bomb if too many incorrect keys are entered. Most references omit the CAT C. It may just be a later model of the CAT B.

CAT D

The CAT D PAL accepts 6-digit keys. A given PAL can accept a number of different keys, permitting different groups of weapons to be unlocked with one transmission. Some keys are used for training; others are used to disarm the weapon or to disable it. One source suggests that PAL codes can also be used to vary the yield on some weapons. There are a number of selectable mechanisms to disable the bomb. In addition, there are "violent or nonviolent methods for destroying the warhead or making it irreparably nonfunctional". (One report, which I have not yet seen confirmed in the literature, is that the violent option involves a shaped charge which destroys the symmetry of the pit. It is thus no longer able to fission until it has been re-machined -- and machining plutonium is non-trivial.) One reference suggests that there is a remote disable option on some PALs.

CAT F

The CAT F PAL appears to be similar to the CAT D, but it accepts a 12-digit key.

The 1984 price for a CAT D PAL was $50,000.

I haven't yet found anything about setting C.R.M.-114 discriminators to "FGD 135", let alone "OPE"...

**Cryptography and PALs**

Given all this, what cryptographic mechanisms are used for PALs? I have not been able to find any public material on the subject.

It is known that PALs work on cryptographic principles. A common supposition is that the arm code is in fact a key that is used to decrypt some of the timing data. Phil Karn made the following suggestion:

Precise timing -- that's the key to my idea for a highly effective PAL. First, design the weapon to make the firing sequence as inherently complex and critical as possible. Vary the chemical composition and detonation velocities of the various pieces of high explosive so they have to be detonated non-simultaneously. Then store all of the required timing data in encrypted form in the weapon's memory. Better yet, encrypt *everything* (program and data) except for a small bootstrap that accepts an external key and decrypts everything for firing. Include this decryption key in the "nuclear weapons release" message from the "National Command Authority" (I've always loved that military terminology!)

I've suggested similar ideas in the past, including the use of somewhat different shapes for each piece of the lens. That way, each individual detonator must fire at a different time.

It isn't clear that that works. Apart from the possible ease of determining the types of the different explosives, the goal of the implosion is as near-perfect a spherical shock wave as possible. Traditionally, this has been done by covering the sphere of explosives with equally-spaced detonators and triggering them simultaneously. There would not appear to be much room for variation, especially since the tolerance is only about 100 nanoseconds.

A timing-based PAL is much more logical if a non-spherical explosive shell is used. If some of the explosives were thicker, they would have to be fired slightly sooner. This may be desirable even with a spherical arrangement, to achieve higher yield. It is mathematically impossible to have both detonators that are exactly equally spaced and an adequate number of them. Timing variation may compensate for that. Similarly, an asymmetric fissile core would require non-simultaneous detonations. Such a variant is not at all inconceivable. Hansen reports early experiments with such things. Furthermore, at least one model of a nuclear artillery shell imploded a cylindrical core. (The motivation for such shapes is the geometry plus size constraints on the warhead. The B61 bomb, for example, is only 12" (30 cm) in diameter. This does not leave much room for a sphere of high explosive surrounding a pusher, a tamper, an air gap, and a fissile core.)

During the investigation into alleged Chinese espionage against the U.S. nuclear weapons programs, it was disclosed that modern U.S. hydrogen bombs do, in fact, use a non-spherical core. This is apparently a key technique in building miniaturized warheads. states that two-point detonation is used on warheads like the W88.

It does not appear to be feasible to build detonators that have their own delay elements. In fact, the problem all along has been to build detonators that would fire at a predictable time after triggering. Known designs require high current and high voltage; switching this is non-trivial.

Modern bombs use complex electronics. An early attempt by India to test their bomb is rumored to have failed because of an electronics malfunction. Some newer U.S. bombs use microprocessor-based controllers and sequencers, an design choice that would not have been taken without pressing need.

Another possible design principle -- this is speculation; no authoritative sources have said this -- would be scrambling the wires. Suppose that a group of wires led into a scrambling unit. The scrambling unit would have a set of Enigma-like rotors; only if they were all in the proper position would the proper connections be made. If it were not obvious how the wires should be connected -- and if, perhaps, they were embedded in epoxy as they entered and left the unit -- it would be very hard to analyze them and hence bypass them. At the very least, there would be a delay of several hours while the circuitry was analyzed.

The simplistic encryption idea doesn't fit the newer CAT D and CAT F devices. As noted, those models use multiple codes that can arm different sets of devices. Some PALs have a "training key" -- a code that gives a useful response during an exercise, but does not actually unlock the device. At the least, these imply a level of indirection in the key structure. Furthermore, there must be a command channel to allow for changes to the group structure.

At least one source suggests that the actuating mechanism is mechanical, not purely electronic. This would also tend to contradict the design hypothesis given above. The course on PALs doesn't seem to explain such details, either... suggests that a possible PAL design principle involves physically moving assorted parts into the proper positions. There is precedent for that -- not only were the very first nuclear weapons partially assembled on board the plane, an "automatic insertion" device was later used to mechanize that step. (Another early mechanical safety mechanism was a boron-cadmium wire in the center of the pit. The boron and cadmium would, in theory, absorb enough neutrons to damp the chain reaction. To arm the bomb, the wire was withdrawn. This turned out to be problematic on the W47 warhead. When the device had been in storage for a while, the wire tended to break during withdrawal. For a time, much of the U.S. nuclear submarine fleet was armed with defective warheads, until the bomb was redesigned.).

PALs seem to rely on cryptographic principles and tamper-proof design:

There are two basic means of foiling any lock, from an automobile ignition switch to a PAL: the first is to pick it, and the second is to bypass it. From the very beginning of the development of PAL technology, it was recognized that the real challenge was to build a system that afforded protection against the latter threat. Rather than attempting to build an indestructible lock, scientists at Livermore Laboratory in 1961 directed their efforts towards constructing a system that would render a weapon unusable if an attempt was made to interfere with its PAL. By 1964, it had been demonstrated that this approach would work.

The design was perfected and incorporated into weapons that utilize CAT D and CAT F PALs. With this system, the insertion of too many false codes or an attempt to bypass the PAL will render the weapon permanently inoperative, and the weapon must then be returned to the weapons plant for reassembly. The protective system is designed to foil the probes of the most sophisticated unauthorized user. It is currently believed that even someone who gained possession of such a weapon, had a set of drawings, and enjoyed the technical capability of one of the national laboratories would be unable to successfully cause a detonation without knowing the code.

The requirement for safety in the face of an enemy with full knowledge is eerily similar to the requirements for the security of a cipher system.

An admiral was less convinced of their absolute safety, though this was 10 years earlier:

All nuclear weapons have some type of command and control mechanism which is designed to preclude unauthorized use, and all nuclear weapons are equipped with safety devices that meet rigid standards.... With regard to enemy capture of a nuclear weapon, similar safety and security devices thwart the arming, fusing, and firing of the weapon, particularly if the enemy has little or no knowledge of the mechanical or electro-mechanical operation of the protective device. It is possible, however, that these mechanisms can be defeated by a sophisticated enemy over a period of time.

Thus, emergency destruction devices and procedures have been developed so that nuclear weapons may be destroyed without producing a nuclear yield in the event that enemy capture is threatened.

The Permissive Action Link (PAL) Program consists of a code system and a family of devices integral or attached to nuclear weapons which have been developed to reduce the probability of an unauthorized nuclear detonation.

It was almost certainly possible to bypass early PALs:

A technical solution to the issues raised by the Joint Committee on Atomic Energy was jointly worked out by the Sandia and Los Alamos Laboratories. The concept was to embed a mechanical or electromechanical code switch in the warhead in a location such that it could not be bypassed readily. To foil any attempt to bypass the device, the switch's appearance and markings were disguised to make its function unclear unless the weapon's manual were also available.

PALs are physically integrated with the bombs:

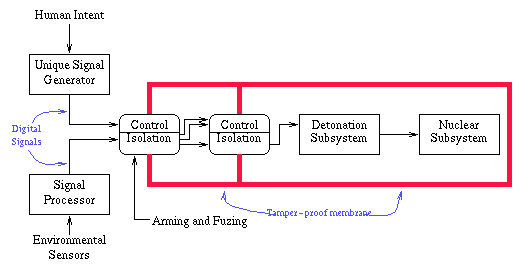
Initially, PAL were simply attached to the electrical circuitry of nuclear weapons. Weapons designers recognized that it would be relatively easy to "wire around" these early PAL and they subsequently "buried" the PAL devices deep inside the weapon, making them virtually inaccessible to anyone trying to arm a weapon without authorization. In addition, weapons designers of more recent PAL have encapsulated the entire nuclear weapon or the PAL with a protective skin. Any penetration of this covering results in automatic, irreparable damage to the weapon, making it impossible to detonate.

We must distinguish between a *safety* mechanism and a *security* system. The former is designed to prevent accidental detonations; the latter is designed to resist a determined adversary.

Unique signals are safety mechanisms. The High Energy Weapons Archive says that the current unique signal uses "digital communications and codes". Earlier unique signal generators used a signal of a type that did not occur elsewhere in the weapon, and was unlikely to arise by accident. For example, describes a train of square waves generated by a wind-up device. Among the (surprising) conclusions of this analysis are that keyboard input does not meet the safety and reliability requirements -- using, say, hexadecimal digits is unsafe; asking the user to type 24 bits is unreliable. (Modern unique signal generators use a 24-bit input, and lock up if an erroneous bit is entered. Some older designs have a "reset" signal, and hence permit multiple tries; these use 47-bit input sequences.) Remarkably, the unique signal is usually considered *unclassified*, which is pretty good evidence that it's not part of a security mechanism.

If a keyboard isn't used, what is? The suggested mechanisms rely on an operator physically inserting something -- a ROM key, a bar code, etc. -- into a reader.

The safety mechanisms are shown in the following schematic:



Drell strongly supports the notion that PALs protect the digital signal path:

The Enhanced Nuclear Detonation Safety System (ENDS) is designed to prevent arming of nuclear weapons subjected to abnormal environments. The basic idea of ENDS is the isolation of electrical elements critical to detonation of the warhead into an exclusion region, which is physically defined by structural cases and barriers that isolate the region from all sources of unintended energy. The only access point into the exclusion region for electrical power for normal arming and firing is through special devices called strong links, which cover small openings in the exclusion barrier.

The strong links are designed so that there is an acceptably small probability that they will be activated by stimuli from an abnormal environment. Detailed analyses and tests give confidence over a very broad range of abnormal environments that a single strong link can provide isolation for the warhead to better than one part in a thousand.

Therefore, the stated safety requirement of a probability of less than one in a million requires two independent strong links in the arming set, and that is the way the ENDS system is designed. Both strong links must be closed electrically -- one by specific operator-coded input and one by environmental input corresponding to an appropriate flight trajectory -- in order for the weapon to be armed.

There are several powerful principles here. First and foremost, a bomb will not detonate unless sufficient electricity reaches the detonators. If you can block that -- and there are two strong links, either one of which can do so -- you've rendered the bomb harmless. Consequently, a good design principle for a PAL is one that blocks the current flow.

It is also reasonable to suspect that the switches are mechanical in operation, rather than electrical. An electrical switch could more easily be closed by accident, if a stray piece of metal were to short-circuit a pair of wires. Furthermore, if the PAL does indeed operate the switch, a rotor-like configuration is ideal. There are many possible settings, and no simple contact closure will produce a current path. In fact, given that Drell notes that each gate has one chance in 103 of failing, it is tempting to conclude that three digits of the PAL code are used to arm each gate. (The environmental sensor gate, then, would be operated by a combination of PAL input and trajectory data.) That is clearly an oversimplification, though; the gates have to resist accidents, including fires and impacts, as well.

The simplicity of the design carries with it a corresponding price, however: it implies a lot of reliance on the protective barrier. Someone who could breach the barrier without activating the safety mechanisms could indeed bypass both the PAL and the environmental sensors. Furthermore, this barrier must also be resistant to enemy attempts to induce bomb failures. To give just one example, X-rays, which could be used in an attempt to probe the barrier, are one form of threat that the protective structure senses, and hence one that could presumably lead to a self-destruct sequence. But X-rays have also been considered as a defensive measure against nuclear weapon attacks. Indeed, bombs release much of their energy as X-rays.

If this guess at a design is correct, the rotor settings are the actual cryptographic key. Presumably, these are rarely changed -- one would have to open the sealed environment to do so. But the settings could be encrypted in an external PAL key; this in turn could easily be changed by a microcomputer embedded inside the bomb's protective skin.

**Other Design Ideas**

There are many other possible approaches to a PAL design. For example, in modern bombs the pit is "levitated" inside the ball of high explosives. Perhaps the placement of the pit can be varied in three dimensions. A seriously off-center pit won't detonate properly. On the other hand, a "fizzle yield" or plutonium dispersal are still serious matters; this approach may not offer enough safety.

Another possibility is changing the timing of the "initiator". The initiator supplies the initial neutrons to start the chain reaction; in a modern bomb, this is done by an electronic device. Hansen notes that this is a critical parameter, and can act as a failsafe device. But it isn't clear that this is reliable enough to be use for PALs; there is a moderately high probability of neutrons being present from spontaneous fission, especially of Pu-240. A chain reaction started by stray neutrons wouldn't have nearly as high a yield, but it would still be significant. (In a related vein, Hansen also notes that the timing of the injection of a deuterium-tritium "booster" into the center of the pit is critical to the yield of the weapon. If this timing is controlled by the PAL, the enabling code can vary the damage done by the weapon, as mentioned earlier.)

Given that earlier PALs seem to work by interrupting the high voltage supply, it is tempting to try to build on this principle but with stronger cryptographic backing. Bombs get their high voltage detonation current from a bank of capacitors; these in turn are charged from batteries. A typical battery-driven charging circuit -- as is incorporated into ordinary electronic flash units -- works by pulsing the battery's DC output and feeding that into a transformer. The output of the transformer is fed to the capacitors. Suppose that the frequency of the pulses is controlled by a microprocessor, with a narrow bandpass filter between its output and the transformer.

The pulse frequency would have to be just right for the charging circuit to work. Better yet, have several filters switched in and out of the circuit by the microprocessor, which of course would switch the pulse frequency accordingly. If the timing and frequency information were encrypted using the PAL as a key, it would be improbable that the capacitor would be charged. One could add a few more wrinkles, such as a computer-controlled drain circuit and closely matching the battery's maximum output to the necessary charge values.

It is quite unclear if this scheme can be made to work. If nothing else, the circuit is quite involved, and would require careful analysis. Furthermore, the high-voltage circuit components are of necessity outside the tamper-resistant barrier; it might be too easy to wire around them. Finally, building a high-voltage power supply is a relatively easy task; an enemy who gained possession of a nuclear weapon might be able to replace those circuits entirely.

Finally, actual sections of microprocessor code could be encrypted. If the essential detonation sequence is complex enough, and in particular if it relies on decisions made by the microprocessor in response to actual conditions in the bomb, this would be a powerful defense. The unknown question, of course, is whether or not an adequate yield could be obtained by a much simpler control mechanism. Also note that the decryption key would have to be present in the actual code. Suitable reverse engineering of the code would reveal this key.

**PALs and Key Management**

A reference and an Air Force Document suggest that PALs are rekeyed periodically. Furthermore, at least some Air Force bases regularly have PAL keys on hand, albeit (apparently) in encrypted form; these are among the highest priority items that must be destroyed in event of an emergency.

It is reasonably probable that public key cryptography is not used directly. No known public key cryptosystem uses keys as short as 6 or 12 digits. (Of course, the lack of any visible plaintext or ciphertext might thwart most cryptanalysts...) Feaver repeatedly points out the difference between the *enabling message* -- the PAL unlock code -- and the *authorization message* -- the message from the National Command Authority authorizing the use of nuclear weapons.

Public key cryptography might be used in the overall command and control system. The code values carried by the President are identification and authentication information, not PAL codes themselves. (There have been accidents with the custody of these, too. Carter's codes were left in some clothing that was sent to the dry cleaners; Reagan's were inadvertently taken by the FBI (with his clothing) when he was in the hospital following the assassination attempt.)

There is a reasonably clear statement about the basic design principles of these codes in a Congressional hearing:

Now, I recall reading a few weeks ago that someone in our armed services who is in the nuclear chain of operation raised the question at an orientation session as to how they could be sure that the order to launch a nuclear strike in point of fact came from the President. After that, the person was removed from the program completely....

How do the people down the chain of command, who are the recipients of the Presidential order, know that the order, in fact, has come from the President, rather than an impostor?

Admiral Miller: We have incorporated in the release process not only the order to do the job, but an elaborate, highly secure, coded authentication system, where you not only get the order, but you get an authentication that the order is valid.

That prevails all the way down the line, actually almost to the weapon itself. In some instances, that technique exists right at the weapon.

That's as good a requirements statement for digital signatures as you're going to get, especially from an admiral talking to a Congressional committee in 1976, when public key cryptography had not yet been reinvented by the civilian community. (Clearly, there are other cryptographic techniques that could be used, most notably one-way hashing of passwords -- an idea that was publicly known at the time. But most of these are vulnerable to replay attacks, especially given the offline nature of an authorization order.)

A counter-argument against use of digital signatures for such purposes is their length. Some of the radio systems used or contemplated for Emergency Action Messages (EAMs) are extremely low bandwidth. Extremely Low Frequency (ELF) radio is restricted to about one bit per *minute* after error correction; Very Low Frequency (VLF) operates at "slow teletype speeds".

The actual PAL codes are in fact fairly widely disseminated, though not to the level of individual weapons commanders. The authorization codes are much more tightly held, though the extent of the delegation is classified. Recently declassified documents confirm that the president has in fact delegated such authority.

There is clearly a place here for sophisticated key management techniques. Cotter suggests that such are used:

Distributing codes too widely could compromise control. Holding the codes at too few locations could compromise survivability under enemy attack. Force survivability was given high priority. The management scheme, devised by Defense Department communications security experts, allows great flexibility in code passing and in recall of control during and after a crisis subsides.

**The Bottom Line -- How do PALs Work?**

From the open literature, it is impossible to come to any definite conclusions. It seems clear, though, that there is no single mechanism in use. PALs that one could build today would be vastly different than those deployed in 1962.

My guess is that the CAT A, B, C, and D PALs were, in effect, electromechanically-operated devices similar to the rotor mechanism described earlier. Most likely, they interrupted the high voltage path. They were definitely electromechanical, and I doubt very much that mid-60's technology would have permitted an electronic encryption-based design.

CAT F is at least partially electronic. The design principle appears to be control of the detonator current, coupled with the tamper-resistant barrier. I have found no evidence to support any of the hypotheses involving encrypted code or timing information. These remain the best bet for an inherently safe PAL design, however, and Cotter does hint that CAT F -- unlike earlier models -- is inherently impossible to bypass. He also says "electronic information processing based on crypto-logical techniques was incorporated in the coded switch and controller circuitry." It seems plausible that control of the D-T pump timing and the initiator are encrypted timing signals; doing so would be very straight-forward, and would provide a strong control over total yield of a stolen bomb, if not necessarily over actual detonation.

**Why are PALs Classified?**

As noted, it is hard to find authoritative technical descriptions of how PALs work. Admiral Miller repeatedly declined to be more precise in his testimony, citing the "highly classified" nature of the material. But from whom are the secrets being kept? There is ample evidence that the U.S. offered design details on PALs to other nuclear powers. The rationale, of course, was to help these countries control their own nuclear weapons. The first approach to the Soviet Union was as early as 1971 (they weren't interested, though they never had PALs of their own; they relied on ``people watching people who watched still other people''. On the other hand, a former Soviet general implies that at some point, the Soviets did have technical control measures of some sort.

This suggests one of two possibilities. First, and most intriguing, the design of PALs may be so closely tied to the design of nuclear weapons that revealing the former gives hints on the latter. Nothing I've seen supports this theory, but it is possible. Second, the incremental risk if a U.S. nuclear weapon is compromised by another nuclear power is comparatively small. But a non-nuclear power -- or group -- would benefit greatly from anything that improved their odds of using someone else's bombs.

If, however, my guesses about the design are correct, PALs per se have little that is sensitive. But the tamper-resistant skin is another matter.