RZECZPOSPOLITA POLSKA

Urząd Patentowy Rzeczypospolitej Polskiej

(12) **OPIS PATENTOWY** (19) **PL** (11) **227584**

(13) **B1**

(21) Numer zgłoszenia: **402548**

(22) Data zgłoszenia: **25.01.2013**

(51) Int.Cl.
G06F 21/62 (2013.01)
H04L 9/08 (2006.01)

(54) **Sposób i układ do selektywnej dystrybucji kluczy grupowych z dynamicznym wykluczaniem członków grupy**

(43) Zgłoszenie ogłoszono:
04.08.2014 BUP 16/14

(45) O udzieleniu patentu ogłoszono:
31.01.2018 WUP 01/18

(73) Uprawniony z patentu:
AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE, Kraków, PL

(72) Twórca(y) wynalazku:
PIOTR PACYNA, Kraków, PL
TOMASZ RAMS, Kraków, PL

PL 227584 B1

Opis wynalazku

Przedmiotem wynalazku jest sposób selektywnej dystrybucji kluczy grupowych z dynamicznym wykluczaniem członków grupy oraz układ do selektywnej dystrybucji kluczy grupowych z dynamicznym wykluczaniem członków grupy. Wynalazek dotyczy dziedziny telekomunikacji, w szczególności kryptografii i aparatury dla celów wymagających tajemnicy.

Komunikacja grupowa może być chroniona przy użyciu efektywnych, wydajnych obliczeniowo technik opartych na współdzielonym, symetrycznym kluczu grupowym. Niestety, raz ustanowiony klucz powinien podlegać okresowej wymianie w celu przeciwdziałania próbom kryptoanalizy. Także w przypadku zmiany składu grupy klucz powinien podlegać natychmiastowej wymianie, aby nie narazić komunikacji w obrębie grupy na utratę bezpieczeństwa. Wynalazek umożliwia wymianę klucza grupowego oraz dynamiczne wykluczanie z grupy jak i dołączanie do grupy nowych urządzeń przy utrzymaniu ochrony komunikacji w obrębie grupy uwzględniającej aktualny na daną chwilę skład grupy. Przyjmując, że sesja jest to taki okres czasu, w trakcie którego skład grupy pozostaje niezmienny, może być stosowany jeden, obowiązujący na daną chwilę współdzielony, grupowy klucz sesyjny. W dalszym opisie i zastrzeżeniach klucz grupowy należy rozumieć jako grupowy klucz sesyjny.

Z artykułu autorstwa M. Naor i in., Efficient Trace and Revoke Schemes, opublikowanego przez Springer w serii "Lecture Notes in Computer Science" w tomie: Vol. 1962, 2001, strony 1–20, w materiałach z konferencji International Conference on Financial Cryptography (FC '00), 2000, znany jest sposób i system dystrybucji kluczy grupowych z dynamicznym wykluczaniem urządzeń użytkowników. W rozwiązaniu tym na początku każdej sesji menedżer grupy wysyła wiadomość rozsiewczą zawierającą zaszyfrowany klucz grupowy do urządzeń użytkowników. Następnie, urządzenia użytkowników deszyfrują otrzymany szyfrogram przy użyciu swoich kluczy personalnych. Klucze personalne są dostarczane w czasie inicjalizacji urządzeń użytkowników i pozostają niezmienne przez cały czas działania systemu. W przytoczonym rozwiązaniu klucz grupowy jest szyfrowany przy użyciu technik opartych na wielomianach i arytmetyce wykładniczej. Rozwiązanie to pozwala na wykluczenie z grupy pewnej z góry określonej liczby urządzeń użytkowników wciągu całego czasu działania systemu, przy czym rozmiar wiadomości rozsiewczej jest proporcjonalny do maksymalnej liczby urządzeń, które można wykluczyć.

Znany jest z opisu patentowego US nr 7313238 sposób i system zarządzania kryptograficznymi kluczami współdzielonymi. Patent ten opisuje system zarządzania kryptograficznymi kluczami współdzielonymi, przeznaczony do ochrony współdzielonego systemu plików, w którym kolejne wersje sekretnego klucza współdzielonego są ze sobą powiązane za pomocą pewnego rodzaju modyfikatora (rotation catalyst). Modyfikatory klucza współdzielonego są generowane za pomocą szyfrowania asymetrycznego, w taki sposób, że urządzenie użytkownika może łatwo wyliczyć poprzednie wersje modyfikatora z aktualnej wartości modyfikatora i dzięki temu może odzyskać brakujące klucze współdzielone bez konieczności interakcji z właścicielem plików, a zarazem dystrybutorem tych kluczy. Selektywna dystrybucja nowej wersji klucza współdzielonego wykorzystuje techniki oparte na wielomianach i arytmetyce wykładniczej oraz mechanizm Bulletin Board. W przywołanym wynalazku US chodzi o osiągnięcie właściwości *„self healing”,* czyli zdolności układu do odzyskiwania niedostarczonych kluczy na podstawie późniejszych wartości kluczy.

Znany jest też z opisu patentowego US nr 7400732 sposób i system dystrybucji kluczy grupowych, z dynamicznym wykluczaniem urządzeń użytkowników. W przykładowych realizacjach zaprezentowanych w opisie używane są techniki dystrybucji kluczy grupowych oparte na wielomianach dwóch zmiennych oraz techniki oparte na arytmetyce wykładniczej, polegające na przeniesieniu obliczeń na wielomianach dwóch zmiennych do wykładników potęg. Głównym przedmiotem przywołanego wynalazku jest mechanizm *„self healing”,* pozwalający na odtworzenie niedostarczonego klucza grupowego na podstawie dwóch wiadomości rozsiewczych: jednej odebranej przez urządzenie użytkownika w sesji wcześniejszej niż niedostarczony klucz oraz drugiej odebranej w sesji późniejszej. Klucz grupowy jest dzielony na dwie części (reprezentowane jako wielomiany), a następnie w każdej wiadomości rozsiewczej transmitowane są pierwsze części kluczy z wszystkich przyszłych sesji oraz drugie części kluczy z wszystkich przeszłych sesji. Poprawne odebranie wiadomości rozsiewczych z dwóch różnych sesji pozwala na odtworzenie wszystkich kluczy z sesji występujących pomiędzy tymi dwoma.

Sposób, według wynalazku, polega na rozsyłaniu w czasie sesji poprzez sieć telekomunikacyjną zaszyfrowanego klucza grupowego z urządzenia menedżera grupy do urządzeń użytkowników i

deszyfrowaniu szyfrogramu tego klucza grupowego w urządzeniach użytkowników przy użyciu kluczy personalnych.

Istotą jest to, że w każdej sesji w urządzeniu menedżera grupy dodatkowo w generatorze modyfikatorów, będącym procesorem zawierającym generator liczb pseudolosowych, generuje się modyfikatory kluczy personalnych. Szyfruje się je za pomocą szyfratora modyfikatorów, zrealizowanego jako programowalny układ logiczny lub procesor lub układ ASIC, wykorzystując dane z pamięci danych maskujących grupy i rozsyła się do urządzeń użytkowników. W urządzeniu użytkownika deszyfruje się odebrany szyfrogram modyfikatorów za pomocą deszyfratora modyfikatora, wykonanego jako programowalny układ logiczny lub procesor lub układ ASIC, wykorzystując dane z pamięci danych maskujących użytkownika i wartość dotychczasowego klucza personalnego z pamięci klucza personalnego pobranych w postaci sygnału zmodulowanego cyfrowego. Z użyciem modyfikatora tworzy się nowy klucz personalny przeznaczony do deszyfrowania szyfrogramów kluczy grupowych w przyszłych sesjach. Sygnał zmodulowany cyfrowy to sygnał dyskretny o odpowiednim poziomie napięcia elektrycznego reprezentującego wartości logiczne 0 lub 1.

Korzystnie jest gdy w urządzeniu menedżera grupy szyfrogram modyfikatorów kluczy personalnych, otrzymany przez zaszyfrowanie modyfikatorów kluczy personalnych z użyciem danych maskujących grupy z pamięci danych maskujących grupy, szyfruje się powtórnie kluczem grupowym w szyfratorze powtórnego szyfrowania. Szyfruje się za pomocą programowalnego układu logicznego lub procesora lub układu ASIC. W ten sposób otrzymuje się drugi szyfrogram. W urządzeniu użytkownika, w deszyfratorze powtórnego szyfrowania, najpierw deszyfruje się ten drugi szyfrogram wykorzystując klucz grupowy otrzymany z deszyfratora klucza grupowego, a następnie deszyfruje się tak otrzymany szyfrogram modyfikatorów kluczy personalnych w deszyfratorze modyfikatora przy użyciu danych z pamięci danych maskujących użytkownika. Deszyfrowania realizuje się za pomocą programowalnych układów logicznych lub procesorów lub układów ASIC.

Korzystnie, jeśli do szyfrowania klucza grupowego używa się technik opartych na arytmetyce wykładniczej, a do szyfrowania modyfikatorów używa się technik opartych na wielomianie wykluczającym realizowanych w szyfratorze kluczy grupowych i szyfratorze modyfikatorów. Szyfratory zrealizowane są jako programowalne układy logiczne lub procesory lub układy ASIC.

Dynamiczne wykluczanie realizowane jest przez unieważnianie kluczy personalnych należących do urządzenia użytkownika. Mechanizm ten opiera się na przeprowadzaniu w każdej sesji selektywnej modyfikacji kluczy personalnych. Urządzenie menedżera grupy generuje modyfikatory potrzebne do zmodyfikowania kluczy personalnych i przesyła je w wiadomości rozsiewczej do urządzeń użytkowników. Modyfikatory kluczy personalnych są przesyłane w formie zaszyfrowanej w taki sposób, że urządzenia użytkowników, które są wdanej sesji aktywnie wykluczane z grupy, nie są w stanie odczytać modyfikatora swojego klucza personalnego z odebranej wiadomości rozsiewczej. Nowy klucz personalny wyliczany przez urządzenie użytkownika, zależy od poprzedniej wartości klucza personalnego oraz od modyfikatora klucza. Dlatego, wystarczy uniemożliwić urządzeniu użytkownika, które chcemy wykluczyć z grupy, odebranie pojedynczego modyfikatora klucza personalnego, aby unieważnić jego klucz personalny we wszystkich przyszłych sesjach. Powtórne szyfrowanie zmusza użytkownika do korzystania z dwóch różnych kluczy przy próbie deszyfrowania uniemożliwiając nieuprawnionym użytkownikom dostęp do modyfikatorów.

Układ według wynalazku składa się z urządzenia menedżera grupy i urządzeń użytkowników połączonych poprzez sieć telekomunikacyjną. Urządzenie menedżera grupy zawiera interfejs administratora, generator kluczy grupowych, szyfrator kluczy grupowych, pamięć kluczy personalnych grupy, moduł nadawczy i moduł sterujący menedżera połączony ze wszystkimi modułami menedżera grupy. Układ w każdym urządzeniu użytkownika zawiera moduł odbiorczy, deszyfrator klucza grupowego z pamięcią klucza personalnego oraz interfejs odbiorcy klucza grupowego. Ponadto ma moduł sterujący użytkownika z interfejsem konfiguracyjnym połączony ze wszystkimi modułami urządzenia użytkownika.

Układ charakteryzuje się tym, że w urządzeniu menedżera grupy interfejs administratora, w postaci minikomputera z komunikacyjnym portem wejścia/wyjścia, przyłączony jest do modułu selekcji grupy, zrealizowanym na procesorze z pamięcią RAM. Z modułem selekcji grupy połączone są szyfrator kluczy grupowych i szyfrator modyfikatorów, a także pamięć urządzeń użytkowników. Z szyfratorem kluczy grupowych połączony jest też generator kluczy grupowych i pamięć kluczy personalnych grupy, a z szyfratorem modyfikatorów generator modyfikatorów i pamięć danych maskujących grupy. Dodatkowo generator modyfikatorów połączony jest z pamięcią kluczy personalnych grupy. Szyfrator

kluczy grupowych i szyfrator modyfikatorów połączone są z modułem nadawczym poprzez moduł przygotowania wiadomości, będący procesorem wyposażonym w pamięć RAM. W każdym urządzeniu użytkownika do modułu odbiorczego przyłączony jest deszyfrator klucza grupowego i deszyfrator modyfikatora, a oba połączone są z pamięcią klucza personalnego. Do deszyfratora modyfikatora dołączona jest też pamięć danych maskujących użytkownika. Deszyfrator klucza grupowego połączony jest z interfejsem odbiorcy klucza. Generator kluczy grupowych oraz generator modyfikatorów są procesorami zawierającymi generator liczb pseudolosowych. Szyfrator kluczy grupowych, szyfrator modyfikatorów, deszyfrator klucza grupowego i deszyfrator modyfikatora są programowalnymi układami logicznymi lub procesorami lub układami ASIC.

Korzystnym jest, gdy w urządzeniu menedżera grupy pomiędzy szyfratorem modyfikatorów, a modułem przygotowania wiadomości, w postaci procesora z pamięcią, włączony jest dodatkowo szyfrator powtórnego szyfrowania, który to szyfrator powtórnego szyfrowania ma połączenie z generatorem kluczy grupowych. Szyfrator powtórnego szyfrowania zrealizowany jest w postaci programowalnego układu logicznego lub procesora lub układu ASIC. W urządzeniu użytkownika pomiędzy modułem odbiorczym a deszyfratorem modyfikatora włączony jest deszyfrator powtórnego szyfrowania, zrealizowany w postaci programowalnego układu logicznego lub procesora lub układu ASIC, połączony z deszyfratorem klucza grupowego.

Zaletą rozwiązania jest to, że komunikacja w obrębie grupy pozostaje chroniona, mimo że dystrybucja klucza następuje przy użyciu mechanizmu rozgłoszeniowego, docierającego również do urządzeń nieuprawnionych, niebędących członkami grupy. Ochrona związana jest z tym, że dostęp do klucza grupowego jest warunkowany posiadaniem przez urządzenie użytkownika właściwego klucza personalnego. Ważną zaletą jest też możliwość realizacji komunikacji bezpiecznej w sytuacji dynamicznego czyli zmieniającego się w czasie składu grupy, określanego przez administratora urządzenia menedżera grupy. Wynalazek umożliwia wykluczanie pewnej predefiniowanej liczby urządzeń. użytkowników w każdej sesji. W odróżnieniu od innych rozwiązań tej klasy, liczba urządzeń użytkowników, które można wykluczyć, nie zależy od całkowitej liczby urządzeń wykluczonych w poprzednich sesjach. Rozmiar wiadomości rozsiewczej jest niezależny od całkowitej liczby urządzeń użytkowników, które można wykluczyć. Dzięki temu obciążenie komunikacyjne wprowadzane przez układ dystrybucji kluczy grupowych jest mniejsze. Wynalazek zapewnia wysoki poziom bezpieczeństwa. Gwarantuje on odporność na ataki grup współpracujących ze sobą urządzeń użytkowników. Uprawnione urządzenie użytkownika należące do grupy jest w stanie zdekodować jedynie wartość modyfikatora swojego własnego klucza personalnego i nie ma żadnej wiedzy o modyfikatorach kluczy personalnych innych urządzeń. Klucz personalny urządzenia komunikacyjnego jest unieważniany w czasie wykluczania tego urządzenia z grupy, poprzez uniemożliwienie mu odszyfrowania co najmniej jednego modyfikatora jego klucza personalnego.

Sposób według wynalazku zostanie bliżej objaśniony na podstawie przykładów przedstawionych na rysunku. Układ selektywnej dystrybucji kluczy grupowych stanowi urządzenie menedżera grupy i urządzenia użytkowników połączone za pomocą sieci komunikacyjnej. Fig. 1 jest schematem blokowym urządzenia menedżera grupy w I przykładzie, fig. 2 schematem blokowym urządzenia użytkownika w I przykładzie, fig. 3 schematem blokowym urządzenia menedżera grupy w II przykładzie, a fig. 4 schematem blokowym urządzenia użytkownika w II przykładzie. Na schematach blokowych zostały objęte linią przerywaną te elementy, z których każdy jest połączony z odpowiednim modułem sterującym. Fig. 5–9 pokazują sieci działań, a mianowicie fig. 5 inicjalizację urządzenia menedżera grupy, fig. 6 inicjalizację urządzenia użytkownika, fig. 7 działanie urządzenia menedżera grupy, fig. 8 działanie urządzenia menedżera grupy – rozwinięcie fragmentu, fig. 9 działanie urządzenia użytkownika.

W czasie sesji poprzez sieć telekomunikacyjną rozsyłany jest zaszyfrowany klucz grupowy z urządzenia menedżera grupy M do urządzeń użytkownika U, w których jest on deszyfrowany przy użyciu klucza personalnego. Ponadto w każdej sesji w urządzeniu menedżera grupy M w generatorze modyfikatorów M9 generuje się modyfikatory kluczy personalnych. Szyfruje się je za pomocą szyfratora modyfikatorów M8 wykorzystując dane z pamięci danych maskujących grupy M10. Do szyfrowania modyfikatora używa się technik opartych na wielomianie wykluczającym. Szyfrogram klucza grupowego i szyfrogram modyfikatorów rozsyła się do urządzeń użytkownika U. W urządzeniu użytkownika U deszyfruje się odebrany szyfrogram modyfikatorów za pomocą deszyfratora modyfikatora U5, wykorzystując dane z pamięci danych maskujących użytkownika U7. Z pamięci klucza personalnego U6 pobiera się wartość dotychczasowego klucza personalnego i tworzy się nowy klucz personalny przeznaczony do deszyfrowania szyfrogramów kluczy grupowych w przyszłych sesjach.

P r z y k ł a d I

W tym przykładowym układzie w urządzeniu menedżera grupy M interfejs administratora M1 przyłączony jest do modułu selekcji grupy M3, z którym połączone są szyfrator kluczy grupowych M5 i szyfrator modyfikatorów M8, a także pamięć urządzeń użytkowników M4. Z szyfratorem kluczy grupowych M5 połączony jest też generator kluczy grupowych M6 i pamięć kluczy personalnych grupy M7, a z szyfratorem modyfikatorów M8 generator modyfikatorów M9 i pamięć danych maskujących grupy M10. Dodatkowo generator modyfikatorów M9 połączony jest z pamięcią kluczy personalnych grupy M7. Szyfrator kluczy grupowych M5 i szyfrator modyfikatorów M8 połączone są poprzez moduł przygotowania wiadomości M11 z modułem nadawczym M12.

W każdym urządzeniu użytkownika U do modułu odbiorczego U3 przyłączony jest deszyfrator klucza grupowego U4 i deszyfrator modyfikatora U5, a oba połączone są z pamięcią klucza personalnego U6. Do deszyfratora modyfikatora U5 dołączona jest też pamięć danych maskujących użytkownika U7. Deszyfrator klucza grupowego U4 połączony jest z interfejsem odbiorcy klucza U8. Interfejs ten łączy urządzenie użytkownika, według wynalazku, z modułami kryptograficznymi ODB odbiorcy.

P r z y k ł a d II

W tym przykładzie układ zawiera wszystkie elementy urządzeń z przykładu I, przy czym włączone zostały dodatkowe moduły i połączenia.

W urządzeniu menedżera grupy M pomiędzy szyfratorem modyfikatorów M8, a modułem przygotowania wiadomości M11 włączony jest dodatkowo szyfrator powtórnego szyfrowania M14. Szyfrator ten ma połączenie z generatorem kluczy grupowych M6.

W urządzeniu użytkownika natomiast pomiędzy modułem odbiorczym U3 a deszyfratorem modyfikatora U5 włączony jest deszyfrator powtórnego szyfrowania U9. Jest on połączony z deszyfratorem klucza grupowego U4.

Układ selektywnej dystrybucji kluczy grupowych może być zrealizowany jako specjalizowane urządzenie programowo-sprzętowe, jak w przedstawionych przykładach, lub stanowić jedną z aplikacji uruchomionych na serwerze. W przykładach został zrealizowany w większości na dostępnych gotowych elementach mikroelektroniki, częściowo zaś zaimplementowany w programowalnych układach FPGA oraz na modułach ASIC.

I tak w urządzeniu menedżera grupy M interfejs administratora M1 stanowi komputer PC z ekranem dotykowym i portem USB, moduł sterujący menedżera M2, moduł selekcji grupy M3 i moduł przygotowania wiadomości M11 to procesor z pamięcią RAM. Jako pamięć urządzeń użytkowników M4, pamięć danych maskujących grupy M10 i pamięć kluczy personalnych grupy M7 wykorzystano dysk twardy zamiennie z pamięciami FLASH. Szyfratorami kluczy grupowych M5 i modyfikatorów M8 są dedykowane układy FPGA. Generatorem kluczy grupowych M6 jest procesor z pamięcią RAM, podobnie jak generator modyfikatorów M9. Modułem nadawczym M12 jest karta sieciowa WLAN standardu IEEE 802.11abg. Szyfrator powtórnego szyfrowania M14 zrealizowano jako układ ASIC realizujący algorytm AES.

W urządzeniu użytkownika U interfejsem konfiguracyjnym U1 jest port USB, modułem sterującym użytkownika U2 jest procesor z pamięcią RAM. Modułem odbiorczym U3 jest karta sieciowa WLAN standardu IEEE 802.11abg. Deszyfrator klucza grupowego U4 i deszyfrator modyfikatora U5 zaimplementowano w układzie FPGA. Jako pamięci klucza personalnego U6 i danych maskujących użytkownika U7 zastosowano pamięci FLASH. Interfejsem odbiorcy klucza U8 jest port USB. Może to być interfejs innego typu dostosowany do modułów kryptograficznych odbiorcy ODB. Deszyfrator powtórnego szyfrowania U9 zrealizowano jako układ ASIC realizujący algorytm AES.

Układ, według wynalazku, składa się z urządzenia menedżera grupy M oraz zbioru urządzeń użytkowników U połączonych za pomocą sieci komunikacyjnej. Jest to dowolna znana obecnie lub wprowadzona w przyszłości sieć komunikacyjna. W szczególności, może to być sieć umożliwiająca komunikację w trybie rozsiewczym, polegającym na tym, że pojedyncza wiadomość przygotowana i wysłana przez urządzenie menedżera grupy M jest dostarczana do wielu urządzeń użytkowników U. Przykładami trybu komunikacji rozsiewczej są: *broadcast* oraz *multicast.* Podzbiór ogółu wszystkich urządzeń użytkowników U tworzy grupę komunikacji chronionej cechującą się tym, że w obrębie tej grupy możliwe jest prowadzenie komunikacji chronionej z wykorzystaniem funkcji bezpieczeństwa takich jak na przykład ochrona poufności lub ochrona integralności komunikatów, które wymagają użycia sekretnego, współdzielonego klucza grupowego. Każda zmiana składu grupy w trakcie pracy układu, implikuje potrzebę wymiany klucza grupowego. W trakcie każdej sesji używany jest inny sekretny, współdzielony klucz grupowy. Na początku sesji urządzenie menedżera grupy M wysyła wia-

domość rozsiewczą, odbieraną przez urządzenia użytkowników U podłączone do sieci komunikacyjnej, w celu bezpiecznego dostarczenia klucza grupowego do grupy komunikacji chronionej.

Urządzenie menedżera grupy M odpowiada, między innymi, za przygotowanie urządzeń użytkownika U do pracy, zarządzanie składem grupy oraz przesyłanie wiadomości zawierających klucz grupowy oraz modyfikatory klucza personalnego do urządzeń U podczas pracy układu selektywnej dystrybucji klucza grupowego. Interfejs administratora M1 umożliwia interakcje pomiędzy urządzeniem menedżera grupy a operatorem systemu. Moduł sterujący menedżera M2 jest odpowiedzialny za inicjalizację wszystkich pozostałych modułów wchodzących w skład urządzenia menedżera grupy M. Przeprowadza on sekwencję czynności inicjalizacyjnych, pokazanych w sieci działań na fig. 5. Moduł ten odpowiada również za generowanie danych inicjalizacyjnych dla nowych urządzeń użytkowników U oraz wyznacza moment zakończenia bieżącej i rozpoczęcia nowej sesji.

Dla lepszego zobrazowania działania urządzenia menedżera grupy M sieć działań uwidoczniono na fig. 7, a fig. 8 jest rozwinięciem fragmentu „Selektywna dystrybucja klucza grupowego". Pamięć urządzeń użytkowników M4 przechowuje identyfikatory urządzeń użytkowników U oraz przypisane im unikalne dla każdego urządzenia dane inicjalizacyjne. Pamięć danych maskujących grupy M10 przechowuje sekretne dane, unikalne dla każdego urządzenia użytkownika U, wygenerowane w procesie inicjalizacji urządzenia menedżera grupy M, wykorzystywane w procesie selektywnej dystrybucji modyfikatorów kluczy personalnych. Pamięć kluczy personalnych grupy M7 przechowuje aktualne klucze personalne, stosowane podczas bieżącej sesji. Wstępne wartości kluczy personalnych, unikalnych dla każdego urządzenia U są generowane w procesie inicjalizacji urządzenia menedżera grupy M. Następnie są one modyfikowane w każdej kolejnej sesji, przy użyciu odpowiednich modyfikatorów kluczy personalnych, mogących przyjmować różne wartości dla poszczególnych urządzeń użytkowników U. Moduł selekcji grupy M3 przeprowadza aktualizację pamięci urządzeń użytkowników M4, Generator kluczy grupowych M6 generuje nowy, losowy, sekretny klucz grupowy i przesyła go do szyfratora kluczy grupowych M5. Szyfrator kluczy grupowych M5 szyfruje otrzymany klucz grupowy przy użyciu aktualnych kluczy personalnych odczytanych z pamięci kluczy personalnych grupy M7 w taki sposób, że urządzenia użytkowników U znajdujące się na liście urządzeń aktywnie wykluczanych w bieżącej sesji, dostarczanej przez moduł selekcji grupy M3 nie będą w stanie odszyfrować zaszyfrowanego klucza grupowego. Szyfrogram klucza grupowego jest przekazywany do modułu przygotowania wiadomości rozsiewczych M11. Równocześnie generator modyfikatorów M9 generuje losowe modyfikatory i przesyła je do szyfratora modyfikatorów M8, a następnie wylicza nowe klucze personalne, które będą obowiązywały w kolejnej sesji i aktualizuje pamięć kluczy personalnych grupy M7. Szyfrator modyfikatorów M8 przeprowadza szyfrowanie otrzymanych modyfikatorów kluczy personalnych przy użyciu danych odczytanych z pamięci danych maskujących grupy M10. Szyfrowanie jest przeprowadzone w taki sposób, że urządzenia użytkowników znajdujące się na liście urządzeń aktywnie wykluczanych w bieżącej sesji, dostarczonej przez moduł selekcji grupy M3, nie będą w stanie odszyfrować modyfikatora swojego klucza personalnego z odebranego szyfrogramu modyfikatorów kluczy personalnych. Nie znając modyfikatora swojego klucza personalnego nie będą mogły wyliczyć swego klucza personalnego dla następnej sesji. Szyfrogram modyfikatorów kluczy personalnych jest przekazywany do modułu przygotowania wiadomości rozsiewczych M11, gdzie tworzona jest wiadomość rozsiewcza zawierająca szyfrogram klucza grupowego oraz szyfrogram modyfikatorów kluczy personalnych. Wiadomość rozsiewcza jest następnie zapisywana w archiwum wiadomości M13 i przekazywana do modułu nadawczego M12. Moduł nadawczy M12 przesyła wiadomość rozsiewczą do urządzeń użytkowników U za pośrednictwem sieci komunikacyjnej.

W urządzeniu użytkownika U Interfejs konfiguracyjny U1, oraz moduł sterujący użytkownika U2 umożliwiają operatorowi systemu wprowadzenie danych inicjalizacyjnych. Moduł sterujący użytkownika U2 jest również odpowiedzialny za identyfikację bieżącej sesji oraz wykrywanie momentu rozpoczęcia nowej sesji. Moduł odbiorczy U3 odbiera wiadomość rozsiewczą wysłaną przez urządzenie menedżera grupy M. Odebrany sygnał jest przekazywany do deszyfratora klucza grupowego U4 oraz do deszyfratora modyfikatora U5. Deszyfrator klucza grupowego U4 odszyfrowuje klucz grupowy z szyfrogramu otrzymanego w wiadomości rozsiewczej przy użyciu aktualnego klucza personalnego odczytanego z pamięci klucza personalnego U6. Klucz grupowy zostanie przekazany do modułów kryptograficznych odbiorcy ODB za pośrednictwem interfejsu odbiorcy klucza U8. Deszyfrator modyfikatora U5 odszyfrowuje modyfikator klucza personalnego z szyfrogramu otrzymanego w wiadomości rozsiewczej przy użyciu danych maskujących urządzenia odczytanych z pamięci danych maskujących użytkownika U7. Odszyfrowany modyfikator jest używany do modyfikacji klucza personalnego prze-

chowywanego w pamięci klucza personalnego U6.

Działanie według przedstawionego poniżej sposobu można realizować zarówno w przykładzie I jak i w przykładzie II.

W przedstawianym tutaj sposobie do szyfrowania klucza grupowego użyto technik opartych na arytmetyce wykładniczej, a do szyfrowania modyfikatorów użyto technik opartych na wielomianie wykluczającym. W opisie sposobu zastosowano notację przedstawioną w Tablicy. Sposób ten obejmuje: Inicjalizację urządzenia menedżera (M), Inicjalizację urządzenia użytkownika (U), działanie urządzenia menedżera (M) oraz działanie urządzenia użytkownika (U).

Tablica

U_i	i-te urządzenie użytkownika
K_j	klucz grupowy dystrybuowany w sesji j
κ_j	wykładnik klucza grupowego dystrybuowany w sesji j, tj. $\mathrm{K_j} = \mathrm{g}^{\kappa_j}$
B_j	wiadomość rozsiewcza transmitowana w sesji j
S_i	klucz personalny urządzenia użytkownika U_i
$s_j(x)$	wielomian maskujący używany w sesji j
$h_j(x)$	wielomian kluczy personalnych używany w sesji j
$\delta_j(x)$	wielomian modyfikatorów kluczy personalnych dystrybuowany w sesji j
G_j	zbiór urządzeń użytkowników należących do grupy komunikacji chronionej w sesji j
R_j	zbiór urządzeń użytkowników wykluczonych z grupy komunikacji chronionej w sesji j
$R_{<1,j>}$	zbiór wszystkich urządzeń użytkowników wykluczonych z grupy w sesji j lub wcześniej, tj. $R_{<1,j>} = R_j \cup R_{j-1} \cup \ldots \cup R_2$
I_{G_j}	zbiór indeksów przypisanych wszystkim urządzeniom użytkowników należącym do grupy G_j, tj. $I_{G_j} = \{x_i \in F_q\}_{U_i \in G_j}$
I_{R_j}	zbiór indeksów przypisanych wszystkim urządzeniom użytkowników wykluczonym w sesji j, tj. $I_{R_j} = \{x_i \in F_q\}_{U_i \in R_j}$
$I_{R_{<1,j>}}$	zbiór indeksów przypisanych urządzeniom użytkowników wykluczonym w sesji j lub wcześniej, tj. $I_{R_{<1,j>}} = I_{R_j} \cup I_{R_{j-1}} \cup \ldots \cup I_{R_2}$
t	maksymalna liczba urządzeń użytkowników które można wykluczyć z grupy komunikacji chronionej w czasie pojedynczej sesji
m	maksymalna liczba sesji
d	rozmiar okna retransmisji
c_j	szyfrogram klucza sesyjnego K_j
$\Delta_j(x)$	szyfrogram wielomianu modyfikatorów kluczy personalnych $\delta_j(x)$

Inicjalizacja urządzenia menedżera M została przedstawiona w postaci sieci działań na Fig. 5. Operator wprowadza za pośrednictwem interfejsu administratora M1 parametry konfiguracyjne systemu: *m, t,* |*p*| oraz |*q*|, gdzie m oznacza maksymalną liczbę sesji, *t* jest parametrem określającym poziom bezpieczeństwa, |*p*| oznacza rozmiar liczby pierwszej *p,* |*q*| jest rozmiarem elementów ciała skończo-

nego F_q. Następnie moduł sterujący menedżera M2 generuje parametry struktury algebraicznej używanej w procesie selektywnej dystrybucji kluczy grupowych. Moduł sterujący menedżera M2 generuje liczbę pierwszą *p,* oraz liczby *q, g,* takie że *g* jest generatorem podgrupy cyklicznej $H \subseteq F_q^*$ rzędu *p,* w której obowiązuje założenie DDH *(Decisional Diffie-Hellman assumption).* Następnie, moduł sterujący menedżera generuje *m* losowych wielomianów maskujących $s_1(x),\ldots s_m(x) \in F_p[x]$ stopnia 2*t* oraz jeden wielomian kluczy personalnych $h_1(x) \in F_p[x]$ stopnia *t*. Wygenerowane wielomiany maskujące $s_1(x),\ldots s_m(x)$ są zapisywane w pamięci danych maskujących grupy M10, a wielomian kluczy personalnych $h_1(x)$ jest zapisywany w pamięci kluczy personalnych grupy M7. Następnie, moduł selekcji grupy M3 określa początkowy zbiór G_1 urządzeń użytkowników należących do grupy komunikacji chronionej. Dla każdego urządzenia $U_1 \in G_1$ moduł sterujący menedżera M2 generuje losowy unikalny indeks $x_1 \in F_p$ i wylicza dane inicjalizacyjne $S_i = [x_i, s_1(x_i), \ldots, s_m(x_i), h_1(x_i)]$. Początkowy zbiór G_1 urządzeń użytkowników należących do grupy komunikacji chronionej wraz z przypisanymi im danymi inicjalizacyjnymi, jest zapisywany w pamięci urządzeń użytkowników M4.

Inicjalizacja urządzenia użytkownika U została przedstawiona w postaci sieci działań na Fig. 6. Moduł sterujący menedżera M2 generuje dla urządzenia użytkownika U_i dane inicjalizujące $S_i = [x_i, s_j(x_i), \ldots, s_m(x_i), h_j(x_i)]$, gdzie *j* oznacza numer sesji w trakcie której urządzenie jest dodawane do grupy komunikacji chronionej. Dane inicjalizacyjne S_i są pobierane przez operatora systemu za pośrednictwem interfejsu administratora M1, a następnie są dostarczane w bezpieczny sposób z zachowaniem poufności do urządzenia użytkownika U_i. Moduł sterujący użytkownika U2 zapisuje punkty $s_j(x_i), \ldots, s_m(x_i)$ w pamięci danych maskujących użytkownika U7, a aktualną wartość klucza personalnego $h_j(x_i)$ w pamięci klucza personalnego U6.

Działanie urządzenia menedżera grupy M zostało przedstawione w postaci sieci działań na Fig. 7. Na początku sesji *j* menedżer grupy M przeprowadza proces selektywnej dystrybucji klucza grupowego K_j. W procesie tym urządzenia użytkowników należące do grupy chronionej G_j w sesji *j* otrzymują nowy klucz sesyjny K_j. Klucz sesyjny K_j jest używany przez cały czas trwania sesji *j* przez urządzenia użytkownika do ochrony komunikacji w obrębie grupy chronionej. Jeśli w czasie trwania sesji zaistnieje potrzeba dodania nowych urządzeń do grupy komunikacji chronionej, to można je dodać bez konieczności rozpoczynania nowej sesji. Jeśli w czasie trwania sesji operator systemu zażąda usunięcia wybranych urządzeń użytkowników z grupy komunikacji chronionej, to najpierw zostaną one oznaczone do usunięcia, a dopiero po rozpoczęciu następnej sesji zostaną one efektywnie wykluczone z grupy. W czasie pojedynczej sesji można wykluczyć z grupy co najwyżej *t* urządzeń użytkowników. Decyzję o rozpoczęciu nowej sesji podejmuje moduł sterujący menedżera M2. Po wprowadzeniu zmian w składzie grupy komunikacji bezpiecznej operator systemu może za pośrednictwem interfejsu administratora M1 wymusić natychmiastowe rozpoczęcie nowej sesji, w celu niezwłocznego wykluczenia z grupy urządzeń użytkowników oznaczonych do usunięcia. Kiedy sesja *j* dobiegnie końca, rozpoczynana jest natychmiast sesja *j* + 1. Po przeprowadzeniu m sesji, układ selektywnej dystrybucji kluczy grupowych kończy działanie. Dalsza praca wymaga reinicjalizacji układu.

Selektywna dystrybucja klucza sesyjnego K_j przeznaczonego dla grupy komunikacji chronionej G_j, przeprowadzana przez menedżera grupy M w sesji *j* została przedstawiona w postaci sieci działań na Fig. 8. Na początku, moduł selekcji grupy M3, określa zbiór R_j urządzeń użytkowników U aktywnie wykluczanych w sesji *j.* Następnie wybiera *t* różnych indeksów $W_j = \{w_1,\ldots, w_t\} \subseteq F_p$, takich, że $I_{Rj} \subseteq W_j$, $I_{Gj} \cap W_j =$ oraz $\emptyset \in 0 \notin W_j$. Następnie, generator kluczy grupowych (M6) generuje losowy wykładnik klucza grupowego $\kappa_j \in F_p$ i wylicza klucz grupowy $K_j = g^{\kappa j}$. Następnie, szyfrator kluczy grupowych (M5) szyfruje klucz K_j używając wielomianu kluczy personalnych $h_j(x)$ odczytanego z pamięci kluczy personalnych M7. Generuje on losową wartość $v_j \in F_p$, a następnie wylicza $z_j = g^{\kappa j + vj \cdot hj(0)}$ i tworzy szyfrogram klucza grupowego c_j w postaci:

$$c_j = \left[g^{v_j}, z_j, \left\{ w_l, g^{v_j \cdot h_j(w_l)} \right\}_{w_l \in W_j} \right]$$

Generator modyfikatorów M9 generuje losowy wielomian modyfikatorów kluczy personalnych $\delta_j(x) \in F_p[x]$ stopnia *t,* taki że $\delta_j(x) \notin \{\delta_1(x), \ldots, \delta_{j-1}(x)\}$, oraz $h_{j+1}(x) \notin \{h_1(x), \ldots, h_j(x)\}$, gdzie $h_i(x) = h_1(x) + \sum_{l=1}^{i-1} \delta_l(x)$. Następnie, szyfrator modyfikatorów M8 szyfruje wielomian $\delta_j(x)$ używając wielomianu

maskującego $s_j(x)$, odczytanego z pamięci danych maskujących grupy M10. Wylicza on szyfrogram modyfikatorów kluczy personalnych $\Delta_j(x)$, w postaci wielomianu $\Delta_j(x) = \delta_j\{x) \cdot r_j(x) + s_j(x)$ stopnia 2t, gdzie $r_j(x)$ jest wielomianem wykluczającym, zdefiniowanym jako $r_j(x) = \Pi_{Xi \in Wj}(x - x_i)$. Moduł przygo-

towania wiadomości rozsiewczych M11 wylicza $b_j = [c_j, \Delta_j]$, tworzy wiadomość rozsiewczą B_j w postaci:

$$B_j = [b_j, b_{j-1}, \ldots, b_{j-d}]$$

korzystając z $b_{j-1}, \ldots, b_{j-d}$ zapamiętanych w poprzednich sesjach w archiwum wiadomości M13, a następnie przekazuje B_j do modułu nadawczego M12. Następnie, moduł nadawczy M12 przesyła wiadomość rozsiewczą B_j do urządzeń użytkowników za pośrednictwem sieci komunikacyjnej. W ostatnim kroku, generator modyfikatorów M9 wylicza wielomian kluczy personalnych $h_{j+1}(x) = h_j(x) + \delta_j(x)$, który będzie używany w następnej sesji i aktualizuje pamięć kluczy personalnych grupy M7.

W przykładzie II szyfrogram modyfikatora kluczy personalnych Δ_j szyfrujemy ponownie przy użyciu szyfratora powtórnego szyfrowania M14, który wykonuje szyfrowanie według algorytmu AES. W ten sposób otrzymujemy drugi szyfrogram Δ'_j, który zastępuje szyfrogram Δ_j w komunikacie $b_j = [c_j, \Delta'_j]$.

Działanie urządzenia użytkownika U zostało przedstawione w postaci sieci działań na Fig. 9. Na początku sesji *j,* moduł odbiorczy (U3) odbiera wiadomość rozsiewczą B_j wysłaną przez urządzenie menedżera grupy M za pośrednictwem sieci komunikacyjnej. Odebraną wiadomość przekazuje do deszyfratora klucza grupowego U4 oraz do deszyfratora modyfikatora U5. Deszyfrator klucza grupowego U4 odszyfrowuje klucz grupowy K_j z ciągu szyfrogramów b_j zawartego w wiadomości B_j, przy użyciu aktualnego klucza personalnego $h_j(x_i)$ odczytanego z pamięci klucza personalnego U6. Najpierw wylicza on $g^{v_j \cdot h_j(x_i)} = (g^{v_j})^{h_j(x_i)}$ na podstawie g^{v_j} zawartego w ciągu szyfrogramów b_j oraz swojego aktualnego klucza personalnego $h_j(x)$.

Następnie wylicza wartość $g^{v_j \cdot h_j(O))}$ przeprowadzając interpolację w wykładnikach na podstawie t punktów $\{(w_l, g^{v_j \cdot h_j(w_l)})\}_{w_l \in w_j}$ zawartych w ciągu szyfrogramów b_j oraz pojedynczego punktu $(x_i, g^{v_j \cdot h_j(x_i)})$ wyliczonego z aktualnego klucza personalnego. Następnie wylicza klucz grupowy $K_j = z_j / g^{v_j \cdot h_j(O)}$ i przekazuje go za pośrednictwem interfejsu odbiorcy klucza U8 do modułów kryptograficznych odbiorcy ODB. Następnie, deszyfrator modyfikatora U5 odszyfrowuje modyfikator $\delta_j(x_j)$ klucza personalnego z ciągu szyfrogramów b_j zawartego w wiadomości Bj, używając punktu maskującego $s_j(x_i)$, odczytanego z pamięci danych maskujących użytkownika U7. Najpierw wylicza on wartość wielomianu $\Delta_j(x)$, zawartego w ciągu szyfrogramów b_j, w punkcie $x = x_i$. Następnie odejmuje od niej punkt maskujący $s_j(x_i)$ i otrzymany wynik dzieli przez wartość $r_j(x_i)$, wyliczoną na podstawie zbioru indeksów W_j zawartego w b_j. W ten sposób otrzymuje modyfikator $\delta_j(x_j)$ klucza personalnego, ponieważ $\delta_i(x_i) = \frac{\Delta_j(x_i) - s_j(x_i)}{r_j(x_i)}$. Następnie, deszyfrator modyfikatora U5 wylicza nowy klucz personalny $h_{j+1}(x_i) = h_j(x_i) + \delta_j(x_i)$, który będzie używany w następnej sesji i aktualizuje pamięć klucza personalnego U6.

W przykładzie II drugi szyfrogram modyfikatorów kluczy personalnych Δ'_j deszyfrujemy przy użyciu modułu deszyfratora powtórnego szyfrowania U9 realizującego algorytm AES, a następnie otrzymany szyfrogram Δ_j jest przekazywany do deszyfratora modyfikatora U5.

Przedstawiony wynalazek może być stosowany do ochrony komunikacji w sieciach multicastowych zarządzanych w scentralizowany sposób, takich jak: systemy machine-to-machine (M2M), sieci sensorowe i embedded, sieci komórkowe na przykład GSM, WCDMA, LTE, sieci bezprzewodowe (WLAN). Wynalazek może być również używany w systemach transmisji rozsiewczej, takich jak: radio, telewizja satelitarna, telewizja kablowa, telewizja płatna oraz serwisy informacyjne. Ze względu na wysoki poziom bezpieczeństwa, może on również znaleźć zastosowanie w systemach wojskowych oraz systemach bezpieczeństwa publicznego.

Podane wyżej szczegółowe opisy poszczególnych struktur funkcjonalnych układu, według wynalazku, nie powinny być interpretowane jako ograniczające ideę wynalazku do odmian opisanych układów i dla znawcy jest oczywiste, że opisane układy mogą być poddane wielu modyfikacjom, dostosowaniom i równoważnym realizacjom nie umniejszając uzyskanych efektów technicznych. Tak więc niniejszy opis wynalazku nie powinien być interpretowany jako ograniczający się do ujawnienia przykładów wykonania i określenia odmian układu zastrzeżeniami patentowymi.

Zastrzeżenia patentowe

1. Sposób selektywnej dystrybucji kluczy grupowych z dynamicznym wykluczaniem członków grupy, polegający na rozsyłaniu w czasie sesji poprzez sieć telekomunikacyjną zaszyfrowanego klucza grupowego z urządzenia menedżera grupy do urządzeń użytkowników i deszyfrowaniu szyfrogramu tego klucza grupowego w urządzeniu użytkownika przy użyciu klucza personalnego, **znamienny tym**, że w każdej sesji w urządzeniu menedżera grupy (M) w generatorze modyfikatorów (M9) będącym procesorem zawierającym generator liczb pseudolosowych, generuje się modyfikatory kluczy personalnych, szyfruje się je za pomocą szyfratora modyfikatorów (M8) wykorzystując dane z pamięci danych maskujących grupy (M10), zrealizowanego jako programowalny układ logiczny lub procesor lub układ ASIC i rozsyła się przez sieć telekomunikacyjną do urządzeń użytkowników (U), po czym w urządzeniu użytkownika (U) deszyfruje się szyfrogram modyfikatorów za pomocą deszyfratora modyfikatora (U5), wykonanego jako programowalny układ logiczny lub procesor lub układ ASIC, wykorzystując dane z pamięci danych maskujących użytkownika (U7), pobiera się w postaci sygnału zmodulowanego cyfrowego, z pamięci klucza personalnego (U6) wartość dotychczasowego klucza personalnego i z użyciem modyfikatora tworzy się nowy klucz personalny przeznaczony do deszyfrowania szyfrogramów kluczy grupowych w przyszłych sesjach.
2. Sposób według zastrz. 1, **znamienny tym**, że w urządzeniu menedżera grupy (M) szyfrogram modyfikatorów kluczy personalnych otrzymany przez zaszyfrowanie modyfikatorów kluczy personalnych z użyciem danych maskujących grupy, szyfruje się powtórnie, za pomocą programowalnego układu logicznego lub procesora lub układu ASIC, wykorzystującego klucz grupowy i otrzymuje się drugi szyfrogram, po czym w urządzeniu użytkownika (U) najpierw deszyfruje się ten drugi szyfrogram za pomocą programowalnego układu logicznego lub procesora lub układu ASIC, wykorzystującego klucz grupowy otrzymany z deszyfratora klucza grupowego (U4), a następnie deszyfruje się tak otrzymany szyfrogram modyfikatorów kluczy personalnych za pomocą programowalnego układu logicznego lub procesora lub układu ASIC, używając danych z pamięci danych maskujących użytkownika (U7).
3. Sposób według zastrz. 1 lub 2, **znamienny tym**, że do szyfrowania klucza grupowego używa się technik opartych na arytmetyce wykładniczej, a do szyfrowania modyfikatorów używa się technik opartych na wielomianie wykluczającym realizowanych w szyfratorze kluczy grupowych (M5) wykonanym jako programowalny układ logiczny lub procesor lub układ ASIC i szyfratorze modyfikatorów (M8) zrealizowanym jako programowalny układ logiczny lub procesor lub układ ASIC.
4. Układ do selektywnej dystrybucji kluczy grupowych z dynamicznym wykluczaniem członków grupy, składający się z urządzenia menedżera grupy i urządzeń użytkowników połączonych poprzez sieć telekomunikacyjną, zawierający w urządzeniu menedżera grupy interfejs administratora, generator kluczy grupowych, szyfrator kluczy grupowych, pamięć kluczy personalnych grupy, moduł nadawczy i moduł sterujący menedżera połączony ze wszystkimi modułami menedżera grupy, oraz zawierający w każdym urządzeniu użytkownika, moduł odbiorczy, deszyfrator klucza grupowego z pamięcią klucza personalnego oraz interfejs odbiorcy klucza ponadto ma moduł sterujący z interfejsem konfiguracyjnym połączony ze wszystkimi modułami urządzenia użytkownika, **znamienny tym,** że w urządzeniu menedżera grupy (M) interfejs administratora (M1) w postaci minikomputera z komunikacyjnym portem wejścia/wyjścia, przyłączony jest do modułu selekcji grupy (M3) zrealizowanym na procesorze z pamięcią RAM, z którym połączone są szyfrator kluczy grupowych (M5) i szyfrator modyfikatorów (M8), a także pamięć urządzeń użytkowników (M4), ponadto z szyfratorem kluczy grupowych (M5) połączony jest generator kluczy grupowych (M6) i pamięć kluczy personalnych grupy (M7), a z szyfratorem modyfikatorów (M8) generator modyfikatorów (M9) i pamięć danych maskujących grupy (M10), przy czym generator modyfikatorów (M9) połączony jest z pamięcią kluczy personalnych grupy (M7), a ponadto szyfrator kluczy grupowych (M5) i szyfrator modyfikatorów (M8) połączone są poprzez moduł przygotowania wiadomości (M11), będący procesorem wyposażonym w pamięć RAM, z modułem nadawczym (M12), natomiast w każdym urządzeniu użytkownika (U) do modułu odbiorczego (U3) przyłączony jest deszyfrator klucza grupowego (U4) i deszyfrator modyfikatora (U5) oba połączone z pamięcią klucza personalnego (U6), przy czym do deszyfratora modyfikatora (U5) dołączona

jest pamięć danych maskujących użytkownika (U7), zaś deszyfrator klucza grupowego (U4) połączony jest z interfejsem odbiorcy klucza (U8), przy czym generator kluczy grupowych (M6) oraz generator modyfikatorów (M9) są procesorami zawierającymi generator liczb pseudolosowych, natomiast szyfrator kluczy grupowych (M5), szyfrator modyfikatorów (M8), deszyfrator klucza grupowego (U4) i deszyfrator modyfikatora (U5) są programowalnymi układami logicznymi lub procesorami lub układami ASIC.

5. Układ, według zastrz. 4, **znamienny tym**, że pomiędzy szyfratorem modyfikatorów (M8), a modułem przygotowania wiadomości (M11) w postaci procesora z pamięcią, włączony jest dodatkowo szyfrator powtórnego szyfrowania (M14), zrealizowany w postaci programowalnego układu logicznego lub procesora lub układu ASIC, który to szyfrator powtórnego szyfrowania (M14), ma połączenie z generatorem kluczy grupowych (M6), natomiast pomiędzy modułem odbiorczym (U3) a deszyfratorem modyfikatora (U5) włączony jest deszyfrator powtórnego szyfrowania (U9), zrealizowany w postaci programowalnego układu logicznego lub procesora lub układu ASIC, połączony z deszyfratorem klucza grupowego (U4).

Rysunki

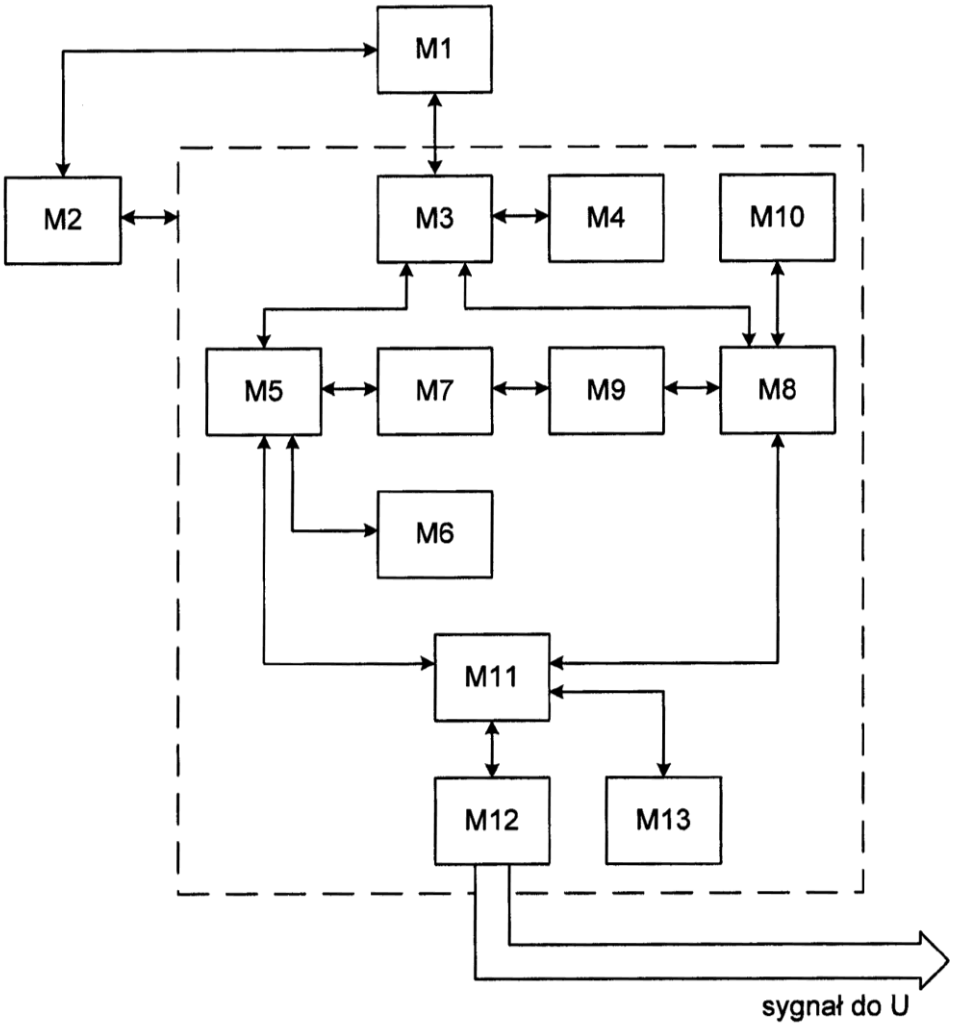

Fig. 1

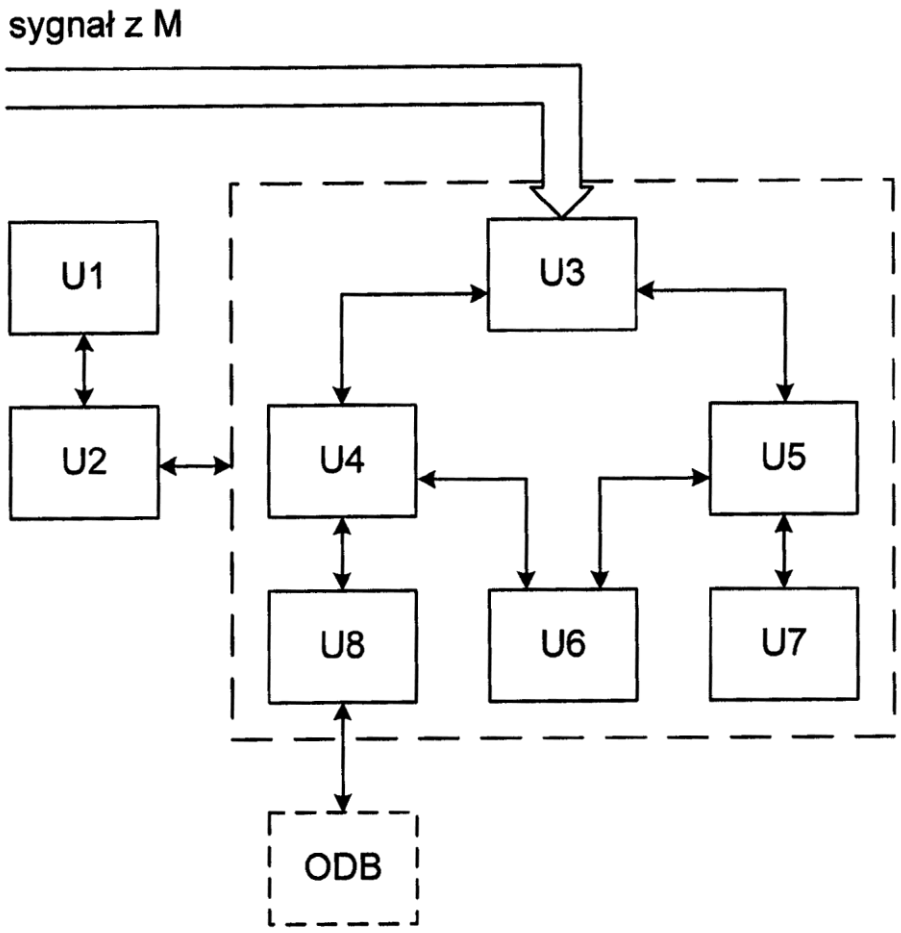

Fig. 2

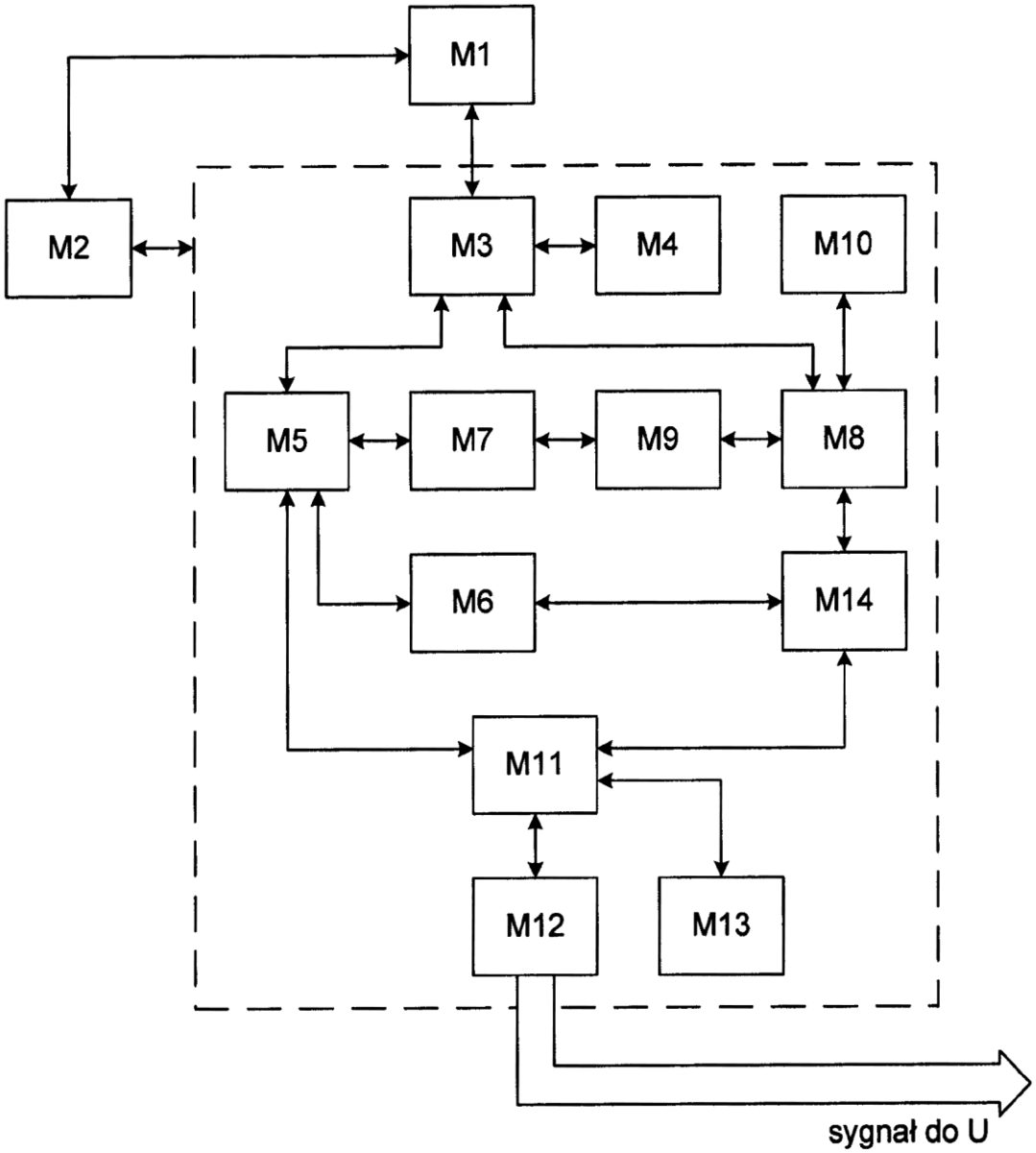

Fig. 3

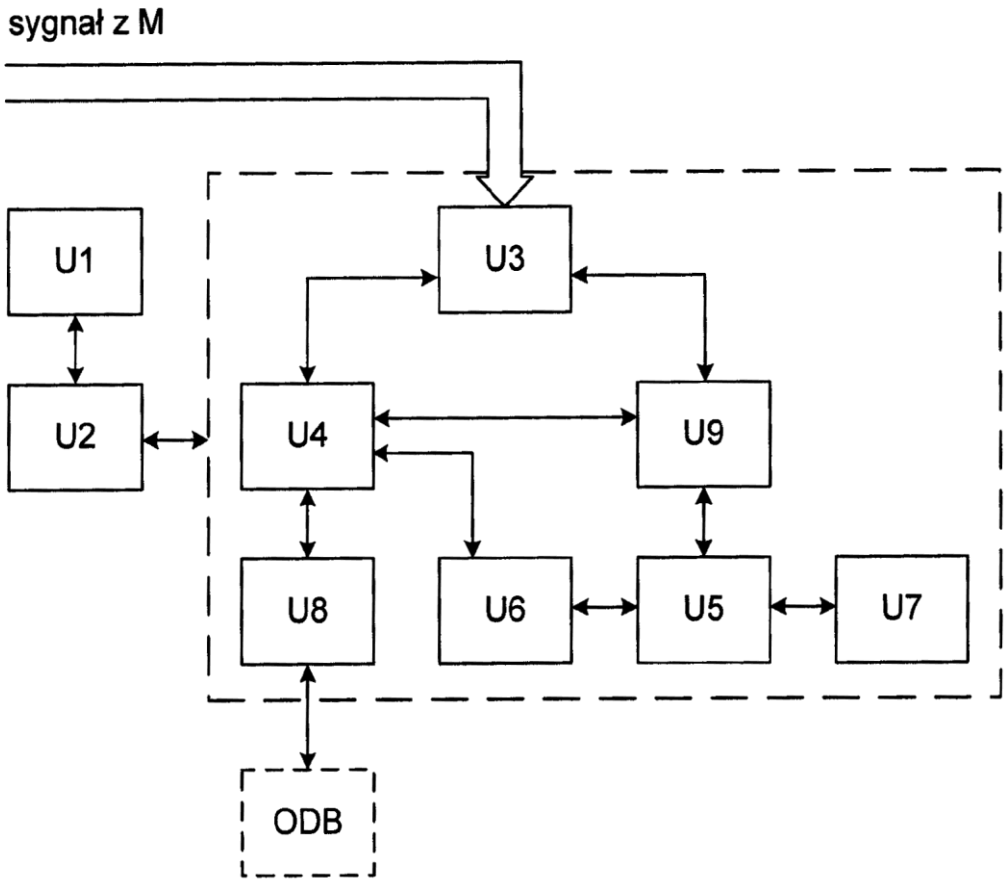

Fig. 4

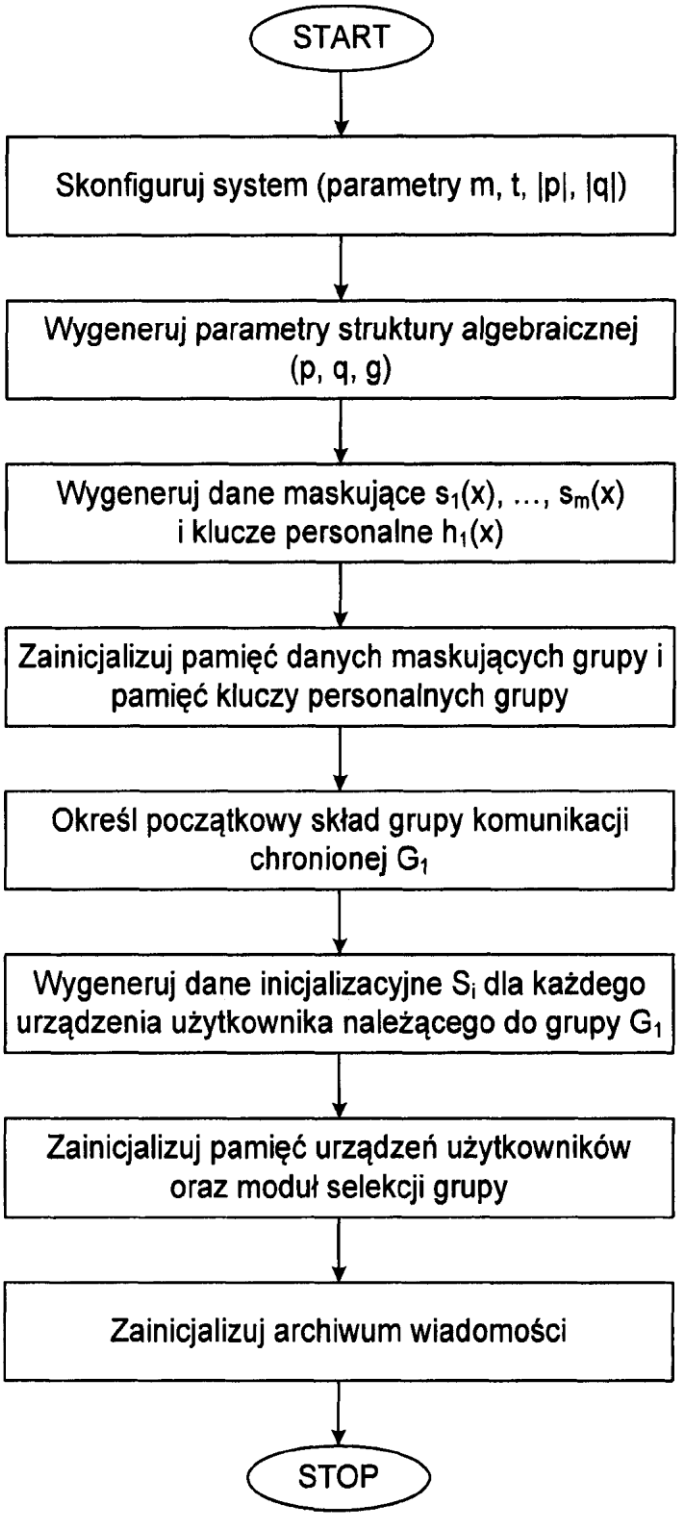
START
Skonfiguruj system (parametry m, t, |p|, |q|)
Wygeneruj parametry struktury algebraicznej (p, q, g)
Wygeneruj dane maskujące $s_1(x)$, ..., $s_m(x)$ i klucze personalne $h_1(x)$
Zainicjalizuj pamięć danych maskujących grupy i pamięć kluczy personalnych grupy
Określ początkowy skład grupy komunikacji chronionej G_1
Wygeneruj dane inicjalizacyjne S_i dla każdego urządzenia użytkownika należącego do grupy G_1
Zainicjalizuj pamięć urządzeń użytkowników oraz moduł selekcji grupy
Zainicjalizuj archiwum wiadomości
STOP

Fig. 5

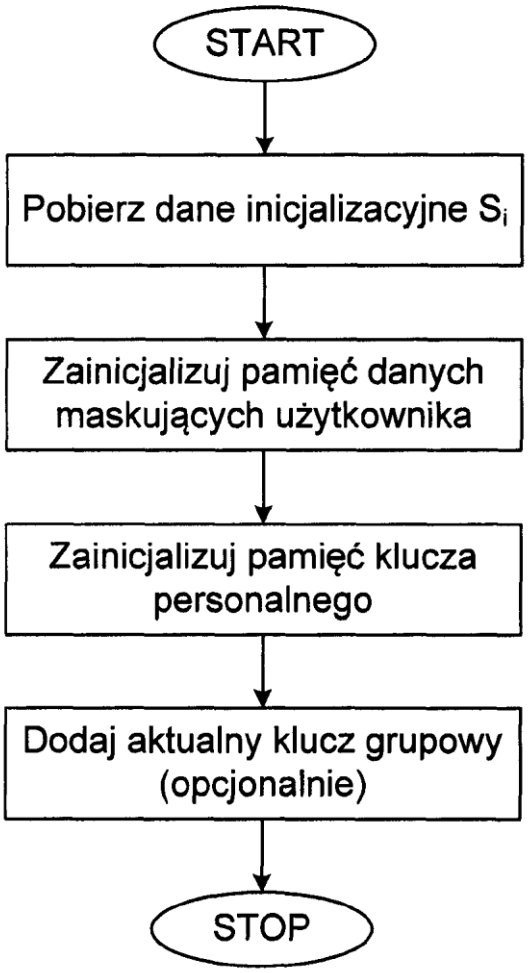
START
Pobierz dane inicjalizacyjne S_i
Zainicjalizuj pamięć danych maskujących użytkownika
Zainicjalizuj pamięć klucza personalnego
Dodaj aktualny klucz grupowy (opcjonalnie)
STOP

Fig. 6

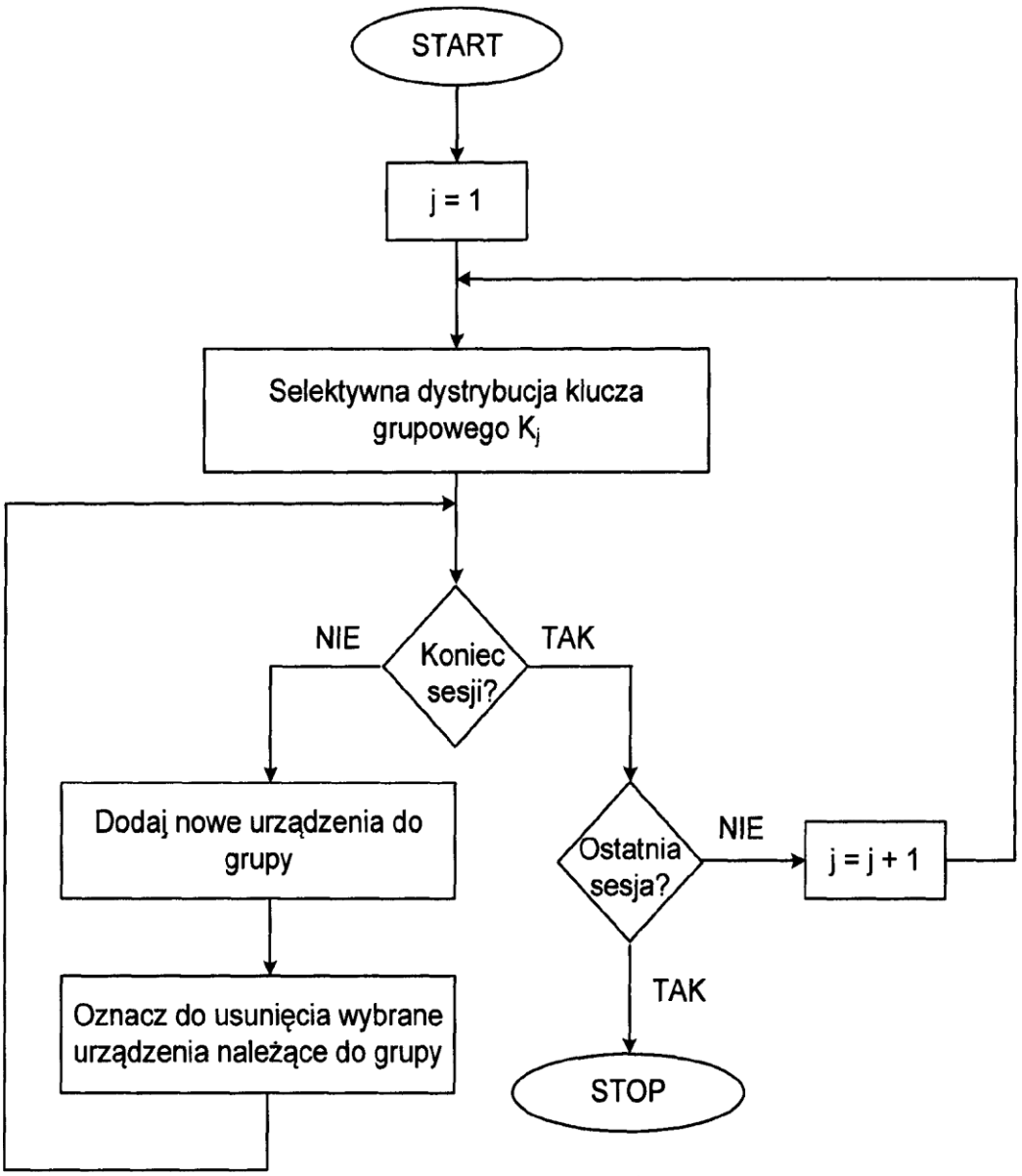
START
j = 1
Selektywna dystrybucja klucza grupowego K_j
NIE
Koniec sesji?
TAK
Dodaj nowe urządzenia do grupy
Oznacz do usunięcia wybrane urządzenia należące do grupy
Ostatnia sesja?
NIE
j = j + 1
TAK
STOP

Fig. 7


START
Skonfiguruj system (parametry m, t, |p|, |q|)
Wygeneruj parametry struktury algebraicznej (p, q, g)
Wygeneruj dane maskujące $s_1(x)$, ..., $s_m(x)$ i klucze personalne $h_1(x)$
Zainicjalizuj pamięć danych maskujących grupy i pamięć kluczy personalnych grupy
Określ początkowy skład grupy komunikacji chronionej G_1
Wygeneruj dane inicjalizacyjne S_i dla każdego urządzenia użytkownika należącego do grupy G_1
Zainicjalizuj pamięć urządzeń użytkowników oraz moduł selekcji grupy
Zainicjalizuj archiwum wiadomości
STOP

Fig. 8

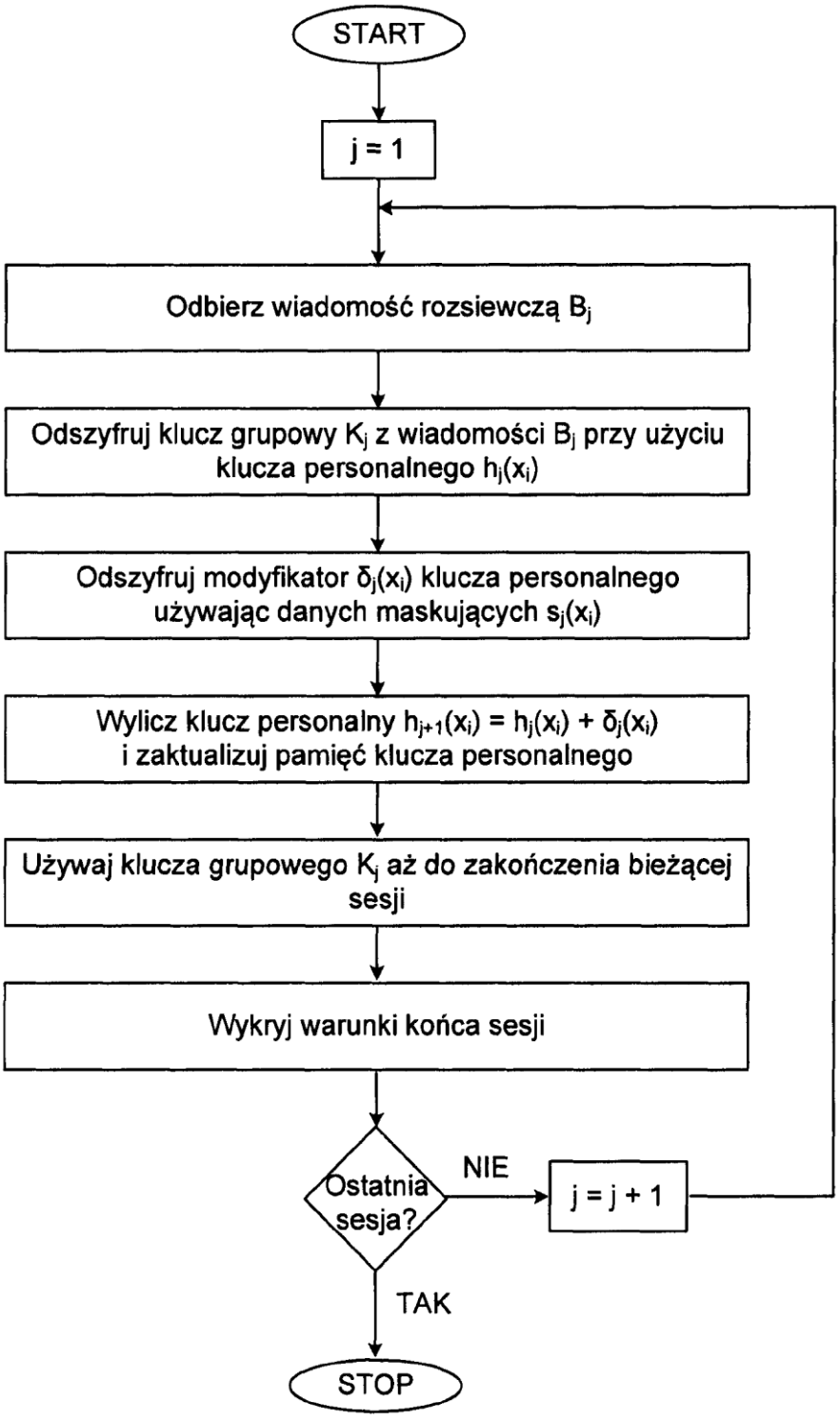
START
j = 1
Odbierz wiadomość rozsiewczą B_j
Odszyfruj klucz grupowy K_j z wiadomości B_j przy użyciu klucza personalnego $h_j(x_i)$
Odszyfruj modyfikator $\delta_j(x_i)$ klucza personalnego używając danych maskujących $s_j(x_i)$
Wylicz klucz personalny $h_{j+1}(x_i) = h_j(x_i) + \delta_j(x_i)$ i zaktualizuj pamięć klucza personalnego
Używaj klucza grupowego K_j aż do zakończenia bieżącej sesji
Wykryj warunki końca sesji
Ostatnia sesja?
NIE
j = j + 1
TAK
STOP

Fig. 9

Departament Wydawnictw UPRP
Cena 4,92 zł (w tym 23% VAT)