

# Utajnianie bez wysiłku

## Nowe układy kryptograficzno-uwierzytelniające firmy Atmel

*Kryptografia, stanowiąca do niedawna domenę operacji szpiegowskich czy wojskowych, wkroczyła do życia codziennego. Korespondencja biznesowa, operacje bankowe, wymiana jakichkolwiek dokumentów muszą być chronione przed niepowołanym dostępem, a ich autor musi być wiarygodny. Dotychczas służył temu, nawet nieczytelny, zawijas pod dokumentem lub pieczęć – świadectwa autentyczności dokumentu.*

Obecnie kryptografia, przy powszechnej elektronicznej obiegu informacji, jest szeroko stosowana, nawet poza naszą świadomością. Bez kryptografii nie byłoby bowiem telefonów komórkowych, bankowości internetowej, bankomatów czy kodowanej telewizji cyfrowej.

Uwiarygodnienie nadawcy wysyłanych dokumentów wymaga jakiegoś sposobu jego identyfikacji, do czego może służyć podpis elektroniczny lub inne charakterystyczne, niepowtarzalne cechy dokumentu – jego cyfrowe „streszczenie”, czyli wartość funkcji skrótu.

Najważniejszym zadaniem kryptografii jest szyfrowanie dokumentów i połączeń telekomunikacyjnych. Upraszczając, do tego celu stosuje się złożone algorytmy kryptograficzne, w tym symetryczne bądź asymetryczne. W algorytmach symetrycznych, używanych przy wymianie informacji, stosowany jest jeden klucz, ten sam do szyfrowania i deszyfrowania wiadomości. Służy on do ochrony danych przed nieuprawnionym odczytem. Dostęp do dokumentu mają tylko dysponenti pilnie strzeżonego klucza, który musi być gdzieś przechowywany i udostępniany adresatowi. Jest z tym związane pewne ryzyko ujawnienia klucza, a więc w znacznym stopniu ograniczona jest skuteczność takiej ochrony danych przez szyfrowanie. Dane po zaszyfrowaniu są przesyłane w postaci kryptogramu, który może być odczytany tylko przez posiadającego klucz, którym zostały zaszyfrowane.

W algorytmach asymetrycznych do szyfrowania i deszyfrowania są stosowane dwa różne klucze, z których jeden jest jawny (publiczny), a drugi niejawny (prywatny). Służą one do uwierzytelniania dokumentów oraz ochrony prywatności korespondencji elektronicznej.

Jeżeli dokument zaszyfrowany utajnionym kluczem prywatnym może być odczytany jawnym kluczem publicznym (skojarzonym z prywatnym i wynikającym z niego), to świadczy, że kryptogram był utworzony tylko przez posiadającego klucz prywatny, a tym samym uwiarygodniony jest autor dokumentu.

Jeżeli natomiast dokument będzie zaszyfrowany kluczem publicznym (nie jest już skuteczny przy deszyfrowaniu), to prawidłowo można odczytać taki kryptogram tylko za pomocą klucza prywatnego. Nieuprawniony ciekawski nie odczyta go, czyli próba odczytania takiej korespondencji przez osoby trzecie jest niemożliwa bez ujawnienia klucza prywatnego.

W przypadku, gdy chcemy dodatkowo potwierdzić autentyczność dokumentu bez ujawniania jego treści bądź chcemy zagwarantować integralność dokumentu (wykręć jego zmodyfikowanie), to możemy dołączyć do dokumentu jego charakterystyczny, unikatowy skrót w postaci ciągu znaków, innego dla każdego dokumentu. Taki skrót jest obliczany za pomocą jednokierunkowej funkcji haszującej (hash function – mieszającej), której wynik powstaje jednoznacznie na podstawie dokumentu, którego dotyczy. Jednak na podstawie tego skrótu nie można odtworzyć dokumentu źródłowego.

Gdy wynik obliczenia wartości funkcji skrótu składa się na przykład ze 128 albo 256 bitów, to liczba możliwych wartości skrótu jest niewyobrażalnie olbrzymia:  $2^{128}$  albo  $2^{256}$  ( $1,16 \times 10^{77}$  – wynik 78-cyfrowy!). Należy zwrócić uwagę, że okres istnienia Wszechświata szacuje się na  $2^{61}$  sekund, natomiast  $2^{256}$ , to jest większa liczba niż atomów, z których zbudowane jest Słońce.

W praktyce używanych jest wiele funkcji haszujących. Wśród nich jest rodzina funkcji



SHA (Secure Hash Algorithm), w tym ostatnio SHA-2 z długością skrótu liczącą do 512 bitów.

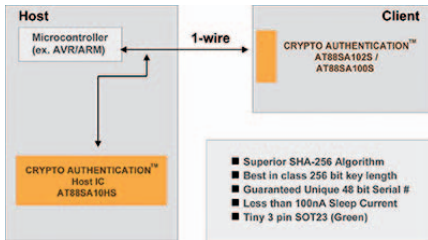
Kontrolowanie wartości funkcji skrótu, obliczonej na danym pliku (programie, zbiorze danych, transakcji bankowej) umożliwia łatwe sprawdzenie autentyczności postaci pierwotnej programów komputerowych czy innych ważnych biznesowo dokumentów. Ich zmodyfikowanie czy doklejenie do nich wirusów może być łatwo wykryte przez kontrolowanie właśnie wartości funkcji skrótu. Jakakolwiek manipulacja na pierwotnym pliku źródłowym zostanie wykryta, gdyż zmiana chociażby jednego bitu w pliku pierwotnym spowoduje gruntowną zmianę wartości funkcji skrótu.

### A może wyspecjalizowane układy scalone?

W większości przypadków powyższe metody ochrony korespondencji są realizowane programowo. Aby je stosować trzeba mieć chociaż podstawową wiedzę o kryptografii oraz przygotować odpowiednie oprogramowanie. Dla przeciętnego użytkownika zadanie nie jest łatwe, to trochę „wyższa szkoła jazdy”. A gdyby tak układy scalone, które sprzętowo same załatwią takie problemy? Oczywiście, można znaleźć przykłady implementowania w układach scalonych (przejdźmy także programowalnych) różnych algorytmów kryptograficznych, w tym także odpornych na kryptoanalizę algorytmów komunikacyjnych DES (Data Description Standard) i AES (Advanced Description Standard).

Innym problemem (poza ochroną korespondencji), z jakim borykają się producenci różnego rodzaju urządzeń jest ich ochrona przed podmianą nieoryginalnych podzespołów eksploatacyjnych. Do tego celu opracowano układy tworzące system identyfikacji:





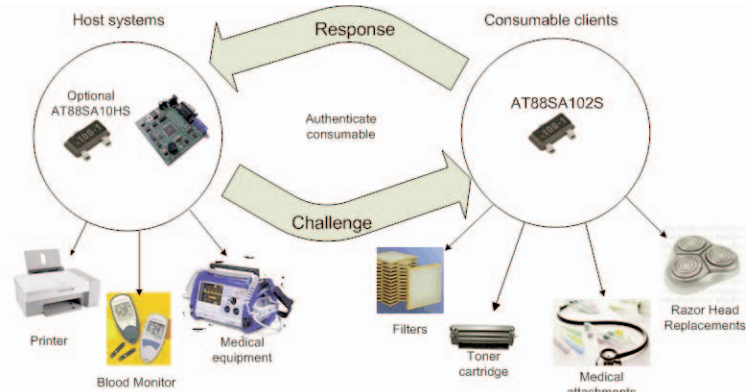
Rys. 1. Schemat blokowy użycia układów hosta i klienta

swój czy obcy, zapewniające niezawodną identyfikację oryginalnych podzespołów dołączanych do urządzenia. Do tej grupy układów kryptograficzno-uwierzytelniających zalicza się więc układy potwierdzające oryginalność dołączanych do urządzenia zużywających się części wymiennych, na przykład akumulatora czy kasety z tonerem. Takie układy do potwierdzenia autentyczności dołączanych podzespołów (oryginalny czy podróbka) oferują różne firmy, w tym Maxim i Texas Instruments. Jednym z takich układów jest na przykład DS2703 firmy Maxim, silny kryptograficznie układ uwierzytelnienia pakietów bateryjnych Li-Ion do telefonów, PDA, i laptopów. Do tych firm dołączyła firma Atmel oferując układy scalone, za pomocą których można tworzyć systemy kryptograficzno-uwierzytelniające bez gruntownej wiedzy z zakresu kryptografii. Trzeba tylko skorzystać z not aplikacyjnych opisujących ich użycie.

### Co oferuje Atmel?

W ubiegłym roku Atmel zapowiedział produkcję układów scalonych dla systemu kryptograficzno – uwierzytelniającego (CryptoAuthentication) typu „plug-and-play”, umożliwiające projektantom zastosowanie w swoich projektach gotowego systemu autoryzacji, bez jakiegokolwiek znajomości protokołów bezpieczeństwa, ich algorytmów i konieczności przygotowywania oprogramowania kryptograficznego. Na system składają się dwa układy. Pierwszy jest przeznaczony dla urządzenia nadrzędnego z procesorem sterującym (hosta) – to jest układ AT88SA10HS instalowany w urządzeniu uwierzytelniającym. Drugi układ jest przeznaczony do urządzenia uwierzytelnianego (klienta) – jest to układ AT88SA102S (rys. 1). Umożliwiają one utworzenie systemu zabezpieczającego urządzenie główne (np. kamerę, telefon, drukarkę itp.) przed instalowaniem w nich nieoryginalnego wyposażenia (np. baterii, kasety) czyli mówiąc kolokwialnie wszelkiego rodzaju podrób. W ten sposób mogą być łatwo i tanio chronione prawa autorskie do wyrobu wraz z jego wyposażeniem. Jednak nie tylko w tym celu można zastosować te układy.

Układ AT88A10HS wraz z jakimkolwiek procesorem, jest instalowany po stronie uwiarygodniającego hosta, natomiast układ



Rys. 2. Konfiguracja systemu do identyfikacji oryginalnego wyposażenia urządzenia

AT88A102S jest instalowany w urządzeniu uwiarygodnianym (które jest autoryzowane) – to jest po stronie klienta. Tym samym powstaje praktycznie niemożliwy do podejrzenia (ingerencji przez osoby nieuprawnione) system autoryzacji, ochrony poufności korespondencji i kontroli integralności dokumentów oraz potwierdzenia autentyczności oprogramowania.

Dotychczas autoryzacja po stronie hosta jest realizowana programowo, której kod jest wykonywany przez system mikroprocesorowy. Ten kod jest narażony na kopiowanie lub modyfikowanie, gdyż jest przechowywany w zewnętrznej pamięci, trudnej do zabezpieczenia przed odczytem, chociaż Atmel już oferuje takie pamięci. Układy kryptograficzno-uwierzytelniające Atmela umożliwiają tworzenie tanich systemów, które zawierają utajniony klucz pamiętany w zabezpieczonym obszarze specjalnej pamięci. Po stronie hosta jest to układ scalony z unikatowym, 48-bitowym numerem seryjnym, układem generacji funkcji skrótu SHA-256 i 256-bitowym kluczem do szyfrowania układu hosta, który jest niedostępny na zewnątrz i niemożliwy do odczytania. Układ AT88A10HS realizuje wszystkie operacje jakie muszą być wykonane po stronie hosta, włączając w to: zapytanie i przyjęcie odpowiedzi, walidację (potwierdzenie autentyczności) oraz weryfikację integralności oprogramowania. Współpracujące z nim układy AT88A102S albo (xx100S) są w pełni bezpiecznymi układami autoryzacji z wbudowanymi układami generacji funkcji skrótu SHA-256 oraz 256-bitowym kluczem kryptograficznym.

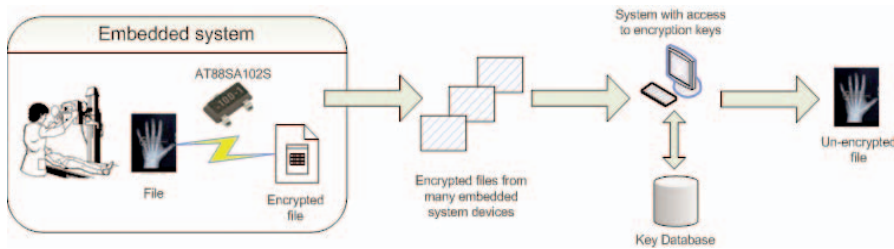
Układ po stronie hosta (AT88A10HS) zawiera również 63-bitową pamięć programowalną jednokrotnie przez użytkownika, zbudowaną z łączników przepalanych (fuse), które umożliwiają zapamiętanie indywidualnego identyfikatora układu (jego indywidualizację) oraz 23 łączniki fuse, które mogą być użyte do zapamiętania informacji o statusie bądź modelu urządzenia. Ponieważ te elementy pamiętające mogą być tylko jednokrotnie i nieodwracalnie przepalane, to niemożliwe jest skasowanie zapamiętanych w tej pamięci informacji.

### Przykłady zastosowań

**Swój czy obcy – potwierdzenie autentyczności wyposażenia.** Po wbudowaniu układu AT88SA102S w podzespół eksploatacyjny (kaseeta z tonerem, wyposażenie jakiegoś urządzenia medycznego) można zapewnić ochronę swoich interesów przed jego niepożądaną podmianą. Wysyłając zapytanie z mikrokontrolera sterującego urządzeniem głównym można łatwo potwierdzić autentyczność wyposażenia. Bezpieczna indywidualizacja podzespołu może być realizowana za pomocą 62-bitowej, jednokrotnie programowalnej pamięci z łącznikami przepalnymi (fuse). Dodatkowy poziom bezpieczeństwa może być zapewniony przez użycie układu AT88SA10HS hosta. W tym układzie jest bowiem zawarty sekretny klucz pamiętany sprzętowo, a nie w kodzie źródłowym mikroprocesora, co czyni go bardziej bezpiecznym, a nawet niemożliwym do złamania. Na rys. 2 zilustrowano takie użycie układu klienta do potwierdzenia oryginalności elementu wyposażenia (jego autoryzacji).

Autoryzacja jest oparta na protokole zapytanie/odpowiedź, który jest realizowany przez mikroprocesor hosta. Nawiązuje on komunikację i przesyła zapytanie do autoryzowanego układu podrzędnego (klienta). Na podstawie jego odpowiedzi jest określone czy klient jest autentyczny.

Na początku transakcji (rozpoczęcie procesu autoryzacji), procesor hosta odczytuje numer seryjny układu AT88SA102S klienta. Ten numer jest przesyłany do układu AT88SA10HS hosta, który oblicza wartość funkcji skrótu SHA-256 w oparciu o swój (hosta) 256-bitowy klucz, numer seryjny klienta i wygenerowany przez mikrokontroler numer losowy (losowy ciąg znaków). Host także wysła do klienta wygenerowany (ten sam) numer losowy jako zapytanie. W odpowiedzi układ klienta AT88SA102S wykonuje obliczenia wartości funkcji skrótu SHA-256 na podstawie numeru losowego przesłanego przez hosta, swojego numeru seryjnego oraz 256-bitowego klucza klienta. Ten skrót, jako odpowiedź, jest przesyłany z powrotem do AT88A10HS przez procesor hosta, który następnie porównuje wartość



Rys. 3. Konfiguracja systemu do szyfrowania dokumentów

odpowiedzi z wartością wcześniej obliczonej funkcji skrótu i podejmuje decyzję czy klient jest autentyczny czy nie. Dzięki temu, że mikroprocesor hosta generuje przy każdym zapytaniu nowy numer losowy dla każdej transakcji, to przechwycenie pary danych (zapytanie i odpowiedź) przesyłanych tam i z powrotem jest nieużyteczne, ponieważ każde nowe zapytanie, jest generowane z nowym numerem losowym. Układ klienta może być konfigurowany z pojedynczym kluczem dla serii produktów lub z unikatowym kluczem dla każdej jednostki produktu. Nie jest możliwe odczytanie tego klucza, bo nie jest on transmitowany na zewnątrz i jest zawsze utajniony w układach uwierzytelniających hosta i klienta.

**Weryfikacja oprogramowania.** Sprawdzenie czy oprogramowanie albo inne dokumenty nie zostały zmienione, jest w wielu przypadkach bardzo ważne i może być z łatwością zrealizowane również za pomocą układu AT88SA10HS hosta. Mikrokontroler wyznacza wartość funkcji skrótu dokumentu czy kodu programu stosując algorytm SHA-256 i przesyła wynik wraz z pamiętaną sygnaturą dokumentu (programu) pierwotnego do układu kryptograficzno-uwierzytelniającego AT88SA10HS, który oblicza oczekiwaną sygnaturę dokumentu w oparciu o wartość funkcji skrótu i 256-bitowego klucza. Integralność dokumentu jest potwierdzona, gdy wynik obliczeń jest zgodny z sygnaturą pamiętaną razem z dokumentem.

**Ochrona plików przez ich szyfrowanie.** Układ AT88SA102S umożliwia łatwe zabezpieczenie przesyłanych dokumentów. Zabezpieczany plik może być szyfrowany za pomocą symetrycznego algorytmu, na przykład AES lub DES. Mikroprocesorowy system sterujący generuje losowy numer i przesyła go do AT88SA102S jako zapytanie. Następnie używa odpowiedzi od tego układu do szyfrowania utajnianego pliku. Zasyfrowane pliki i losowe zapytania mogą być zatem transmitowane poprzez publiczne media. Aby odczytać (rozszyfrować) odebrany plik, to po stronie odbierającej musi być znany klucz z układu AT88SA102S, który posłużył do szyfrowania. W tym celu system odbierający, na podstawie losowego zapytania przesłanego z plikiem i indywidualnego klucza układu AT88SA102S strony nadającej (niestety musi

go mieć w bazie danych), oblicza za pomocą algorytmu SHA-256 wartość funkcji skrótu. Następnie skrót ten jest używany jako klucz do rozszyfrowania otrzymanego pliku. Szyfrowane pliki mogą mieć ten sam klucz lub każdy plik może mieć unikatowy klucz. Na rys. 3 pokazano konfigurację, w której układ kryptograficzno – uwierzytelniający AT88SA102S jest po stronie nadającej systemu transmitującego zasyfrowane pliki. Należy tu podkreślić, że algorytm szyfrujący jest realizowany przez procesor po stronie nadającej, a układ uwierzytelniający dostarcza tylko bezpiecznego klucza.

**Ochrona przed klonowaniem oprogramowania.** Oprogramowanie stosowane w systemach mikroprocesorowych jest często kopiowane lub zmieniane przez fałszerzy. Autorzy oryginalnych rozwiązań poszukują więc taniego i skutecznego sposobu ochrony swojego oprogramowania przed fałszerzami lub klonowaniem przez konkurencję. W tym celu do ochrony można użyć, jako lokalnego (na płytce) układu kryptograficzno-uwierzytelniającego, właśnie układu AT88SA102S współpracującego z mikroprocesorem. W losowo określanych przedziałach czasu mikrokontroler wysyła zapytanie do układu AY88SA102S. Odpowiedź z tego układu jest następnie porównywana z odpowiedzią oczekiwaną. W przypadku niezgodności zawieszane jest działanie programu. Przy dostatecznie dużej liczbie zapytań i umieszczeniu ich w różnych miejscach kodu źródłowego, program może być relatywnie dobrze chroniony. Taki mechanizm ochrony stwarza bowiem duże utrudnienie dla kopiującego, uniemożliwiające łatwe odtworzenie kodu źródłowego. To utrudnienie może być także zbyt kosztowne do omińnięcia dla konkurencji, co skłoni ją raczej do opracowania swojego oprogramowania, zamiast modyfiko-

wania istniejącego kodu. Konfigurację takiego systemu zabezpieczenia zilustrowano na rys. 4.

**Właściwości układów systemu**

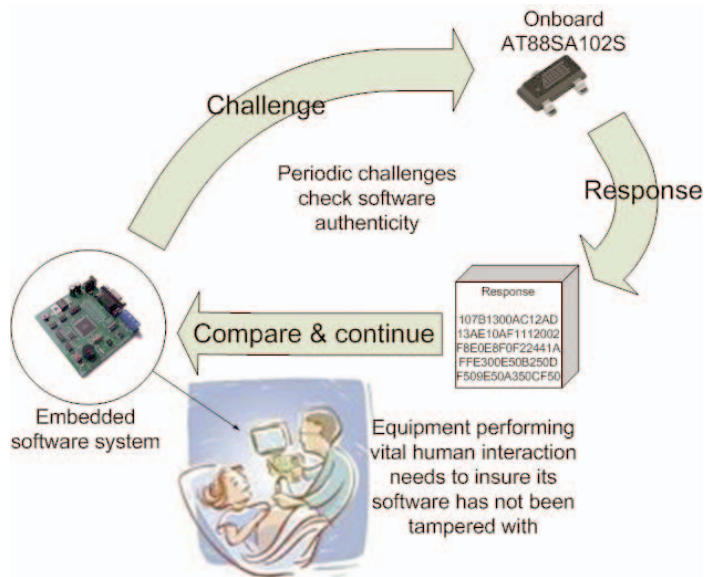
W układach scalonych systemu uwierzytelniającego, zarówno po stronie hosta jak i klienta, stosowane są liczne mechanizmy zabezpieczające klucz i inne dane indywidualnie. Wśród nich jest ekran nad całą powierzchnią układu. Zarówno sygnał zegarowy jak i zasilanie układów logicznych jest generowane wewnętrznie, co uniemożliwia jakiegokolwiek bezpośredni atak poprzez wprowadzenia tych dwóch sygnałów. Zaprogramowane w układzie AT88AS10HS klucze są w taki sposób, że odczytanie ich wartości poprzez zewnętrzną analizę jest praktycznie niemożliwe.

Układ uwierzytelniający jest aktywny przez 1/1000 procenta swojego czasu włączenia, a więc jest przede wszystkim w stanie uśpienia, w którym pobór energii jest nieznaczny. W tym stanie pobiera on mniej niż 100 nA prądu, co praktycznie nie wpływa na czas życia baterii zasilającej, gdyż zazwyczaj prąd upływu baterii jest znacznie większy. Napięcie zasilania układów tej rodziny wynosi od 2,5 do 5,5 V.

Atmel zapewnia bezpłatną bibliotekę oprogramowania w celu łatwego zestawienia systemu. Chociaż kody źródłowe są w pełni sprawdzone dla mikrokontrolerów AVR ARM, to prawdopodobnie mogą być także zastosowane do innych mikrokontrolerów. Układ od strony hosta wymaga tylko pojedynczego wprowadzenia mikroprocesora, które może być współdzielone, zarówno przez układ hosta jak i klienta. Do połączenia tego układu z układem klienta potrzebne są tylko trzy linie.

Gdy zamówimy ponad 1000 sztuk, to obecnie zapłacimy za komplet (host-klient) mniej niż 1,5\$. Próbkę można zamówić bezpłatnie.

JJP



Rys. 4. Konfiguracja systemu ochrony przed klonowaniem