



Nhận ngày 31 tháng 12 năm 2019, chấp nhận ngày 18 tháng 1 năm 2020, ngày xuất bản ngày 27 tháng 1 năm 2020, ngày có phiên bản hiện tại ngày 6 tháng 2 năm 2020.

Mã định danh đối tượng kỹ thuật số 10.1109/ACCESS.2020.2969474

Phân tích chính thức về xác thực 5G EAP-TLS

Giao thức sử dụng Proverif

JINGJING ZHANG^{1,2}, LIN YANG AND QIANG WANG¹ ¹Trường Cao đẳng Kỹ thuật Công nghệ và Điều khiển, Đại học Kỹ thuật Quân đội PLA, Nam Kinh 210007, Trung Quốc ² Phòng thí nghiệm Khoa học và Công nghệ Trọng điểm Quốc gia về An ninh Hệ thống Thông tin, Viện Kỹ thuật Hệ thống, Học viện Khoa học Quân sự Trung Quốc, Bắc Kinh 100039, Trung Quốc ³ Trường Cao đẳng Khoa học Máy tính và Kỹ thuật Phần mềm, Đại học Thâm Quyển, Thâm Quyển 518060, Trung Quốc Tác giả tương ứng: Qiang Wang (wenjunwang.nudt@gmail.com) ²

Công trình này được hỗ trợ bởi Phòng thí nghiệm khoa học và công nghệ trọng điểm quốc gia về An toàn hệ thống thông tin.

TÓM TẮT Là một thành phần quan trọng trong kiến trúc bảo mật của mạng 5G, giao thức xác thực đóng vai trò là biện pháp bảo vệ đầu tiên trong việc đảm bảo an ninh liên lạc, chẳng hạn như tính bảo mật của dữ liệu người dùng. EAP-TLS là một trong những giao thức như vậy được xác định trong tiêu chuẩn 5G để cung cấp các dịch vụ chính trong các trường hợp IoT cụ thể. Giao thức này hiện đang trong quá trình tiêu chuẩn hóa và điều quan trọng là phải đảm bảo rằng giao thức được tiêu chuẩn hóa không có bất kỳ lỗi thiết kế nào, điều này có thể dẫn đến các lỗ hổng nghiêm trọng và hậu quả nghiêm trọng khi triển khai trong các hệ thống thực. Tuy nhiên, vẫn chưa rõ liệu giao thức xác thực 5G EAP-TLS được đề xuất có cung cấp các đảm bảo bảo mật như đã tuyên bố hay không. Để lấp đầy khoảng trống này, trong công trình này, chúng tôi trình bày bản phân tích chính thức toàn diện về các thuộc tính liên quan đến bảo mật của giao thức xác thực 5G EAP-TLS dựa trên phương pháp kiểm tra mô hình ký hiệu. Cụ thể, chúng tôi xây dựng mô hình chính thức đầu tiên của giao thức xác thực 5G EAP-TLS trong phép tính pi được áp dụng và thực hiện phân tích bảo mật tự động của mô hình giao thức chính thức bằng cách sử dụng trình kiểm tra mô hình ProVerif. Kết quả phân tích của chúng tôi cho thấy có một số sai sót nhỏ trong thiết kế giao thức hiện tại có thể ảnh hưởng đến các mục tiêu bảo mật đã được xác nhận. Vì mục đích này, chúng tôi cũng đề xuất và xác minh một giải pháp khắc phục khả thi có thể giảm thiểu những sai sót này.


Theo hiểu biết tốt nhất của chúng tôi, đây là phân tích chính thức kỹ lưỡng đầu tiên về giao thức xác thực 5G EAP-TLS.

CHỈ SỐ ĐIỀU KHOẢN Giao thức xác thực, mạng 5G, xác minh chính thức, kiểm tra mô hình, phép tính pi được áp dụng, ProVerif, EAP-TLS.

I. GIỚI THIỆU Là một cơ

sở hạ tầng không thể thiếu, mạng di động đã phát triển qua nhiều thế hệ trong những thập kỷ qua. Với mạng 5G mới nhất, cả thuê bao và nhà mạng đều mong đợi thông lượng mạng tăng lên cũng như đảm bảo bảo mật mạnh mẽ hơn. Trong số tất cả các đảm bảo an ninh, xác thực và thỏa thuận khóa là mối quan tâm hàng đầu, cung cấp cơ chế cơ bản để thiết lập kênh liên lạc an toàn.

Việc xác thực và thỏa thuận khóa thường đạt được bằng cách thực hiện giao thức xác thực giữa thuê bao và mạng. Trong mạng 5G, ba giao thức xác thực khác nhau được xác định trong các tài liệu 3GPP liên quan, bao gồm giao thức 5G AKA (Xác thực và Thỏa thuận chính) [1], giao thức EAP-AKA [1] và 5G

Phó biên tập viên điều phối việc xem xét bản thảo này và người chấp thuận xuất bản nó là Miguel López-Benítez. ¹

Giao thức EAP-TLS [1], [2]. Hai giao thức đầu tiên dựa trên mật mã khóa chung (với những khác biệt nhỏ trong cách lấy khóa phiên) và giao thức cuối cùng dựa trên mật mã khóa công khai. Mặc dù tất cả đều nhằm mục đích cung cấp xác thực lẫn nhau giữa người đăng ký và mạng, các giao thức khác nhau được sử dụng để cung cấp dịch vụ trong các trường hợp khác nhau, ví dụ: giao thức EAP-TLS được xác định để xác thực thuê bao trong các trường hợp sử dụng hạn chế, chẳng hạn như mạng riêng hoặc Môi trường IoT.

Hiện tại, các giao thức này đang trong quá trình chuẩn hóa. Chúng chủ yếu được phát triển dưới dạng RFC, một tài liệu bằng ngôn ngữ không chính thức (thường là tiếng Anh) cung cấp hướng dẫn sâu rộng cho các kỹ sư giao thức, nhưng dù sao cũng mơ hồ và có nhiều cách diễn giải.

Sự mơ hồ của các thiết kế giao thức không chính thức là nguồn gốc của nhiều lỗ hổng bảo mật nghiêm trọng trong quá trình triển khai, như đã báo cáo trong [3], [4]. Một cơ chế hữu ích để giải quyết những sự mơ hồ này và xác nhận tính đúng đắn của giao thức

thiết kế là thực hiện phân tích chính thức, trong đó trước tiên chúng tôi xây dựng mô hình toán học của giao thức bằng ngôn ngữ chính thức, sau đó phân tích xem mô hình giao thức chính thức có đáp ứng các thuộc tính bảo mật cần thiết hay không. Một cách tiếp cận nổi bật để thực hiện phân tích chính thức các giao thức bảo mật là kiểm tra mô hình tương đương [5]. Kể từ khi công trình tiên phong [6] phát hiện ra lỗ hổng thiết kế của giao thức Needham-Schroeder sử dụng kỹ thuật này, việc kiểm tra mô hình biểu tượng của các giao thức bảo mật đã trở thành một lĩnh vực nghiên cứu tích cực và được công nhận là một kỹ thuật mạnh mẽ để phân tích chính thức thiết kế của các giao thức bảo mật [7]–[13] và được áp dụng cho một số giao thức thực tế, chẳng hạn như TLS [14]. Nghiên cứu về kiểm tra mô hình các giao thức bảo mật nằm ngoài phạm vi của công việc này. Chúng tôi tham khảo bài viết [5] để có phần giới thiệu chi tiết về lĩnh vực này.

Trong công việc của mình, chúng tôi sử dụng trình kiểm tra mô hình ProVerif [15] để thực hiện phân tích chính thức. ProVerif lấy mô hình giao thức chính thức được chỉ định trong phép tính pi [13], [16] được áp dụng làm đầu vào và tự động kiểm tra xem mô hình này có đáp ứng các thuộc tính bảo mật nhất định khi có kẻ tấn công độc hại hay không. Do thực tế là việc kiểm tra mô hình của giao thức bảo mật nói chung là không thể quyết định được [5], nên ProVerif có thể không chấm dứt trong một số trường hợp. Trong trường hợp chấm dứt, ProVerif có thể cho biết liệu các thuộc tính bảo mật được chỉ định có được thỏa mãn hay không và nếu một số thuộc tính bị vi phạm, các ví dụ phản biện sẽ được tạo ra để chứng minh các vi phạm.

Nói chung, ProVerif dựa trên mô hình biểu tượng của mã và mô hình kẻ tấn công Dolev-Yao [17]. Các thông báo giao thức được trừu tượng hóa bằng các thuật ngữ và các nguyên hàm đồ họa mã được trừu tượng hóa bằng các ký hiệu hàm và được coi là hoàn hảo (nghĩa là không thể phá vỡ). Các thuộc tính đại số của mã nguyên thủy được mô tả bằng các quan hệ phương trình trên các ký hiệu hàm. Logic giao thức sau đó được mô hình hóa bằng một mô hình quy trình, mô hình này được mã hóa sâu hơn dưới dạng tập hợp các mệnh đề sừng cho lý luận chính thức và các thuộc tính bảo mật được chỉ định là thuộc tính khả năng tiếp cận hoặc tương ứng của mô hình chính thức. Phân tích bảo mật sau đó tập trung vào vấn đề thống nhất mệnh đề Horn [18]. Điểm mạnh chính của ProVerif là như sau. Đầu tiên, nó cung cấp một cơ chế mô hình hóa mạnh mẽ để mô tả một loạt các nguyên mẫu mã hóa bằng cách sử dụng các quy tắc và phương trình viết lại.

Nó cũng hỗ trợ các thuộc tính bảo mật khác nhau, bao gồm bí mật mạnh và yếu, xác thực và một số thuộc tính tương đương quan sát. Nó cũng có thể xử lý số lượng thực thi giao thức song song không giới hạn, điều này rất quan trọng để phát hiện các cuộc tấn công tình vi, chẳng hạn như kẻ trung gian. Cuối cùng, nó có thể tự động tạo ra các mẫu phản biện dưới dạng thực thi giao thức, khi quá trình xác minh cho thấy các thuộc tính bảo mật bị vi phạm.

Chúng tôi nhận thấy rằng công việc của chúng tôi được lấy cảm hứng từ các công trình liên quan [19], [20], trong đó các tác giả đã phân tích các thuộc tính bảo mật của giao thức 5G AKA (và biến thể EAP-AKA của nó) dựa trên bộ phân tích giao thức TAMARIN [21]. Tuy nhiên, theo những gì chúng tôi biết, chưa có phân tích chính thức nào về giao thức 5G EAP-TLS và vẫn chưa rõ liệu thiết kế giao thức 5G EAP-TLS hiện tại có đáp ứng được yêu cầu bảo mật hay không.

các thuộc tính như đã nêu trong các tài liệu 3GPP. Kết quả phân tích của giao thức 5G AKA trong [19], [20] không thể áp dụng cho trường hợp của chúng tôi, vì giao thức 5G EAP-TLS khác với giao thức 5G AKA đáng kể ở cả nguyên hàm mã được sử dụng và cách lấy phiên. phim.

Hơn nữa, chúng tôi sử dụng một khung mô hình hóa khác dựa trên phép tính quy trình dành riêng cho các giao thức bảo mật, trong khi mô hình hóa của chúng dựa trên thuật ngữ quy tắc viết lại [22].

Để đạt được mục đích này, chúng tôi có những đóng góp sau đây trong công việc này:

- 1) Chúng tôi xây dựng mô hình chính thức đầu tiên của giao thức xác thực 5G EAP-TLS trong phép tính pi được áp dụng, đây là ngôn ngữ chính thức cho các giao thức bảo mật. Chúng tôi cũng gọi ra tập hợp các thuộc tính bảo mật từ các tài liệu tiêu chuẩn hóa không chính thức và mã hóa chúng dưới dạng các truy vấn có thể phân tích được trong mô hình chính thức. Chúng tôi nhận thấy rằng việc đưa ra mô hình giao thức chính thức và mã hóa các thuộc tính bảo mật là rất khó vì nó đòi hỏi sự hiểu biết sâu sắc về logic giao thức và hành vi có thể xảy ra của cuộc tấn công.
- 2) Chúng tôi thực hiện phân tích chính thức toàn diện về giao thức 5G EAP-TLS dựa trên trình kiểm tra mô hình ProVerif. Kết quả phân tích của chúng tôi cho thấy một số điểm yếu và sai sót trong thiết kế trong giao thức hiện tại, dẫn đến phá vỡ các thuộc tính xác thực dự định. Các phản ví dụ chứng minh được tạo ra và phân tích để xác định nguyên nhân gốc rễ của sai sót này.
- 3) Chúng tôi cũng đề xuất một bản sửa lỗi khả thi cho giao thức xác thực 5G EAP-TLS hiện tại và xác minh rằng bản sửa lỗi đáp ứng tất cả các thuộc tính bắt buộc. Theo hiểu biết tốt nhất của chúng tôi, đây là phân tích chính thức kỹ lưỡng đầu tiên về giao thức xác thực 5G EAP-TLS.

Phần còn lại của bài viết này được tổ chức như sau. Trong Phần II, chúng tôi xem xét các công trình có liên quan nhất. Trong Phần III, chúng tôi trình bày cú pháp và ngữ nghĩa của phép tính số pi ứng dụng. Trong Phần IV, chúng tôi giới thiệu chi tiết về giao thức 5G EAP-TLS. Trong Phần V, chúng tôi trình bày mô hình giao thức chính thức cũng như các thuộc tính bảo mật. Trong Phần VI, chúng tôi báo cáo kết quả xác minh. Cuối cùng, trong Phần VII, chúng tôi kết thúc bài viết này và phác thảo công việc trong tương lai.

II. CÁC CÔNG TRÌNH LIÊN

QUAN Trong phần này, chúng tôi xem xét các công trình liên quan nhất về phân tích chính thức về giao thức xác thực 5G và giao thức TLS.

Trước hết, liên quan đến phân tích chính thức các giao thức xác thực 5G, đây là một chủ đề tương đối mới và hầu hết công việc tập trung vào phân tích giao thức 5G AKA và biến thể EAP-AKA của nó. các giao thức xác thực 5G liên quan được minh họa trong Bảng 1. .

Trong [19], các tác giả đã mô hình hóa và phân tích giao thức 5G AKA và các thuộc tính bảo mật của nó bằng TAMARIN. Trong mô hình của họ, họ hợp nhất hai thành phần chính (mạng phục vụ và mạng gia đình) thành một thực thể mạng duy nhất. Họ đã tìm thấy các vấn đề về xác thực do thiếu

BẢNG 1. So sánh các mô hình chính thức của giao thức xác thực 5G.

Protocol	5G AKA				5G AKA'	5G EAP-TLS	
Article	[19]	[20]	[27]	[24]	[19]	[28]	This paper
Cryptographic primitives	Shared key cryptography	Shared key cryptography	Shared key cryptography	Shared key cryptography	Shared key cryptography	Public key cryptography	Public key cryptography
Modeling entities	UE,SEAF,AUSF	UE,SEAF,AUSF,ARPF	UE,SEAF,AUSF	UE,AUSF	UE,SEAF,AUSF	UE,SEAF,AUSF	UE,SEAF,AUSF,ARPF
Model checker being used	TAMARIN	TAMARIN	TAMARIN	-	TAMARIN	Scyther	ProVerif
Modeling language	Multiset rewriting rules	Multiset rewriting rules	Multiset rewriting rules	Bana-comon logic	Multiset rewriting rules	Role scripts	Applied pi calculus
Security Properties	Confidentiality of session key, SUPI and SQN; Authentication of each entity	Confidentiality of session key, SUPI and SQN; Authentication of each entity	Confidentiality of SQN	Unlinkability between UE and AUSF	Confidentiality of session key, SUPI and SQN; Authentication of each entity	Confidentiality of session key and SUPI; Authentication of each entity	Confidentiality of session key and SUPI; Authentication of each entity and session key
Threat model	Dolev-Yao model and compromised components	Dolev-Yao model and compromised components	Dolev-Yao model	Customize model	Dolev-Yao model and compromised components	Dolev-Yao model	Dolev-Yao model

bảo vệ tính toàn vẹn cho danh tính mạng dịch vụ. Ngoài ra, họ cũng lập mô hình và phân tích giao thức EAP-AKA, sử dụng sơ đồ mã hóa tích hợp đường cong elip và sử dụng tính năng ẩn danh tính để đảm bảo quyền riêng tư của người dùng. Sau đó trong [23], các tác giả đề xuất một phiên bản mới của giao thức 5G AKA để khắc phục tất cả các điểm yếu hiện được xác định trong [19].

Trong [20], các tác giả đã mô hình hóa tất cả các thành phần chính của giao thức 5G AKA (tức là thiết bị người dùng, mạng phục vụ và mạng gia đình) theo định nghĩa trong tài liệu đặc tả 3GPP. Mô hình của họ chi tiết hơn, bao gồm mô hình hóa kênh mạng lõi giữa mạng phục vụ và mạng gia đình và mô hình hóa những người tham gia không trung thực, so với mô hình trong [19]. Họ phát hiện ra một cuộc tấn công khai thác một điều kiện chạy đua tiềm năng và cũng cho thấy rằng việc giải quyết điều kiện chạy đua cho trường hợp trung thực không nhất thiết ngăn chặn được cuộc tấn công. Họ cũng đề xuất các bản sửa lỗi và chứng minh rằng những bản sửa lỗi này có thể ngăn chặn cuộc tấn công, sau đó báo cáo phát hiện của họ cho 3GPP.

Trong [24], các tác giả đã nghiên cứu các thuộc tính bảo mật của giao thức xác thực 5G AKA, theo logic Bana-Comon [25], [26], là phần mở rộng của logic bậc nhất. Họ phát hiện ra một cuộc tấn công khử đồng bộ hóa mới chống lại phiên bản sửa đổi của giao thức AKA (tức là PRIV-AKA), mặc dù nó đã được xác nhận là an toàn. Họ cũng đề xuất cách khắc phục điểm yếu này và chứng minh rằng giao thức cố định đảm bảo các đặc tính riêng tư.

Trong [27], các tác giả đã tìm thấy một lỗ hổng logic mới trong thông số kỹ thuật của tất cả các biến thể AKA nói trên. Họ tuyên bố rằng cơ chế bảo vệ số thứ tự (SQN) có thể bị đánh bại trong các cuộc tấn công phát lại cụ thể do sử dụng Exclusive-OR (XOR) và thiếu tính ngẫu nhiên.

Về phân tích chính thức của giao thức TLS, chúng tôi xem xét những giao thức có liên quan nhất. Trong [14], các tác giả đã phát triển một mô hình biểu tượng của đặc tả TLS 1.3 (dự thảo 21), xem xét tất cả các tương tác có thể có của các chế độ bắt tay có sẵn. Họ chứng minh phần lớn các yêu cầu bảo mật được chỉ định bằng cách sử dụng bộ chứng minh TAMARIN [21] và phát hiện ra hành vi có thể dẫn đến các vấn đề bảo mật trong các ứng dụng cho rằng TLS 1.3 cung cấp các đảm bảo xác thực mạnh mẽ.

Trong [29], các tác giả trình bày các định lý cấu thành các giao thức bảo mật để soạn thảo một giao thức trao đổi khóa và một giao thức khóa đối xứng sử dụng khóa trao đổi. Kết quả của họ dựa trên mô hình tính toán của mật mã và được nêu trong khuôn khổ của trình kiểm tra mô hình Cryp-toVerif [30]. Chúng hỗ trợ các giao thức trao đổi khóa bảo đảm xác thực nội bộ hoặc không nội bộ. Chúng cũng cho phép chia sẻ các oracle ngẫu nhiên giữa các protocol tổng hợp. Họ tuyên bố rằng đây là định lý tổng hợp đầu tiên về trao đổi khóa được nêu cho một công cụ xác minh giao thức tính toán và cũng là định lý đầu tiên cho phép tính linh hoạt như vậy. Như một trường hợp nghiên cứu, họ áp dụng các định lý thành phần của mình vào chứng minh TLS 1.3 Draft-18 và đã chính thức chứng minh điều đó.

Trong [31], các tác giả trình bày một khung mô hình mới giải thích cho tất cả các cuộc tấn công gần đây vào TLS, bao gồm cả những cuộc tấn công dựa vào mật mã yếu. Họ sử dụng ProVerif để đánh giá các chế độ và bản nháp khác nhau của TLS 1.3, đỉnh cao là phân tích biểu tượng đầu tiên của Draft-18 và phân tích tổng hợp đầu tiên của TLS 1.3+1.2. Các phân tích của họ phát hiện ra cả những lỗ hổng đã biết và mới đã ảnh hưởng đến thiết kế cuối cùng của Draft. Một số tính năng họ nghiên cứu không còn xuất hiện trong giao thức nhưng họ tin rằng kết quả phân tích vẫn hữu ích cho thể hệ sau như một lời cảnh báo cho giao thức

các nhà thiết kế và nhà phát triển có thể cố gắng giới thiệu lại các tính năng có vấn đề này trong tương lai.

Trong [32], các tác giả xem xét việc triển khai pro-tocol hơn là thiết kế. Họ đã trình bày một phân tích kỹ lưỡng về việc triển khai TLS thường được sử dụng bằng cách sử dụng phương pháp tiếp cận mang tính hệ thống được gọi là làm mờ trạng thái giao thức. Họ sử dụng máy học trạng thái, vốn chỉ dựa vào kiểm thử hộp đen, để suy ra máy trạng thái của việc triển khai giao thức, sau đó họ thực hiện phân tích thủ công các máy trạng thái thu được để kiểm tra xem việc triển khai có phù hợp với đặc điểm kỹ thuật hay không. Họ đã phân tích các cách triển khai TLS được sử dụng phổ biến nhất và phát hiện ra những sai sót mới.

Trong [33], các tác giả đã chính thức hóa và phân tích một biến thể của giao thức tín hiệu cho một loạt mục tiêu bảo mật bằng cách sử dụng cả ProVerif [15] và CryptoVerif [30]. Họ cũng đã triển khai giao thức tín hiệu trong ProScript, đây là ngôn ngữ dành riêng cho miền mới để viết mã giao thức mật mã. Việc triển khai trong ProScript có thể được thực thi trong các chương trình JavaScript và cũng được dịch tự động sang mô hình có thể đọc được trong phép tính pi được áp dụng. Phân tích của họ phát hiện ra một số điểm yếu của giao thức, bao gồm các cuộc tấn công mạo danh tấn công lặp lại chưa được báo cáo trước đây và các cuộc tấn công mạo danh xâm phạm chính. Hơn nữa, họ cũng đã triển khai các bản sửa lỗi và xác minh tính bảo mật của phiên bản đã sửa lỗi.

Trong [34], các tác giả thực hiện phân tích góc rộng về kiến trúc và quy trình bảo mật mạng truy cập vô tuyến (RAN) 5G cũng như các thách thức triển khai tiềm ẩn của nó do khuôn khổ bảo mật 5G được đề xuất. Nó không phải để cung cấp phân tích toàn diện về tính bảo mật của các lớp và thành phần mạng 5G mà là để đánh giá những thách thức quan trọng của các thông số kỹ thuật bảo mật 5G hiện tại cũng như triển vọng triển khai mạng trong tương lai. Nghiên cứu của họ nêu bật một số trường hợp và hạn chế về giao thức không an toàn tiềm ẩn do các yêu cầu hoặc giả định không khả thi. Một cuộc khảo sát về bảo mật và quyền riêng tư của công nghệ 5G có sẵn trong [35].

Cuối cùng, chúng tôi nhận xét rằng công việc này một phần dựa trên ấn phẩm trước đây của chúng tôi [28], trong đó chúng tôi đã lập mô hình và phân tích giao thức xác thực 5G EAP-TLS bằng Scyther [36]. Chúng tôi đã cải tiến và mở rộng công việc trước đây của mình theo nhiều hướng. Trước hết, chúng tôi sử dụng một ngôn ngữ hình thức biểu cảm hơn có thể mô tả các hàm do người dùng xác định và các bài kiểm tra tính bằng nhau trong công việc này. Ngôn ngữ này chính xác hơn Scyther trong việc mô hình hóa hành vi của giao thức. Thứ hai, chúng tôi xây dựng một mô hình chính thức chi tiết hơn về giao thức xác thực 5G EAP-TLS, bao gồm mô hình hóa tất cả các thành phần và kênh chính của giao thức. Trong khi, mô hình trong [28] chỉ tính đến hai thực thể là thiết bị người dùng và mạng. Chúng tôi coi mạng phục vụ và mạng gia đình là một thực thể duy nhất và chúng tôi không phân biệt các mô-đun chính của mạng gia đình. Cuối cùng, chúng tôi thực hiện phân tích toàn diện hơn về các yêu cầu bảo mật và thảo luận về những phát hiện chính của chúng tôi bằng cách chỉ ra nguyên nhân của từng điểm yếu. Chúng tôi cũng đề xuất một bản sửa lỗi đã được xác minh là an toàn.

BẢNG 2. Cú pháp các thuật ngữ.

$M, N ::=$	terms
a, b, c, k, m, n, s	names
x, y, z	variables
(M_1, \dots, M_k)	tuple
$h(M_1, \dots, M_k)$	constructor/destructor
$M = N$	term equality
$M <> N$	term inequality
$M \&\& M$	conjunction
$M M$	disjunction
$\text{not}(M)$	negation

BẢNG 3. Cú pháp của tiên trình.

$P, Q, R ::=$	processes
0	null process
$P Q$	parallel composition
$!P$	replication
$\text{new } n : t; P$	name restriction
$\text{in}(M, x : t); P$	message input
$\text{out}(M, N); P$	message output
$\text{if } M \text{ then } P \text{ else } Q$	conditional
$\text{let } x = M \text{ in } P \text{ else } Q$	term evaluation
$R(M_1, \dots, M_n)$	macro usage

III. Sơ bộ về phép tính PI ứng dụng Trong phần này, chúng tôi

trình bày cả cú pháp và ngữ nghĩa của phép tính pi được áp dụng [13], [16], là ngôn ngữ chính thức để mô hình hóa giao thức bảo mật và được phổ biến bởi mô hình ProVerif [15] người kiểm tra.

Ngữ pháp cơ bản của các thuật ngữ được sử dụng trong phép tính số pi ứng dụng được trình bày trong Bảng 2. Thuật ngữ có thể là tên đại diện cho một kênh hoặc mục dữ liệu. Một thuật ngữ cũng có thể là một biến hoặc một bộ thuật ngữ (M_1, \dots, M_k) . Các thuật ngữ được xây dựng bởi ứng dụng hàm tạo/hàm hủy được ký hiệu là $h(M_1, \dots, M_k)$, trong đó k là độ của hàm h . Chúng được sử dụng để đại diện cho các ứng dụng chức năng được gửi, chẳng hạn như mã hóa hoặc giải mã. Cụ thể, chúng tôi cung cấp cho các ứng dụng hàm một kiểu sắp xếp boolean. Thuật ngữ $M = N$ ($M <> N$) tương ứng thể hiện các phép thử đẳng thức (bất đẳng thức). Lưu ý rằng cả đẳng thức và bất đẳng thức đều hoạt động theo lý thuyết phương trình [37]. Thuật ngữ $M \&\& N$ dành cho phép kết hợp boolean, và $M || M$ dành cho phép phân tách boolean, chứ không phải (M) dành cho phép phủ định boolean.

Hành vi được mô hình hóa bởi các quy trình như trong Bảng 3. Quá trình null 0 đại diện cho một quá trình không làm gì cả. $P || Q$ là thành phần song song của các quá trình P và Q , được sử dụng để thể hiện những người tham gia chạy song song. Bản sao $!P$ là thành phần vô hạn của P (tức là $P | P | \dots$), thường được sử dụng để nắm bắt số phiên không giới hạn của một giao thức. Hạn chế tên mới $n : t; P$ liên kết tên n của loại t bên trong quy trình P . Việc đưa ra các tên bị hạn chế (hoặc tên riêng) rất hữu ích để nắm bắt cả các số ngẫu nhiên mới (ví dụ: mô hình hóa nonces và khóa) và các kênh riêng tư. Thông tin liên lạc được nắm bắt bởi đầu vào tin nhắn và đầu ra tin nhắn. Quá trình $\text{in}(M, x : t); P$ chờ một tin nhắn loại t từ kênh M và sau đó hoạt động như P với tin nhắn nhận được gắn với biến x , nghĩa là mọi sự xuất hiện tự do của x trong P đều đề cập đến tin nhắn nhận được.

BẢNG 4. Cú pháp khớp mẫu.

$T ::=$	patterns
$x : t$	typed variable
x	variable without explicit type
(T_1, \dots, T_n)	tuple
$= M$	equality test

Quá trình $\text{out}(M, N)$; P sẵn sàng gửi thuật ngữ N trên kênh M và sau đó chạy P. Trong cả hai trường hợp này, chúng ta có thể bỏ qua P khi nó là tiến trình null \emptyset . Điều kiện nếu M thì P còn lại Q là tiêu chuẩn: nó chạy P khi boolean Thuật ngữ M đánh giá là đúng và nó chạy Q khi M đánh giá một số giá trị khác. Để thuận tiện, các điều kiện có thể được viết tắt là M rồi P, khi Q là quá trình rỗng. Khi câu lệnh $\text{let } x = M \text{ trong } P$ khác Q gặp phải trong quá trình thực hiện quy trình, có hai kết quả có thể xảy ra. Nếu việc đánh giá số hạng M theo hàm hủy không thất bại (nghĩa là M tương đương với một số hạng khác không có hàm hủy nào theo lý thuyết phương trình), thì x bị ràng buộc với số hạng M và nhánh P được lấy. Ngược lại, nhánh Q sẽ được lấy. Tương tự, nó có thể được viết tắt là $\text{let } x = M \text{ trong } P$ khi Q là quá trình rỗng. Cuối cùng, chúng ta có $R(M_1, \dots, M_n)$, biểu thị việc sử dụng macro R với các số hạng M_1, \dots, M_n làm đối số.

Chúng tôi cũng bao gồm tính năng khớp mẫu (Bảng 4) được ProVerif hỗ trợ. Mẫu biến $x : t$ khớp với bất kỳ thuật ngữ nào thuộc loại t và liên kết thuật ngữ khớp với x. Mẫu biến x tương tự nhưng chỉ có thể được sử dụng khi loại x có thể được suy ra từ ngữ cảnh. Mẫu tuple (T_1, \dots, T_n) khớp với các bộ dữ liệu (M_1, \dots, M_n) trong đó mỗi thành phần M_i ($i = 1, \dots, n$) được so khớp đệ quy với T_i . Cuối cùng, mẫu $= M$ khớp với bất kỳ thuật ngữ N nào trong đó $M = N$.

Như trong phép tính số pi ứng dụng, các số hạng tuân theo lý thuyết phương trình. Xác định một lý thuyết phương trình với dấu hiệu của nó, chúng ta viết $M = N$ cho một đẳng thức modulo cho lý thuyết phương trình, và $M = N$ một bất đẳng thức modulo cho lý thuyết phương trình. (Chúng ta viết $M = N$ và $M = N$ tương ứng cho đẳng thức cú pháp và bất đẳng thức.) Lý thuyết phương trình được xác định bởi một tập hữu hạn các phương trình $M_i = N_i$, trong đó M_i và N_i là các thuật ngữ chỉ chứa các hàm tạo và biến. Sau đó, lý thuyết phương trình thu được từ tập hợp các phương trình này bằng cách đóng phản xạ, đối xứng và bắc cầu, đóng bằng thay thế (với mọi thay thế σ , nếu $M = N$ thì $\sigma M = \sigma N$) và đóng bằng ứng dụng ngữ cảnh (nếu $M = N$ thì $M\{M/x\} = N\{M/x\}$, trong đó $\{M/x\}$ là phép thay thế x bằng M).

Chúng tôi trình bày ngữ nghĩa hình thức trong Bảng 5. Định nghĩa bao gồm hai phần. Đầu tiên, chúng ta xác định ngữ nghĩa của các biểu thức: mối quan hệ $D \rightarrow U$ có nghĩa là biểu thức đóng D đánh giá thuật ngữ đóng có thể-không thành công U, có thể là thuật ngữ đóng M hoặc hằng số thất bại. Hai quy tắc đầu tiên của định nghĩa biểu thị rằng một thuật ngữ đóng M và không tự đánh giá được; Quy tắc thứ ba liên quan đến ứng dụng chức năng.

Đầu tiên nó đánh giá các đối số của hàm D_1, \dots, D_n đến U_1, \dots, U_n tương ứng. Sau đó, nó áp dụng quy tắc viết lại thứ j của h, $h(U)$ được khởi tạo bằng sự thay thế $j, 1, \dots, U_j$, U_j, n

BẢNG 5. Ngữ nghĩa hoạt động.

$D \Downarrow U$	
$\text{fail} \Downarrow \text{fail}$	
$h(D_1, \dots, D_n) \Downarrow \sigma U'_j$ if and only if	
$D_1 \Downarrow U_1, \dots, D_n \Downarrow U_n$,	
$\text{def}(h)$ consists of the rewrite rules	
$h(U'_{i,1}, \dots, U'_{i,n}) \rightarrow U'_i$ for $i \in \{1, \dots, k\}$,	
$\sigma U'_{j,1} = U_1, \dots, \sigma U'_{j,n} = U_n$, and	
for all $i \leq j$, for all $\sigma', \sigma' U'_{i,1} \neq U_1, \dots, \sigma' U'_{i,n} \neq U_n$.	
$E, \mathcal{P} \subseteq \{0\} \rightarrow E, \mathcal{P}$	(Nil)
$E, \mathcal{P} \subseteq \{P Q\} \rightarrow E, \mathcal{P} \subseteq \{P, Q\}$	(Par)
$E, \mathcal{P} \subseteq \{!P\} \rightarrow E, \mathcal{P} \subseteq \{P, !P\}$	(Repl)
$(\mathcal{N}_{\text{pub}}, \mathcal{N}_{\text{priv}}), \mathcal{P} \subseteq \{\text{new } a; P\} \rightarrow$	
$(\mathcal{N}_{\text{pub}}, \mathcal{N}_{\text{priv}} \subseteq \{a'\}), \mathcal{P} \subseteq \{P\{a'/a\}\}$	(Res)
where $a' \notin \mathcal{N}_{\text{pub}} \subseteq \mathcal{N}_{\text{priv}}$	
$E, \mathcal{P} \subseteq \{\text{out}(N, M); Q, \text{in}(N, x); P\} \rightarrow$	
$E, \mathcal{P} \subseteq \{Q, P\{M/x\}\}$	(I/O)
$E, \mathcal{P} \subseteq \{\text{let } x = D \text{ in } P \text{ else } Q\} \rightarrow$	
$E, \mathcal{P} \subseteq \{P\{M/x\}\}$ if $D \Downarrow M$	(Eval 1)
$E, \mathcal{P} \subseteq \{\text{let } x = D \text{ in } P \text{ else } Q\} \rightarrow$	
$E, \mathcal{P} \subseteq \{Q\}$ if $D \Downarrow \text{fail}$	(Eval 2)
$E, \mathcal{P} \subseteq \{\text{if true then } P \text{ else } Q\} \rightarrow$	
$E, \mathcal{P} \subseteq \{P\}$	(Cond 1)
$E, \mathcal{P} \subseteq \{\text{if } M \text{ then } P \text{ else } Q\} \rightarrow$	
$E, \mathcal{P} \subseteq \{Q\}$ if $M \neq \text{true}$	(Cond 2)

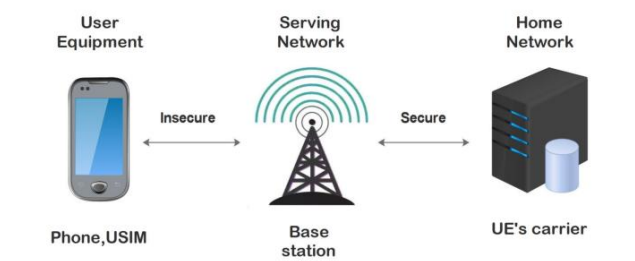
ơ, do đó $h(U_1, \dots, U_n) = h(\sigma U \sigma U)$ rút gọn, thành $\sigma U_{j,1}, \dots, \sigma U_{j,n}$.

Dòng cuối cùng kiểm tra xem quy tắc viết lại thứ j không thể được áp dụng.

Thứ hai, chúng tôi trình bày ngữ nghĩa của các quy trình bằng cách rút gọn các cấu hình ngữ nghĩa. Cấu hình ngữ nghĩa là một cặp (E, P) trong đó môi trường E là một cặp gồm hai tập hữu hạn tên $(N_{\text{pub}}, N_{\text{priv}})$ và P là tập hợp nhiều tập hữu hạn của các tiến trình khép kín. Tập N_{pub} chứa các tên công khai, tập N_{priv} chứa các tên riêng và tập hợp nhiều tiến trình P chứa các tiến trình hiện đang chạy. Cấu hình $((\{a_1, \dots, a_n\}, \{b_1, \dots, b_m\}), \{P_1, \dots, P_k\})$ tương ứng trực quan với quá trình $\text{new } b_1; \dots; \text{new } b_m; (P_1 | \dots | P_k)$. Cấu hình $((N_{\text{pub}}, N_{\text{priv}}), P)$ hợp lệ khi N_{pub} và N_{priv} tách rời nhau và $\text{fn}(P) \subseteq N_{\text{pub}} \cup N_{\text{priv}}$. Chúng tôi chỉ xem xét các cấu hình hợp lệ. Mối quan hệ rút gọn về cấu hình ngữ nghĩa được xác định trong Bảng 5.

Các quy tắc rút gọn xác định ngữ nghĩa của từng cấu trúc ngôn ngữ. Quy tắc Nil loại bỏ các tiến trình \emptyset vì chúng không làm gì cả. Quy tắc Par mở rộng các tác phẩm song song. Quy tắc Repl tạo một bản sao bổ sung của một quy trình được sao chép; vì quy tắc này có thể được áp dụng lại trên cấu hình kết quả, nên nó cho phép tạo số lượng bản sao không giới hạn của quy trình được sao chép. Quy tắc Res tạo một tên mới thay thế cho a và thêm nó vào tên riêng N_{priv} .

Tên mới a được yêu cầu không xuất hiện trong N_{priv} , chứa các tên miễn phí riêng tư ban đầu cũng như bất kỳ tên mới nào được tạo bởi ứng dụng Res trước đó, cũng như trong N_{pub} , chứa các tên miễn phí công khai. Quy tắc (I/O) cho phép giao tiếp giữa các tiến trình. Thông báo M được gửi bởi đầu ra và được nhận bởi đầu vào trong biến x,



HÌNH 1. Kiến trúc mạng 5G.

miễn là các kênh đầu ra và đầu vào bằng nhau. Các quy tắc (Eval 1) và (Eval 2) xác định ngữ nghĩa của việc đánh giá biểu thức. Họ đánh giá D. Trong trường hợp thành công, (Đánh giá 1) chạy P với kết quả M của đánh giá được thay thế cho x.

Trong trường hợp thất bại, (Đánh giá 2) chạy Q. Các quy tắc (Cond 1) và (Cond 2) xác định ngữ nghĩa của các điều kiện. Khi M đúng, (Cond 1) chạy P. Khi M khác true, (Cond 2) chạy Q.

Với quy trình giao thức P0, nó thường chạy song song với quy trình đối thủ Q trong quá trình xác minh.

Trong trường hợp này, cấu hình ban đầu là (Npub, Npriv), P0, Q.

IV. GIAO THỨC XÁC THỰC EAP-TLS 5G

Trong phần này, chúng tôi trình bày đánh giá chi tiết về giao thức xác thực 5G EAP-TLS theo tài liệu 3GPP TS 33.501 v15.4.0 [1].

Kiến trúc điển hình của mạng 5G được hiển thị trong Hình 1. Nó bao gồm ba thực thể chính: thiết bị người dùng (UE), mạng gia đình (HN) và mạng phục vụ (SN). Thiết bị người dùng đại diện cho thiết bị của thuê bao (ví dụ: điện thoại di động) được kết nối với mạng. Mạng gia đình là nhà cung cấp dịch vụ của thuê bao và là thực thể chính chịu trách nhiệm xác thực người dùng. Mạng phục vụ là nơi thiết bị người dùng có thể gắn trực tiếp (ví dụ: mạng không dây của trạm gốc). Lưu ý rằng trong công việc này, chúng tôi phân biệt giữa mạng gia đình, là mạng mà người dùng đăng ký và mạng phục vụ, là trạm cơ sở thực tế mà điện thoại di động kết nối tới. Trong một số trường hợp, mạng gia đình có thể giống với mạng phục vụ, trong khi trong một số trường hợp khác, chẳng hạn như trường hợp chuyển vùng, chúng lại khác.

Thiết bị người dùng thường liên lạc với mạng phục vụ thông qua kênh không dây, kênh này công khai và chịu sự tấn công của những người dùng độc hại. Vì vậy, thật hợp lý khi coi nó là một kênh không an toàn. Ngược lại, kênh giữa mạng gia đình và mạng phục vụ là riêng tư và nội bộ đối với các nhà khai thác mạng. Kênh này có thể được coi là an toàn, như trong các công trình liên quan về phân tích giao thức 5G AKA [19], [20].

Sau đây, chúng tôi trình bày chi tiết các mô-đun chính của ba thực thể có liên quan đến giao thức xác thực EAP-TLS 5G. Trong thiết bị người dùng, mô-đun chính là Mô-đun nhận dạng thuê bao đa năng (USIM), chứa hai thành phần chính có liên quan sau đây:

- Mã định danh vĩnh viễn đăng ký (SUPI), được sử dụng làm danh tính thuê bao duy nhất và

lâu dài;

- khóa bất đối xứng công khai pkHN của mạng gia đình tương ứng.

Mô-đun này cũng chứa khóa đối xứng dài hạn K, được sử dụng làm bí mật chung giữa các thuê bao và mạng gia đình tương ứng của họ và một bộ đếm, được gọi là số thứ tự SQN. Tuy nhiên, chúng không được sử dụng trong giao thức xác thực 5G EAP-TLS mà được sử dụng trong giao thức 5G AKA.

Mô-đun chính của mạng phục vụ là Chức năng neo bảo mật (SEAF), hoạt động như một 'người trung gian' trong quá trình xác thực giữa thiết bị người dùng và mạng gia đình của nó. Nó có thể được xem như một trình xác thực minh bạch bằng cách chuyển tiếp tất cả các tin nhắn giữa thiết bị người dùng và mạng gia đình. Ngược lại với giao thức 5G AKA, mạng phục vụ không tham gia vào việc tính toán quy trình xác thực 5G EAP-TLS mà tham gia vào thành phần định tuyến cấp thấp hơn.

Mạng gia đình là mạng phức tạp nhất và chứa các mô-đun chính sau:

- Chức năng Máy chủ Xác thực (AUSF), thực

hiện xác thực mẫu với thiết bị người dùng. Khi đưa ra quyết định xác thực, nó sẽ gọi một dịch vụ phụ trợ để tính toán dữ liệu xác thực và vật liệu khóa.

- mô-đun Quản lý Dữ liệu Hợp nhất (UDM), là một thực thể lưu trữ các chức năng liên quan đến quản lý dữ liệu. Hai chức năng chính là Chức năng xử lý và kho lưu trữ thông tin xác thực (ARPF) và Chức năng loại bỏ mã định danh đăng ký (SIDF).

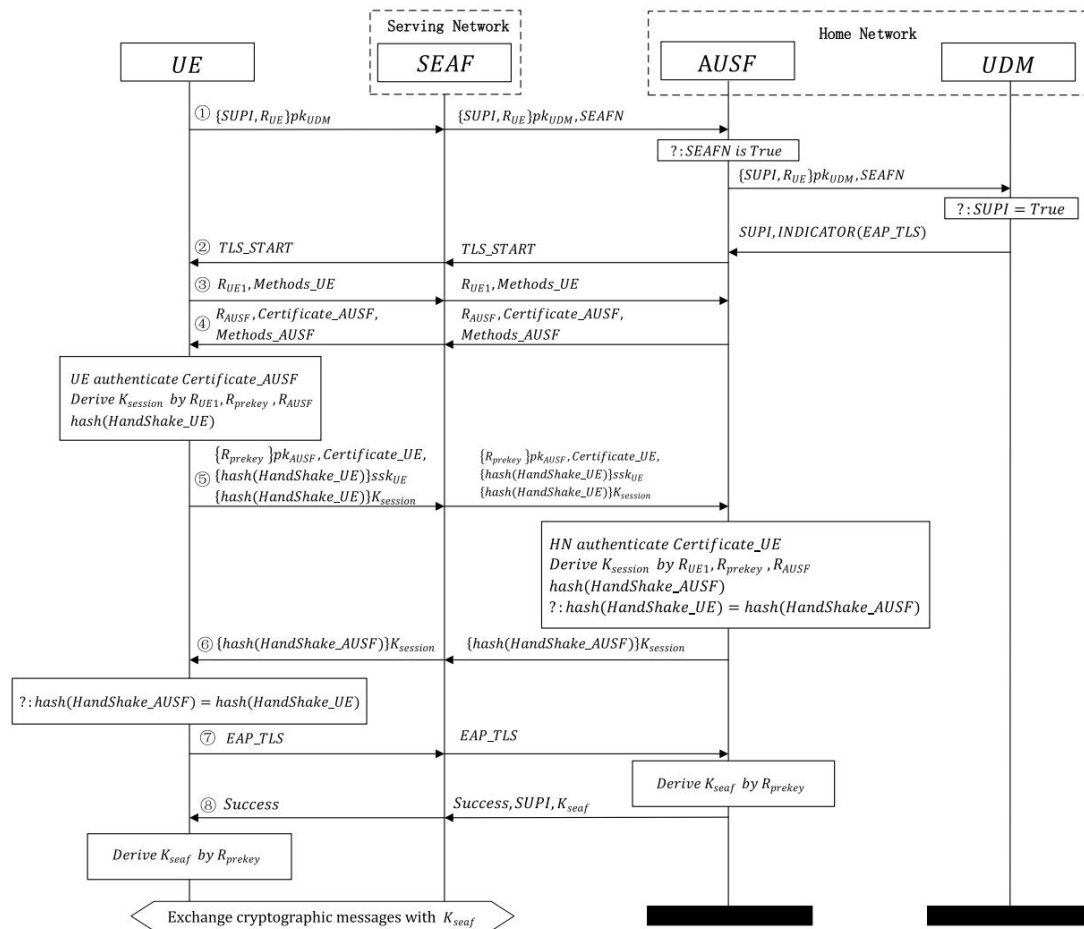
ARPF chọn phương thức xác thực dựa trên nhận dạng thuê bao và chính sách được định cấu hình, sau đó tính toán dữ liệu xác thực và tài liệu khóa cho AUSF. SIDF chịu trách nhiệm giải mã tin nhắn từ người đăng ký và cũng truy xuất danh tính SUPI của người đăng ký.

A. THỰC HIỆN GIAO THỨC BÌNH THƯỜNG

Khi được mạng gia đình chọn làm phương thức xác thực, giao thức 5G EAP-TLS sẽ được thực hiện giữa thiết bị người dùng và mạng gia đình thông qua mạng phục vụ. Chúng tôi mô hình hóa giao thức được chỉ định trong tài liệu 3GPP TS 33.501 phiên bản 15.4.0 [1]. Chúng tôi cũng muốn lưu ý rằng việc xây dựng mô hình chính thức của giao thức 5G EAP-TLS không phải là một nhiệm vụ dễ dàng, do tài liệu đặc tả cực kỳ phức tạp, kéo dài hàng trăm trang. Hơn nữa, bản chất không chính thức của các yêu cầu bảo mật khiến cho việc lập mô hình và phân tích càng khó khăn hơn. Các bước chi tiết của giao thức xác thực 5G EAP-TLS được mô tả trong Hình 2.

- 1) Ban đầu, thiết bị người dùng bắt đầu yêu cầu kết nối và chuyển tiếp mã hóa SUPI và số RUE ngẫu nhiên tới mạng phục vụ.

Mã hóa được ký hiệu là SUCI và ký hiệu aenc(·, pkUDM) thể hiện mã hóa bất đối xứng của phần tử đầu tiên sử dụng khóa chung của UDM.



HÌNH 2. Giao thức xác thực EAP-TLS 5G.

- 2) Mạng phục vụ sẽ bắt đầu quy trình xác thực khi nhận được tin nhắn SUCI và chuyển tiếp SUCI cùng với tên SEAFN của anh ấy đến mạng chủ.

- 3) Mô-đun AUSF của mạng gia đình sẽ kiểm tra xem tên SEAFN có phải là tên của mạng phục vụ hợp pháp hay không. Nếu quá trình kiểm tra thành công thì AUSF sẽ gửi thông báo tới UDM, trong đó hàm SDF được gọi để giải mã SUCI nhằm lấy danh tính SUPI của người đăng ký.

Sau đó, UDM sẽ kiểm tra xem SUPI thu được có phải là danh tính hợp pháp của người đăng ký hay không.

- 4) Nếu bước kiểm tra trên đạt, mô-đun UDM sẽ gửi phản hồi bao gồm SUPI và phương thức xác thực đã chọn (được biểu thị bằng INDICATOR(EAP_TLS)) tới AUSF. Trong trường hợp này, nó biểu thị giao thức 5G EAP-TLS.

- 5) Sau đó, AUSF gửi tin nhắn TLS_START đến thiết bị người dùng thông qua mạng phục vụ để báo hiệu việc bắt đầu quy trình xác thực EAP-TLS.

- 6) Thiết bị người dùng tạo ra một RUE1 mới và gửi nó tới SEAF cùng với thông tin về nó

các thuật toán được hỗ trợ Methods_UE. SEAF sẽ chuyển tiếp thông điệp này trực tiếp tới AUSF.

- 7) AUSF phản hồi một tin nhắn tới thiết bị người dùng thông qua SEAF, trong đó có RAUSF nonce , chứng chỉ mạng gia đình Chứng chỉ_AUSF và thông tin về các thuật toán được hỗ trợ của nó Methods_AUSF.
- 8) Khi nhận được tin nhắn Chứng chỉ_AUSF, trước tiên thiết bị người dùng sẽ xác minh tính hợp lệ của chứng chỉ này. Trong trường hợp xác minh thành công, thiết bị người dùng sẽ tạo một Rprekey nonce mới, được gọi là khóa chính trước và lấy khóa phiên Ksession bằng cách sử dụng Rprekey, RUE1 và RAUSF . Chúng tôi tham khảo [2] để biết chi tiết về đạo hàm này. Sau đó, thiết bị người dùng tính toán hàm băm (HandShake_UE) của các thông báo bắt tay trước đó (tức là các thông báo trong các bước , và). Thiết bị người dùng chuyển tiếp đến mạng phục vụ SEAF các thông báo sau: mã hóa {Rprekey}pkAUSF của khóa chính trước bằng khóa chung của AUSF, mã hóa {hash(HandShake_UE)} Ksession của hàm băm sử dụng phiên dẫn xuất chia khóa và chữ ký

$\{ \text{hash}(\text{HandShake_UE}) \} \text{sskUE}$ với khóa ký riêng sskUE . Sau đó SEAF chuyển tiếp tin nhắn trên tới AUSF trực tiếp.

- 9) AUSF sau đó kiểm tra chứng chỉ của thiết bị người dùng.
- Nếu hợp lệ, nó sẽ giải mã $\{ \text{Rprekey} \} \text{pkAUSF}$ để lấy khóa chính trước và tính khóa phiên Ksession cùng với các nonces trước đó là RUE1 và RAUSF .
- Sau đó, nó thu được hàm băm $\{ \text{HandShake_UE} \}$ bằng cách giải mã $\{ \text{hash}(\text{HandShake_UE}) \} \text{Ksession}$ và so sánh với giá trị trong chữ ký $\{ \text{hash}(\text{HandShake_UE}) \} \text{sskUE}$ bằng cách sử dụng khóa ký công khai spkUE của UE.
- AUSF cũng tính toán hàm băm $\{ \text{HandShake_AUSF} \}$ của các tin nhắn bắt tay trước đó của anh ấy và so sánh với giá trị băm nhận được từ hàm băm thiết bị của người dùng $\{ \text{HandShake_UE} \}$. Nếu chúng bằng nhau, AUSF sẽ mã hóa hàm băm này bằng khóa phiên Ksession và gửi nó trở lại thiết bị người dùng.
- 10) Thiết bị người dùng giải mã tin nhắn và nhận hàm băm $\{ \text{HandShake_AUSF} \}$ và so sánh với hàm băm của chính nó $\{ \text{HandShake_UE} \}$. Nếu chúng bằng nhau, thiết bị người dùng sẽ xác nhận thành công và gửi tin nhắn EAP_TLS tới SEAF, tin nhắn này sẽ chuyển tiếp tới AUSF.
- 11) Khi AUSF nhận được tin nhắn EAP_TLS , nó tạo ra một khóa Kseaf mới dựa trên khóa chính Rprekey [2] và gửi nó đến SEAF cùng với danh tính của SUPI thiết bị người dùng và một thông báo Thành công.
- 12) SEAF chuyển tiếp thông báo Thành công đến thiết bị người dùng, kết thúc quy trình xác thực ở phía máy chủ. Khi nhận được thông báo này, thiết bị người dùng sẽ tạo khóa Kseaf theo cách tương tự như AUSF.
- Sau đó, khóa Kseaf sẽ được sử dụng để bảo mật các liên lạc tiếp theo giữa thiết bị người dùng và mạng.

B. CÁC ĐẶC TÍNH BẢO MẬT BẮT BUỘC Tài liệu 3GPP TS

33.501 mô tả các yêu cầu bảo mật một cách không chính thức. Bây giờ chúng tôi trình bày các phân ảnh hưởng trực tiếp đến giao thức EAP-TLS. Đối với mỗi yêu cầu, chúng tôi chỉ ra các văn bản có liên quan trong tài liệu gốc.

Chúng tôi trích dẫn các yêu cầu xác thực và ủy quyền trong Hình 3. Các yêu cầu xác thực đăng ký và ủy quyền UE được hiển thị trong Hình 3 chỉ ra rằng cả mạng phục vụ và mạng gia đình đều có thể xác thực danh tính của thuê bao, sao cho chỉ những thuê bao trung thực mới có thể truy cập vào mạng. Sau đó, khi các yêu cầu xác thực mạng phục vụ và ủy quyền mạng phục vụ chỉ ra, các thuê bao phải đảm bảo rằng việc xác thực chỉ có thể thành công với mạng phục vụ được mạng gia đình của họ ủy quyền, sao cho mạng phục vụ không thể giả mạo các yêu cầu xác thực với mạng gia đình dành cho những thuê bao không gắn liền với một trong các trạm cơ sở của nó. Nói cách khác, giao thức xác thực 5G EAP-TLS sẽ cung cấp xác thực lẫn nhau giữa các thuê bao và mạng gia đình của họ. Việc xác thực là

5.1.2 Authentication and Authorization

The 5G system shall satisfy the following requirements.

Subscription authentication: The serving network shall authenticate the Subscription Permanent Identifier (SUPI) in the process of authentication and key agreement between UE and network.

Serving network authentication: The UE shall authenticate the serving network identifier through implicit key authentication.

UE authorization: The serving network shall authorize the UE through the subscription profile obtained from the home network. UE authorization is based on the authenticated SUPI.

Serving network authorization by the home network: Assurance shall be provided to the UE that it is connected to a serving network that is authorized by the home network to provide services to the UE. This authorization is 'implicit' in the sense that it is implied by a successful authentication and key agreement run.

Access network authorization: Assurance shall be provided to the UE that it is connected to an access network that is authorized by the serving network to provide services to the UE. This authorization is 'implicit' in the sense that it is implied by a successful establishment of access network security. This access network authorization applies to all types of access networks.

HÌNH 3. Xác thực và ủy quyền (từ [1] trang 21).

5.1.3 Confidentiality

The following security features are provided with respect to confidentiality of data on the network access link:

cipher key agreement: the property that the MS and the SN agree on a cipher key that they may use subsequently;

confidentiality of user data: the property that user data cannot be overheard on the radio access interface;

HÌNH 4. Tính bảo mật (từ [38] trang 15).

đạt được khi chúng đồng ý về danh tính của nhau cũng như về khóa chính được sử dụng để lấy khóa phiên.

Do đó, chúng tôi giải thích các yêu cầu như các thuộc tính xác thực sau:

A1 Cả mạng nhà và

thuê bao phải thống nhất về danh tính của nhau sau khi kết thúc thành công.

A2 Cả mạng gia đình và thuê bao phải thống nhất về khóa chính Rprekey sau khi kết thúc thành công.

Chúng tôi trích dẫn các yêu cầu bảo mật trong Hình.4 và Hình.5. Chúng tôi cũng giả định rằng người dùng và mạng đã hoàn tất việc trao đổi chứng chỉ và khóa chung của họ, việc này thường được thực hiện bằng phương pháp thiết lập ngoài băng tần hoặc cài đặt trước khóa chung.

Mặc dù tài liệu TS 33.501 không chỉ định rõ ràng tính bảo mật của khóa chính Rprekey hoặc phiên

5.1.1 User identity confidentiality

The following security features related to user identity confidentiality are provided:

user identity confidentiality: the property that the permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;

HÌNH 5. Bảo mật danh tính người dùng (từ [38] trang 14).

khóa Ksession, thỏa thuận khóa mật mã và tính bảo mật của dữ liệu người dùng được hiển thị trong Hình 4 ngụ ý mạnh mẽ tính bảo mật của khóa phiên Ksession, lấy khóa chính Rprekey làm hạt giống. Hơn nữa, cùng một khóa phiên Ksession không bao giờ được thiết lập hai lần. Điều này sẽ được phân tích như một phần của các thuộc tính thỏa thuận nội tại trên phiên K khóa đã thiết lập cho các cặp bên khác nhau. Ngoài ra, tính bảo mật danh tính người dùng được hiển thị trong Hình.5 ngụ ý rằng SUPI phải được coi là nhạy cảm và phải được giữ bí mật vì

nó xác định duy nhất người dùng.

Cụ thể, chúng tôi giải thích các yêu cầu như sau thuộc tính bí mật.

- S1 Kẻ tấn công không thể lấy được SUPI nhận dạng của một thuê bao trung thực.
- S2 Kẻ tấn công không thể lấy được khóa chính Rprekey của một thuê bao trung thực.
- S3 Kẻ tấn công không thể lấy được khóa phiên Ksession của một thuê bao trung thực.

V. MÔ HÌNH CHÍNH THỨC CỦA GIAO THỨC XÁC THỰC EAP-TLS

5G Trong phần này, chúng tôi trình bày

mô hình chính thức của giao thức 5G EAP-TLS trong phép tính pi ứng dụng, sau đó chúng tôi trình bày cách chính thức hóa các thuộc tính bảo mật dự kiến.

A. MÔ HÌNH GIAO THỨC BIỂU TƯỢNG

1) MÔ HÌNH TẤN CÔNG VÀ SỰ HOÀN HẢO
GIẢ ĐỊNH MÃ HÓA

Chúng tôi coi tất cả những người tham gia giao thức (tức là thiết bị và mạng của người dùng) đều trung thực. Tất cả đều hoạt động trung thực theo đặc tả giao thức. chúng tôi cũng xem xét sự tồn tại của kẻ tấn công độc hại, kẻ có toàn quyền kiểm soát mạng. Kẻ tấn công có thể gửi, chặn, giả mạo và phát lại tin nhắn trên các kênh công cộng. Tuy nhiên, khả năng chặn tin nhắn của kẻ tấn công bị hạn chế theo giả định mật mã hoàn hảo, tức là kẻ tấn công chỉ có thể giải mã tin nhắn được mã hóa khi và chỉ khi anh ta sở hữu đúng khóa. Mô hình kẻ tấn công này được gọi là mô hình Dolev-Yao [17].

Trong giả định mật mã hoàn hảo, chúng tôi giải thích các nguyên hàm mật mã như các hàm tượng trưng. Dưới đây chúng tôi chỉ định mã hóa đối xứng bằng hàm tạo nhị phân senc, hàm này nhận hai đối số loại chuỗi bit và khóa tương ứng và trả về mã hóa loại chuỗi bit.

Việc giải mã đối xứng được chỉ định bởi hàm tạo sdec.
Tính chất số học của quá trình mã hóa và giải mã được đặc trưng bởi phương trình $sdec(senc(m, k), k) = m$, nghĩa là với văn bản mật mã $senc(m, k)$, việc giải mã bằng cùng khóa k sẽ trả về tin nhắn M .

Trong khi giải mã bằng một số khóa khác sẽ không thành công.

```
fun senc(chuỗi bit,khóa):chuỗi bit.  
giảm forall m:bitstring,k:key; sdec(senc(m,k),k) = m.
```

Để mã hóa và giải mã bất đối xứng, chúng tôi xác định hàm tạo đơn nhất pk để nắm bắt khái niệm xây dựng một cặp khóa, lấy khóa riêng loại skey làm đối số và trả về khóa chung loại pkey. Tương tự, việc mã hóa và giải mã lần lượt được thực hiện bởi các toán tử aenc và adec .

```
vui pk(skey): pkey.  
fun aenc(chuỗi bit, pkey): chuỗi bit.  
giảm forall m:bitstring,sk:skey; adec(aenc(m,pk(sk)),sk)=m.
```

Tương tự như mã hóa bất đối xứng, chữ ký số sử dụng một cặp khóa. Một là khóa riêng loại sskey để ký tin nhắn và khóa còn lại là khóa chung loại spkey để kiểm tra chữ ký. Chúng tôi sử dụng hàm tạo spk để ánh xạ khóa chung tới khóa riêng tương ứng. Dấu hiệu xây dựng để xây dựng chữ ký bằng khóa riêng là tiêu chuẩn. Dấu kiểm tra hàm hủy kiểm tra chữ ký bằng khóa chung và trả về thông báo khi chữ ký đúng.

```
fun spk(sskey): spkey.  
dấu hiệu vui nhận(bitstring, sskey):  
bitstring. giảm forall m: bitstring,  
k: sskey; checksign(sign(m,k),spk(k))=m.
```

Ngoài ra, chúng tôi xác định hàm băm và hàm chuyển đổi loại cho mục đích lập mô hình. Hàm băm được biểu diễn dưới dạng hàm tạo h nhận ba thông báo đầu vào và trả về bản tóm tắt của các thông báo này. Bộ chuyển đổi kiểu chỉ đơn giản là một hàm tạo dữ liệu đặc biệt b2k, nhận đầu vào kiểu chuỗi bit và trả về giá trị kiểu khóa.

```
fun h(chuỗi bit,chuỗi bit,chuỗi bit): bitstring.  
fun b2k(chuỗi bit):key.
```

Theo cuộc thảo luận trước đây của chúng tôi, UE liên lạc với SEAF thông qua kênh không dây công khai và chịu sự tấn công của những người dùng độc hại. Vì vậy, chúng tôi sử dụng kênh công cộng c1 để đại diện cho kênh giữa UE và SEAF.
Ngược lại, kênh giữa AUSF và SEAF, cũng như AUSF và UDM, là kênh riêng tư và nội bộ đối với các nhà khai thác mạng. Do đó, chúng tôi khai báo kênh riêng c2 đại diện cho kênh giữa SEAF và AUSF và kênh riêng c3 đại diện cho kênh giữa AUSF và UDM.

c1: kênh miễn phí.
c2: kênh miễn phí [riêng tư].
c3 miễn phí: kênh [riêng tư].

2) QUY TRÌNH THIẾT BỊ NGƯỜI DÙNG ĐẦU

tiên, nó khai báo nonce Rue, sau đó mã hóa cả SUPI và Rue bằng khóa chung của UDM và xuất văn bản mật mã trên kênh chung c1. Chúng tôi nhận thấy rằng những kẻ tấn công có thể truy cập được kênh công khai này. Sau đó, quy trình UE chờ một thông báo đầu vào (được liên kết với biến Startx trên kênh c1. Sau đó, UE tạo và xuất ra một nonce Rue1 mới trên kênh c1 và chờ đầu vào có dạng (Rausfx, CertAUSFx).

Khi nhận được thông báo này, UE sẽ kiểm tra xem phần tử thứ hai của bộ dữ liệu này có phải là chữ ký của chứng chỉ CertAUSF của mạng nhà hay không. Nếu nó hợp lệ, UE sẽ tạo một Rprekey nonce đại diện cho khóa chính trước và tính toán hàm băm của Rue1, Rausfx và Rprekey, được chuyển đổi thành khóa Ksession bằng cách sử dụng bộ chuyển đổi loại b_to_k. Sau đó, UE tính toán senc mã hóa (HSUE,Ksession), dấu hiệu đặc trưng (HSUE,sskUE) của các thông điệp bắt tay HSUE và aenc mã hóa (Rprekey, pkAUSF) của khóa chính Rprekey bằng cách sử dụng khóa chung pkAUSF của mạng gia đình. Sau khi gửi các tin nhắn này trên kênh c1 cùng với chứng chỉ CertUE của người dùng , UE đợi HSAUSFx đầu vào và giải mã nó bằng khóa Ksession. Nếu quá trình giải mã trả về các thông báo bắt tay phải (tức là nó bằng HSUE), thì UE sẽ gửi thông báo EAPM, thông báo này được sử dụng để thông báo cho AUSF rằng quá trình xác thực đã được thông qua. và chờ thông báo thành công SUCMx từ mạng. Ngoài ra, chúng tôi chèn các sự kiện AcceptUE(Rue1), termUE(Rausfx) và sendPrek(prekey) trong quy trình để mã hóa các thuộc tính xác thực.

hãy để UE(pkAUSF:pkey,pkUDM:pkey,spkAUSF:spkey,
spkUE:spkey,sskUE:sskey) = new
Rue:bitstring;
out(c1,aenc((SUPI,Rue),pkUDM));
in(c1,Startx:bitstring);
Rue1 mới: chuỗi bit;
out(c1,Rue1);
in(c1,(Rausfx:bitstring,CertAUSFx:bitstring)); let
(=CertAUSF) = CertAUSFx trong
Rprekey:bitstring mới; let
prekey = Rprekey in let a
= h(Rue1,Rausfx,prekey) in let
Ksession = b_to_k(a) in let
HSUE = (Startx,Rue1,Rausfx,CertAUSFx) trong sự kiện
chấp nhậnUE(Rue1); sự kiện
sendPrek(prekey); out(c1,
(aenc(prekey,pkAUSF),CertUE,
sign(HSUE,sskUE),senc(HSUE,Ksession)));
in(c1,HSAUSFx:chuỗi bit); let
(=HSUE) = sdec(HSAUSFx,Ksession) trong
EAPM:bitstring mới;
out(c1,EAPM);
in(c1,SUCMx);
thuật ngữ sự kiệnUE(Rausfx).

3) QUY TRÌNH MẠNG PHỤC VỤ Chúng tôi xử lý

mạng phục vụ như một thành phần định tuyến cấp thấp hơn và mô hình hóa hành vi của nó bằng quy trình SEAF sau . Chức năng chính của nó là chuyển tiếp các tin nhắn giữa thiết bị người dùng và mạng gia đình một cách xuyên suốt. Hơn nữa, trong mô hình tin cậy của chúng tôi, kết nối giữa mạng phục vụ và mạng gia đình được coi là an toàn và không thể truy cập được đối với những kẻ tấn công. Vì vậy, chúng tôi tuyên bố kênh này (tức là kênh c2 đang được xử lý) là riêng tư.

Ngược lại, kênh giữa thiết bị người dùng và mạng phục vụ là công khai và có thể truy cập được đối với những kẻ tấn công (tức là kênh c1 được khai báo trong quy trình sau). Đặt SEAF(pkAUSF:pkey,pkUDM:pkey,spkAUSF:spkey,

spkUE:spkey) = in(c1,x1:bitstring); out(c2,(x1,SEAFN));
in(c2,x2:chuỗi
bit); out(c1,x2);
in(c1,x3:chuỗi bit);
out(c2,x3); in(c2,

(x4:bitstring,x5:bitstring)); out(c1,
(x4,x5)); in(c1,
(x6:bitstring,x7:bitstring,
x8:bitstring,x9:bitstring));
out(c2,(x6,x7,x8,x9));
in(c2,x10:chuỗi bit);
out(c1,x10);
in(c1,EAPMx);
out(c2,EAPMx);
in(c2,SUCMx);
out(c1,SUCMx).

4) QUY TRÌNH MẠNG GIA ĐÌNH Chúng tôi lập

mô hình mạng gia đình bằng hai quy trình, quy trình AUSF và quy trình UDM . Trong quy trình AUSF, trước tiên nó nhận được một tin nhắn đầu vào (SUPIx, SEAFNx) trên kênh c2 từ SEAF và kiểm tra xem SEAFNx có phải là tên mạng phục vụ hợp pháp SEAFN hay không. Nếu kiểm tra thành công, nó sẽ chuyển tiếp tin nhắn này tới UDM trên kênh riêng c3.

Sau đó AUSF nhận được tin nhắn Startx trên kênh c3 từ UDM và chuyển tiếp tin nhắn này tới SEAF. Sau đó AUSF nhận được một tin nhắn và giới hạn với biến Rue1x và tạo ra một Rausf nonce mới và xuất nó cùng với chứng chỉ của nó. AUSF sau đó chờ đợi một thông báo bao gồm bốn phần tử (tương ứng với biến y, CertUEx, t và z). AUSF kiểm tra xem CertUEx có phải là chứng chỉ của UE hay không và nếu đúng như vậy, nó sẽ giới hạn việc giải mã y với biến prekeyx. AUSF sau đó tính toán hàm băm của Rue1x, Rausf và prekeyx và chuyển đổi hàm băm này thành khóa Ksessionx. Sau đó, AUSF sẽ giải mã tin nhắn đầu vào z bằng khóa Ksessionx và kiểm tra chữ ký của t bằng khóa chung spkUE của UE. Cả hai lần kiểm tra sẽ trả về các thông báo bắt tay được biểu thị bằng bộ HSAUSF.

Nếu kiểm tra thành công, AUSF sẽ xuất mã hóa HSAUSF bằng khóa Ksessionx. Và sau đó AUSF chờ gửi tin nhắn thành công SUCM sau khi nhận được tin nhắn EAPMx. Tương tự, chúng ta thêm sự kiện AcceptPrek(prekeyx),

chấp nhậnAUSF(Rausf) và termAUSF(Rue1x) để kiểm tra các thuộc tính xác thực.

Theo đó, trong quy trình UDM, nó nhận được tin nhắn đầu vào (x, SEAFNx) trên kênh c3, sau đó giải mã x bằng khóa riêng của nó, khóa này trả về một bộ dữ liệu (SUPIx, Ruex).

Quá trình UDM tiếp tục nếu phần tử đầu tiên của bộ dữ liệu là SUPI nhận dạng của UE. Sau đó UDM chuyển tiếp thông tin khởi đầu đến AUSF để bắt đầu bắt tay.

```
hãy để AUSF(skAUSF:skey,pkUE:pkey,spkUE:spkey,
sskAUSF:sskey,spkAUSF:spkeyg) = in(c2,
(SUPIx:bitstring,SEAFNx:bitstring)); nếu SEAFNx
= SEAFN thì out(c3,
(SUPIx,SEAFNx)); in(c3,
Startx:bitstring); out(c2,
Startx); in(c2,
(Rue1x:bitstring)); Rausf
mới:chuỗi bit; out(c2,
(Rausf,CertAUSF)); in(c2,
(y:bitstring,CertUEx:bitstring,t:bitstring,
z:bitstring));
let (=CertUE) = CertUEx trong
let prekeyx = adec(y,skAUSF) trong
let b = h(Rue1x,Rausf,prekeyx) trong
let Ksessionx = b_to_k(b) trong
HSAUSF mới:bitstring; let
HSAUSF = (Startx,Rue1x,Rausf,CertAUSF) trong let
(=HSAUSF) = sdec(z,Ksessionx) in let
(=HSAUSF) = checksign(t,spkUE) trong sự kiện
AcceptPrek(prekeyx); sự kiện
chấp nhậnAUSF(Rausf);
out(c2,senc(HSAUSF,Ksessionx));
in(c2,EAPMx);
SUCM mới:chuỗi bit;
out(c2,SUCM);
thời hạn sự kiệnAUSF(Rue1x).
```

```
hãy để UDM(skUDM:skey) =
in(c3,(x:bitstring,SEAFNx:bitstring)); let
(SUPIx:bitstring,Ruex:bitstring) = adec(x,skUDM) trong nếu SUPIx
= SUPI thì new
start:bitstring;
out(c3,bắt đầu).
```

5) QUY TRÌNH GIAO THỨC ĐẦU

tiên, nó tạo ra các khóa riêng để mã hóa và chữ ký bất đối xứng, đồng thời xuất ra các khóa chung tương ứng trên kênh c1, c2 và c3. SEAFN là tên mạng phục vụ được sử dụng để tạo ra khóa neo. Nó cũng được phát trên kênh công cộng và có thể truy cập được đối với những kẻ tấn công.

Sau đó, quy trình giao thức là thành phần song song của việc sao chép vô hạn các quy trình UE, SEAF, AUSF và UDM.

```
xử lý
skUE mới:skey;
skAUSF mới: skey;
skUDM mới:skey;
sskAUSF mới: sskey;
sskUE mới:sskey;
SEAFN mới:chuỗi bit; đặt
pkUE = pk(skUE) vào out(c1,pkUE);
out(c2,pkUE);out(c3,pkUE);
```

```
đặt pkAUSF = pk(skAUSF) vào out(c1,pkAUSF);
out(c2,pkAUSF);out(c3,pkAUSF); đặt
pkUDM = pk(skUDM) vào out(c1,pkUDM);
out(c2,pkUDM);out(c3,pkUDM); đặt
spkAUSF = spk(sskAUSF) vào out(c1,spkAUSF);
out(c2,spkAUSF);out(c3,spkAUSF); đặt
spkUE = spk(sskUE) vào out(c1,spkUE);
out(c2,spkUE);out(c3,spkUE);
out(c1,SEAFN);out(c2,SEAFN);out(c3,SEAFN); ( (!
UE(pkAUSF,pkUDM,spkAUSF,spkUE,sskUE)) | (!
SEAF(pkAUSF,pkUDM,spkAUSF,spkUE)) | (!
AUSF(skAUSF,pkUE,spkUE,sskAUSF,spkAUSF))
| (!UDM(skUDM)))
```

B. QUY CÁCH TÀI SẢN BẢO ĐẢM

Trong ProVerif, một dữ kiện được mô hình hóa như một thuật ngữ cơ bản. Để chứng minh tính bí mật của thuật ngữ M, ProVerif về cơ bản giải quyết vấn đề về khả năng tiếp cận, tức là liệu kẻ tấn công có thể đạt đến trạng thái có sẵn thuật ngữ M hay không. Trong công việc này, ProVerif thực hiện các truy vấn sau trong mô hình giao thức để kiểm tra tính bảo mật của danh tính SUPI của người dùng và khóa chính Rprekey:

kẻ tấn công truy vấn(SUPI)

kẻ tấn công truy vấn (prekey)

Các thuộc tính xác thực được ghi lại bằng các xác nhận tương ứng, có thể thể hiện mối quan hệ giữa các sự kiện dưới dạng '' nếu một số sự kiện đã được thực thi trong giao thức thì một số sự kiện khác đã được thực thi trước đó.'' Trong ProVerif, các sự kiện thuộc về dạng sự kiện e(M1, . .

, Mn) và truy vấn của một xác nhận tương ứng là

truy vấn x1 : , xn : tn; sự kiện(e(M1, . . , Mj))

t1, . . . sự kiện(e (N1, . . ,Nk))

trong đó các số hạng M1, . . . , Mj , N1, . . . ,Nk được xây dựng bằng cách áp dụng các hàm tạo cho các biến x1, . . . , xn. Truy vấn được thỏa mãn nếu, với mỗi lần xuất hiện của sự kiện e(M1, . . . , Mj), có sự thực thi trước đó của sự kiện e (N1, . . . ,Nk). Ngoài ra còn có một biến thể mạnh mẽ hơn của khẳng định tương ứng, trong đó có thể nắm bắt được mối quan hệ một đối một giữa các sự kiện. Chúng thường được gọi là các xác nhận tương ứng nội xạ, có dạng:

truy vấn x1 : , xn : tn; inj sự kiện(e(M1, . . . , Mj))

t1, . . . inj sự kiện(e (N1, . . . ,Nk))

Một cách không chính thức, sự tương ứng này khẳng định rằng, với mỗi lần xuất hiện của sự kiện e(M1, . . . , Mj), có sự xuất hiện sớm hơn rõ rệt của sự kiện e (N1, . . ,Nk). Điều này khác với các xác nhận tương ứng trước đó ở chỗ không có sự kiện đơn lẻ e (N1, . . , Nk) nào có thể ảnh xạ tới hai sự kiện nữa e(M1, . . , Mj).

Trong công việc này, chúng tôi khai báo các sự kiện sau trong mô hình chính thức:

- sự kiện chấp nhậnUE(x), cho biết người dùng tin rằng cô ấy đã chấp nhận chạy giao thức với mạng gia đình và tham số được cung cấp;

- sự kiện chấp nhậnAUSF(x), cho biết mạng gia đình tin rằng nó đã chấp nhận chạy giao thức với máy khách và tham số được cung cấp; • sự kiện termUE(x), cho biết người dùng tin rằng cô ấy đã kết thúc quá trình chạy giao thức bằng cách sử dụng tham số đã cho; • sự kiện termAUSF(x), cho biết mạng gia đình tin rằng cô ấy đã chấm dứt quá trình chạy giao thức bằng cách sử dụng tham số đã cho; • sự kiện sendPrek(x), cho biết người dùng tin rằng cô ấy đã truyền một khóa trước tới mạng gia đình được cung cấp dưới dạng tham số; • sự kiện AcceptPrek(x), cho biết mạng gia đình tin rằng mạng gia đình đã chấp nhận khóa trước từ người dùng được cung cấp làm tham số.

Vì vậy, chúng ta xem xét các khẳng định tương ứng sau đây để chứng minh các thuộc tính xác thực.

- truy vấn x : chuỗi bit;inj sự kiện(termAUSF(Rue1x)) inj sự kiện(chấp nhậnUE(Rue1)).
- truy vấn x : bitstring;inj sự kiện(termUE(Rausfx)) inj sự kiện(chấp nhậnAUSF(Rausf)).
- truy vấn x : key;inj event(acceptPrek(prekeyx)) inj sự kiện(sendPrek(prekey)).

Theo trực quan, xác nhận đầu tiên có nghĩa là bất cứ khi nào mạng chấm dứt chạy giao thức, sẽ tồn tại một người dùng đã chấp nhận chạy với mạng. Lưu ý rằng chúng tôi sử dụng xác nhận tương ứng nội tại để ngăn chặn trường hợp một phiên máy khách được xác thực cho nhiều phiên máy chủ.

Điều này có thể xảy ra khi kẻ tấn công có thể phát lại tin nhắn của khách hàng. Ý nghĩa của hai khẳng định cuối cùng được xác định tương tự.

VI. KẾT QUẢ XÁC MINH VÀ THẢO LUẬN

Chúng tôi đã xác minh xem mô hình giao thức chính thức có đáp ứng các thuộc tính bảo mật được liệt kê trong Phần IV hay không. Chúng tôi lấy ProVerif 2.001 làm công cụ xác minh và các thử nghiệm được thực hiện trên PC được trang bị HĐH chuyên nghiệp Windows 10 và Intel Core i5-7300HQ với CPU 2,5 GHz và RAM 8,0 GB. Tổng thời gian để xác minh các thuộc tính là khoảng ba giây.

Kết quả được trình bày trong Bảng 6. Kết quả cho thấy tất cả các thuộc tính bí mật (tức là S1, S2 và S3) đều được thỏa mãn, trong khi các thuộc tính thỏa thuận (tức là A1 và A2) bị vi phạm. ProVerif có thể tạo ra các ví dụ mẫu cho các thuộc tính bị vi phạm. Để đơn giản cho việc trình bày, chúng tôi không báo cáo các kết quả đầu ra từ hệ thống của ProVerif trong bài viết này mà trình bày chi tiết về các ví dụ mẫu và các cách khắc phục có thể có. Lưu ý rằng trong tất cả các phân ví dụ, chúng tôi đánh dấu các tin nhắn không có thật từ kẻ tấn công bằng màu đỏ. Mô hình giao thức và kết quả được cung cấp công khai trong kho lưu trữ Github.2

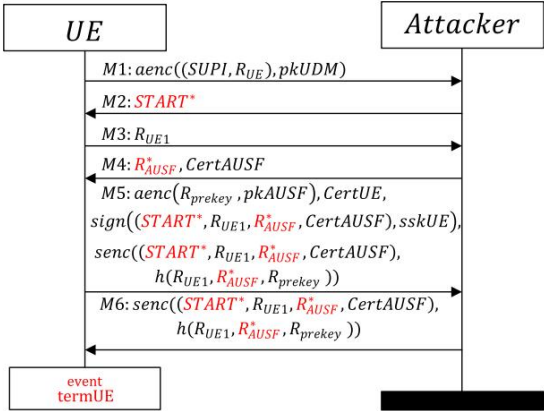
A. VI PHẠM TÀI SẢN A1

Thuộc tính này yêu cầu rằng khi những người tham gia chấm dứt việc thực hiện giao thức thành công, họ phải đồng ý về

1https://prosecco.gforge.inria.fr/personal/bblanche/proverif/
2https://github.com/bxk2008/5G-tls-protocol-analysis.git

BẢNG 6. Kết quả xác minh.

Security property	Result
A1. Both the home network (AUSF) and the subscriber (UE) should agree on the identity of each other after successful termination.	False
A2. Both the home network (AUSF) and the subscriber (UE) should agree on the pre-master key (Rprekey) after successful termination.	False
S1. The adversary must not be able to obtain the SUPI of an honest subscriber.	True
S2. The adversary must not be able to obtain the pre-master key (Rprekey) of an honest subscriber.	True
S3. The adversary must not be able to obtain the session key (Ksession) of an honest subscriber.	True



HÌNH 6. Phân ví dụ cho tính chất A1.

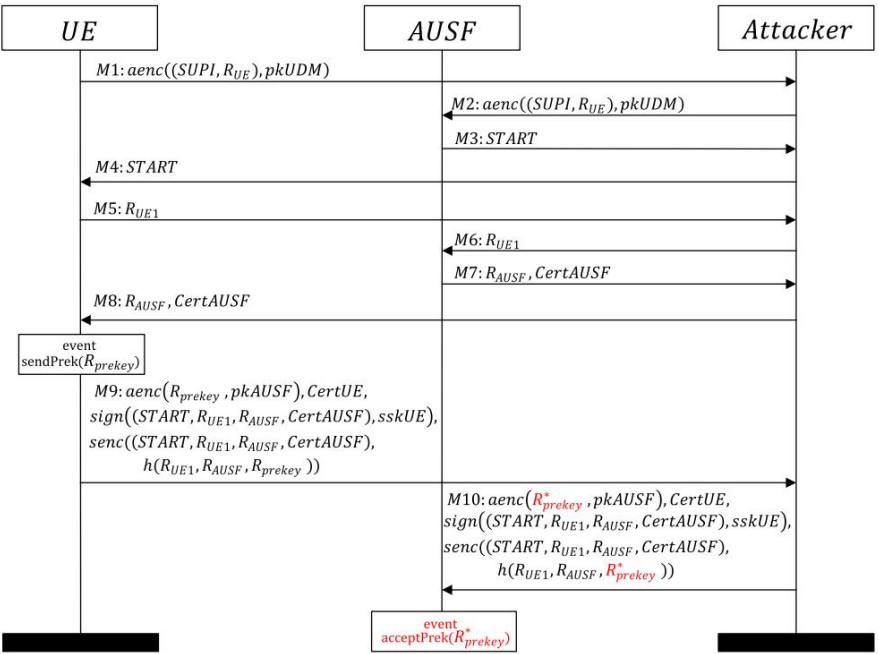
đanh tính của nhau để đạt được xác thực lẫn nhau. Tuy nhiên, phân tích của chúng tôi cho thấy rằng trong giao thức 5G EAP-TLS hiện tại, thuộc tính này bị vi phạm ở chỗ người dùng không thể xác thực danh tính của mạng gia đình. Bộ đếm mẫu được hiển thị trong Hình.6. Nó cho thấy kẻ tấn công có thể mạo danh mạng gia đình và thiết lập kết nối với người dùng. Tuy nhiên, người dùng không biết liệu mình được kết nối với mạng gia đình hợp pháp hay kẻ tấn công. Chúng tôi sẽ giải thích chi tiết về tính khả thi của phân ví dụ này ở phần sau.

Khi người dùng xuất mã hóa danh tính SUPI và số ngẫu nhiên RUE, kẻ tấn công sẽ trả lời bằng thông báo START , thông báo này có thể nhận được bằng cách lưu vào bộ nhớ đệm các thông tin liên lạc trước đó của mạng gia đình. Vì không bắt buộc phải kiểm tra tính hợp pháp của thông báo này nên người dùng sẽ tiếp tục thực hiện giao thức và xuất ra một số ngẫu nhiên mới RUE1 ở dạng bản rõ. Sau đó, kẻ tấn công sẽ giả mạo câu trả lời (R và chứng chỉ của mạng gia đình, được công khai.

AUSF ,CertAUSF) với số ngẫu nhiên R của riêng mình AUSF

Chúng tôi nhận xét rằng theo quan điểm của người dùng, liệu số ngẫu nhiên R là của kẻ tấn công hay AUSF chủ nhà

mạng không thể đoán trước được. Khi nhận được tin nhắn này từ kẻ tấn công, người dùng sẽ tính toán chữ ký và mã hóa các tin nhắn bắt tay theo cách tương tự như trước và chờ mã hóa các tin nhắn bắt tay từ phía mạng. Tuy nhiên, kẻ tấn công có thể chỉ cần chặn đầu ra của người dùng và trả lời bằng



HÌNH 7. Phần ví dụ cho tính chất A2.

mã hóa của người dùng. Người dùng không thể biết liệu phản hồi là từ kẻ tấn công hay mạng gia đình. Và khi kết thúc quá trình thực thi này, người dùng tin rằng mình đã thiết lập kết nối được xác thực với mạng gia đình.

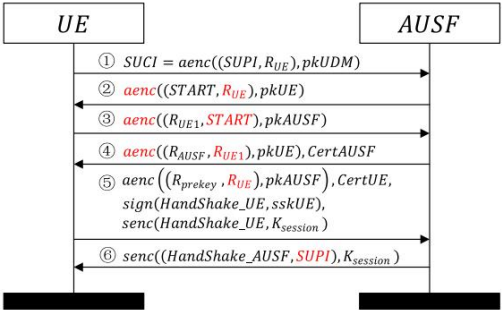
B. VI PHẠM TÀI SẢN A2

Thuộc tính này yêu cầu sau khi thực hiện thành công giao thức, cả người dùng và mạng gia đình phải đồng ý về khóa chính trước được sử dụng để tạo khóa phiên.

Ví dụ mẫu thể hiện sự vi phạm đặc tính này được thể hiện trong Hình 7. Đây là kiểu tấn công trung gian điển hình. Ban đầu, kẻ tấn công chỉ cần chặn và chuyển tiếp tin nhắn (tức là tin nhắn M1 và M5 từ người dùng và tin nhắn M3 và M7 từ mạng gia đình) giữa người dùng và mạng gia đình. Khi nhận được tin nhắn M9, kẻ tấn công sẽ thay thế mã hóa khóa chính Rprekey của người dùng bằng mã hóa khóa Rprekey của chính hắn và giả mạo tin nhắn trả lời M10 tới mạng gia đình. Việc giả mạo này có thể xảy ra do kẻ tấn công đang lưu vào bộ nhớ đệm tất cả các tin nhắn bắt tay giữa người dùng và mạng gia đình và mạng gia đình không thể biết liệu khóa chính Rprekey có phải là của kẻ tấn công hay không. Do đó, khi quá trình thực thi kết thúc, người dùng tin rằng mình đã thiết lập khóa chính Rprekey với mạng gia đình (tức là sự kiện sendPrek(prekey)), tuy nhiên, mạng gia đình tin rằng đó là khóa Rprekey được thiết lập (tức là sự kiện chấp nhậnPrek(prekey)).

C. BÀI HỌC rút ra VÀ cách khắc phục CÓ THỂ

Liên quan đến việc vi phạm tính chất A1, nguyên nhân chính là do các tin nhắn cần kiểm tra được truyền đi



HÌNH 8. Giao thức 5G EAP-TLS đã sửa đổi.

trong bản rõ. Kẻ tấn công có thể dễ dàng giả mạo các tin nhắn bắt tay bằng văn bản gốc giữa người dùng và mạng gia đình.

Đối với trường hợp thứ hai, nguyên nhân chính là do thiếu cơ chế phản hồi thách thức giữa người dùng và mạng gia đình. Cả người dùng và mạng gia đình đều không biết liệu các tin nhắn có được gửi đúng đối tượng hay không. Khi người dùng hoặc mạng gia đình nhận được một tin nhắn, anh ta có thể xác minh rằng tin nhắn đó thực sự đến từ vai trò hợp pháp mà nó giao tiếp tại thời điểm này. Ví dụ: khi người dùng gửi tin nhắn SUCI đến mạng gia đình, người dùng có thể kiểm tra xem tin nhắn BẮT ĐẦU sau có được nhận từ mạng gia đình hay không, mạng này đã nhận được tin nhắn SUCI trước đó hay chưa. Điều này đạt được bằng cách đưa số ngẫu nhiên RUE do người dùng tạo ra vào thư trả lời, vì chỉ mạng gia đình hợp pháp mới có thể giải mã tin nhắn đầu tiên để nhận được RUE. Để khắc phục, chúng tôi đề xuất thiết kế xác thực 5G EAP-TLS đã sửa đổi giữa UE và AUSF trong Hình 8. Vì mạng phục vụ không tham gia vào

Khi tính toán quy trình xác thực 5G EAP-TLS, chúng tôi đơn giản hóa việc trình bày thiết kế giao thức thành hai bên. Bản sửa lỗi dựa trên mật mã bất đối xứng và các phần tử mới được thêm vào được đánh dấu màu đỏ. Phân tích của chúng tôi cho thấy giao thức sửa đổi này đáp ứng tất cả các thuộc tính bảo mật.

Lưu ý: Trong [20], các tác giả phát hiện ra một cuộc tấn công khai thác một tình trạng chạy đua tiềm năng, trong đó việc cho phép nhầm lẫn các phiên của những người dùng khác nhau gây ra sự vi phạm cả đặc tính bí mật và xác thực. Tuy nhiên, công việc của họ dựa trên phiên bản cũ hơn của tài liệu (TS 33.501 V0.7.0). Chúng tôi không tìm thấy cuộc tấn công này trong phiên bản mới nhất.

VII. KẾT LUẬN VÀ CÔNG VIỆC TRONG TƯƠNG LAI

Trong công việc

này, chúng tôi điều tra các thuộc tính bảo mật của giao thức xác thực 5G EAP-TLS đang được 3GPP chuẩn hóa cho mạng di động thế hệ tiếp theo. Phân tích của chúng tôi dựa trên cách tiếp cận mang tính biểu tượng chính thức, trong đó chúng tôi lập mô hình giao thức và các thuộc tính bảo mật của nó trong phép tính pi được áp dụng và thực hiện phân tích bằng trình kiểm tra mô hình ProVerif. Phân tích của chúng tôi cho thấy một số sai sót trong thiết kế và các ví dụ phân biện được đưa ra để chỉ ra khả năng xảy ra của những sai sót này. Chúng ta cần chỉ ra rằng những sai sót này được tìm thấy ở cấp độ mô hình chính thức, tuy nhiên, chúng cũng sẽ tồn tại trong các hệ thống thực nếu giao thức được triển khai như hiện tại.

Chúng tôi cũng đề xuất một số chiến lược để sửa chữa các lỗ hổng này và chứng minh rằng giao thức sửa đổi đáp ứng tất cả các đặc tính bảo mật.

Về những nhược điểm của công việc hiện tại, chúng tôi muốn lưu ý rằng kết quả phân tích của ProVerif dựa trên mô hình giao thức ký hiệu, trong đó chúng tôi cho rằng mật mã là hoàn hảo và chúng tôi không tính đến sức mạnh tính toán của nguyên thủy. Mặc dù giả định này chỉ được quan tâm nghiên cứu về mặt lý thuyết nhưng nó quá mạnh để có thể thực tế. Do đó, nếu các nguyên tắc mã hóa cơ bản bị hỏng thì giao thức cũng sẽ bị lỗi, mặc dù nó đã được chứng minh là đúng và an toàn trên mô hình ký hiệu.

Trong tương lai, chúng tôi muốn tiến thêm một bước nữa để điều tra tính chính xác của việc triển khai giao thức liên quan đến thông số kỹ thuật. Ý tưởng là việc đảm bảo tính bảo mật của thiết kế giao thức là chưa đủ mà chúng ta còn cần đảm bảo rằng việc triển khai máy trạng thái giao thức là an toàn. Một kỹ thuật khả thi để đạt được mục tiêu này là kỹ thuật làm mờ trạng thái giao thức [32]. Chúng tôi cũng sẽ mở rộng công việc hiện tại sang mô hình mật mã tính toán, trong đó xác suất phá vỡ các nguyên tắc mã hóa được tính đến. Ngoài ra, chúng tôi muốn sử dụng một số kỹ thuật học máy như mạng nơ-ron [39] và thuật toán học trực tuyến [40] để tự động hóa quá trình xác thực giao thức.

NGƯỜI GIỚI THIỆU

[1] Kiến trúc và quy trình bảo mật cho hệ thống 5G, tài liệu 3GPP, TS 33.501, v15.4.0.2019, tháng 3 năm 2019

[2] Giao thức Bảo mật Lớp Vận chuyển (TLS) Phiên bản 1.2, tài liệu RFC5246, tháng 8 năm 2008.

[3] D. Basin, C. Cremers, K. Miyazaki, S. Radomirovic và D. Watanabe, '' Cải thiện tính bảo mật của các tiêu chuẩn giao thức mật mã, '' IEEE Secur. Quyền riêng tư, tập. 13, không. 3, trang 24-31, tháng 5 năm 2015.

[4] L. Hirschi, R. Sasse và J. Dreier, '' Các vấn đề bảo mật trong tiêu chuẩn 5G và cách giải quyết các phương pháp chính thức'' ERCIM News, Paris, Pháp, Tech. Dân biểu, tháng 4 năm 2019, tập. 2019, không. 117. [Trực tuyến]. Có sẵn: <https://ercim-news.ercim.eu/en117/special/security-issues-in-the-5g-standard-and-how-formal-methods-come-to-the-rescue>

[5] D. Basin, C. Cremers và C. Meadows, ''Các giao thức bảo mật kiểm tra mô hình'' trong Sổ tay kiểm tra mô hình, EM Clarke, TA Henzinger, H. Veith và R. Bloem, Eds. Châm, Thụy Sĩ: Springer, 2018, trang 727-762, doi: [10.1007/978-3-319-10575-8_22](https://doi.org/10.1007/978-3-319-10575-8_22).

[6] G. Lowe, '' Một cuộc tấn công vào giao thức xác thực khóa công khai Needham-Schroeder, '' Inf. Quá trình. Lett., tập. 56, không. 3, trang 131-133, tháng 11 năm 1995.

[7] J. Mitchell, M. Mitchell và U. Stern, '' Phân tích tự động các giao thức mật mã bằng Murϕ, '' trong Proc. Tiêu chuẩn IEEE An toàn. Quyền riêng tư, tháng 11 năm 2002, trang 141-151.

[8] DX Song, ''Athena: Trình kiểm tra tự động hiệu quả mới để phân tích giao thức bảo mật'' trong Proc. Máy tính IEEE thứ 12. Đã tìm thấy bảo mật. Workshop, tháng 1 năm 2003, trang 192-202.

[9] EM Clarke, S. Jha và W. Marrero, ''Xác minh các giao thức bảo mật với Brutus, '' ACM Trans. Phần mềm. Anh. Phương pháp, tập. 9, không. 4, trang 443-487, tháng 10 năm 2000.

[10] A. Armando và L. Compagna, '' SATMC: Trình kiểm tra mô hình dựa trên SAT cho các giao thức bảo mật, '' trong Logic trong trí tuệ nhân tạo, JJ Alferes và J. Leite, Eds. Berlin, Đức: Springer, 2004, trang 730-733.

[11] D. Basin, S. Mödersheim và L. Viganò, '' OFMC: Trình kiểm tra mô hình biểu tượng cho các giao thức bảo mật, '' Int. J. Inf. Bảo mật, tập. 4, không. 3, trang 181-208, tháng 6 năm 2005.

[12] V. Cortier, S. Delaune và P. Lafourcade, '' Một cuộc khảo sát về các đặc tính đại số được sử dụng trong các giao thức mật mã, '' J. Comput. Bảo mật, tập. 14, không. 1, trang 1-43, tháng 2 năm 2006.

[13] B. Blanchet, '' Lập mô hình hóa và xác minh các giao thức bảo mật bằng phép tính pi được áp dụng và ProVerif, '' Found. Xu hướng Bảo mật quyền riêng tư, tập. 1, không. 1-2, trang 1-135, 2016.

[14] C. Cremers, M. Horvat, J. Hoyland, S. Scott và T. van der Merwe, ''Một phân tích biểu tượng toàn diện về TLS 1.3, '' trong Proc. Hội nghị ACM SIGSAC. Máy tính. Cộng đồng. An toàn. (CCS), Dallas, TX, Hoa Kỳ, tháng 10/tháng 11. 2017, trang 1773-1788.

[15] B. Blanchet, ''Trình xác minh giao thức mật mã hiệu quả dựa trên các quy tắc prolog, '' trong Proc. Máy tính IEEE thứ 14. An toàn. Thành lập. Workshop, tháng 8 năm 2005, trang 82-96.

[16] M. Abadi, B. Blanchet và C. Fournet, '' Phép tính pi được áp dụng: Giá trị di động, tên mới và liên lạc an toàn, '' J. ACM, tập. 65, không. 1, trang 1:1-1:41, tháng 10 năm 2017.

[17] D. Dolev và A. Yao, ''Về tính bảo mật của các giao thức khóa công khai, '' IEEE Trans. Thông tin Lý thuyết, tập. CNTT-29, không. 2, trang 198-208, tháng 3 năm 1983.

[18] B. Blanchet, '' Sử dụng các mệnh đề Horn để phân tích các giao thức bảo mật, '' trong Mô hình chính thức và Kỹ thuật phân tích các giao thức bảo mật (Loạt bài về Mật mã và bảo mật thông tin), tập. 5, V. Cortier và S. Kremer, Eds. Amsterdam, Hà Lan: Nhà xuất bản IOS, 2011, trang 86-111.

[19] DA Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse và V. Stettler, ''Một phân tích chính thức về xác thực 5G'' trong Proc. Hội nghị ACM SIGSAC. Máy tính. Cộng đồng. An toàn. (CCS), Toronto, ON, Canada, tháng 10 năm 2018, trang 1383-1396.

[20] C. Cremers và M. Dehnel-Wild, '' Phân tích chính thức dựa trên thành phần của 5G-AKA: Các giả định về kênh và sự nhầm lẫn phiên, '' trong Proc. Ngày 26 hàng năm. Mạng. Phân phối. Hệ thống. An toàn. Triệt chủng. (NDSS), San Diego, CA, Hoa Kỳ, tháng 2 năm 2019, trang 1-15.

[21] S. Meier, B. Schmidt, C. Cremers và D. Basin, '' Trình chứng minh tamarin cho phân tích biểu tượng của các giao thức bảo mật, '' trong Xác minh được hỗ trợ bằng máy tính, N. Sharygina và H. Veith, Biên tập. Berlin, Đức: Springer, 2013, trang 696-701.

[22] D. Basin, C. Cremers, J. Dreier và R. Sasse, '' Phân tích tượng trưng các giao thức bảo mật bằng cách sử dụng tamarin, '' ACM SIGLOG, tập. 4, không. 4, trang 19-30, tháng 10 năm 2017.

[23] A. Braeken, M. Liyanage, P. Kumar và J. Murphy, ''Giao thức xác thực 5G mới để cải thiện khả năng chống lại các cuộc tấn công đang hoạt động và mạng phục vụ độc hại, '' IEEE Access, tập. 7, trang 64040-64052, 2019.

[24] A. Koutsos, ''Quyền riêng tư của giao thức xác thực 5G-AKA'' trong Proc. IEEE Eur. Triệt chủng. An toàn. Quyền riêng tư (EuroS&P), Stockholm, Thụy Điển, tháng 6 năm 2019, trang 464-479.

[25] G. Bana và H. Comon-Lundh, "Hướng tới sự đúng đắn về điều kiện: Kế tấn công mang tính biểu tượng hoàn chỉnh về mặt tính toán," trong Proc. Quốc tế thứ nhất Conf. Hoàng tử. An toàn. Trust (ETAPS), Tallinn, Estonia, tháng 3/tháng 4. 2012, trang 189-208.

[26] G. Bana và H. Comon-Lundh, "Kế tấn công mang tính biểu tượng hoàn chỉnh về mặt tính toán đối với các thuộc tính tương đương" trong Proc. Hội nghị ACM SIGSAC. Máy tính. Cộng đồng. Secur., Scottsdale, AZ, Hoa Kỳ, tháng 11 năm 2014, trang 609-620.

[27] R. Borgeonkar, L. Hirschi, S. Park và A. Shaik, "Mối đe dọa bảo mật mới trên 3G, 4G và các giao thức 5G AKA sắp tới," Công nghệ nâng cao quyền riêng tư., tập. 2019, không. 3, trang 108-127, 2019.

[28] J. Zhang, Q. Wang, L. Yang, và TF và "Xác minh chính thức giao thức xác thực 5G-EAP-TLS" trong Proc. IEEE quốc tế lần thứ 4 Conf. Khoa học dữ liệu. Không gian mạng (DSC), Hàng Châu, Trung Quốc, tháng 6 năm 2019, trang 503-509.

[29] B. Blanchet, "Các định lý thành phần cho mật mã và ứng dụng cho TLS 1.3," trong Proc. Máy tính IEEE lần thứ 31. An toàn. Thành lập. Triệu chứng. (CSF), Oxford, Vương quốc Anh, tháng 7 năm 2018, trang 16-30.

[30] B. Blanchet, "Một phương pháp cơ giới hóa hợp lý về mặt tính toán cho các giao thức bảo mật," IEEE Trans. Máy tính an toàn đáng tin cậy, tập. 5, không. 4, trang 193-207, tháng 10 năm 2008.

[31] K. Bhargavan, B. Blanchet và N. Kobeissi, "Các mô hình đã được xác minh và triển khai tham chiếu cho ứng cử viên tiêu chuẩn TLS 1.3" trong Proc. Tiêu chuẩn IEEE An toàn. Quyền riêng tư (SP) 2017, San Jose, CA, Hoa Kỳ, tháng 5 năm 2017, trang 483-502.

[32] J. de Ruiter và E. Poll, "Làm mờ trạng thái giao thức của việc triển khai TLS," trong Proc. USENIX Secur lần thứ 24. Symp., USENIX Secur., tập. 15, Washington, DC, Hoa Kỳ, tháng 8 năm 2015, trang 193-206.

[33] N. Kobeissi, K. Bhargavan và B. Blanchet, "Xác minh tự động cho các giao thức nhắn tin an toàn và cách triển khai chúng: Một cách tiếp cận mang tính biểu tượng và tính toán," trong Proc. IEEE Eur. Triệu chứng. An toàn. Pri-vacy (EuroS&P), Paris, Pháp, tháng 4 năm 2017, trang 435-450.

[34] RP Jover và V. Marojovic, "Phân tích khai thác giao thức và bảo mật của các thông số kỹ thuật 5G," IEEE Access, tập. 7, trang 24956-24963, 2019.

[35] R. Khan, P. Kumar, DNK Jayakody và M. Liyanage, "Khảo sát về bảo mật và quyền riêng tư của công nghệ 5G: Các giải pháp tiềm năng, những tiến bộ gần đây và hướng đi trong tương lai," IEEE Commun. Khảo sát Tuts., sẽ được xuất bản.

[36] CJF Cremers, "Công cụ Scyther: Xác minh, làm sai lệch và phân tích các giao thức bảo mật," trong Xác minh có sự hỗ trợ của máy tính, A. Gupta và S. Malik, Eds. Berlin, Đức: Springer, 2008, trang 414-418.

[37] H. Comon-Lundh, S. Delaune và JK Millen, "Các kỹ thuật giải quyết ràng buộc và làm phong phú mô hình bằng các lý thuyết phương trình," trong Mô hình chính thức và Kỹ thuật phân tích các giao thức bảo mật (Loạt bài về Mật mã và bảo mật thông tin), tập. 5, V. Cortier và S. Kremer, Eds. Amsterdam, Hà Lan: Nhà xuất bản IOS, 2011, trang 35-61.

[38] Bảo mật 3G; Kiến trúc bảo mật, tài liệu TS 33.102, v11.5.1, 3GPP, Tháng 6 năm 2013.

[39] W. Cao, X. Wang, Z. Ming và J. Gao, "Đánh giá về mạng lưới thần kinh với các trọng số ngẫu nhiên," Neurocomputing, tập. 275, trang 278-287, tháng 1 năm 2018, doi: 10.1016/j.neucom.2017.08.040.

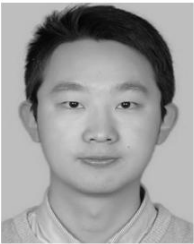
[40] W. Cao, J. Gao, Z. Ming, S. Cai và Z. Shan, "Máy học cực đoan tuần tự trực tuyến dựa trên mô cho các vấn đề phân loại," Soft. Máy tính, tập. 22, không. 11, trang 3487-3494, tháng 6 năm 2018, doi: 10.1007/s00500-018-3021-4.



JINGJING ZHANG nhận bằng Cử nhân về bảo mật thông tin của Đại học Khoa học và Công nghệ Thông tin, Bắc Kinh, Trung Quốc và bằng Thạc sĩ về kỹ thuật điện tử và truyền thông của Đại học Buu chính Viễn thông Bắc Kinh, Bắc Kinh. Anh ấy hiện đang theo đuổi bằng tiến sĩ. tốt nghiệp tại Trường Cao đẳng Kỹ thuật Chỉ huy và Điều khiển, Đại học Kỹ thuật Quân đội PLA. Anh là sinh viên trao đổi tại Phòng thí nghiệm Khoa học và Công nghệ Trọng điểm Quốc gia về An ninh Hệ thống Thông tin, Viện Kỹ thuật Hệ thống, Bắc Kinh, kể từ năm 2018. Chủ đề nghiên cứu của anh chủ yếu là phân tích chính thức các giao thức bảo mật từ góc độ mô hình thiết kế và triển khai.



LIN YANG nhận bằng BS và MS về tự động hóa và bằng Tiến sĩ. bằng về hệ thống thông tin liên lạc và điện tử của Đại học Công nghệ Quốc phòng Quốc gia, Trường Sa, Hồ Nam, lần lượt vào năm 1995 và 1998. Ông hiện là Nghiên cứu viên của Phòng thí nghiệm Khoa học và Công nghệ Trọng điểm Quốc gia về An ninh Hệ thống Thông tin, Viện Kỹ thuật Hệ thống, Bắc Kinh. Mối quan tâm nghiên cứu của ông bao gồm bảo mật máy tính, bảo mật hệ thống thông tin, bảo mật mạng, điện toán đáng tin cậy, phòng thủ mục tiêu di động, phân tích quy trình bảo mật và bảo mật dữ liệu lớn.



WEIPENG CAO nhận bằng Tiến sĩ. bằng khoa học máy tính của Đại học Thâm Quyển, vào tháng 6 năm 2019. Kể từ năm 2017, anh là Học giả thỉnh giảng của Trường Kỹ thuật và Khoa học Máy tính, Đại học Thái Bình Dương, Stockton, CA, Hoa Kỳ. Ông hiện là Phó nhà nghiên cứu tại Trường Cao đẳng Khoa học Máy tính và Kỹ thuật Phần mềm, Đại học Thâm Quyển.

Mối quan tâm nghiên cứu của ông bao gồm học máy và học sâu.



QIANG WANG nhận bằng cử nhân và thạc sĩ của Đại học Công nghệ Quốc phòng Quốc gia năm 2010 và 2012, và bằng Tiến sĩ. bằng cấp của EPFL, Thụy Sĩ, năm 2017, nơi ông là người chủ chốt trong việc phát triển khung thiết kế hệ thống nhưng dựa trên thành phần BIP. Mối quan tâm nghiên cứu hiện tại của ông tập trung vào các kỹ thuật và công cụ xác minh chính thức cho các hệ thống quan trọng về an toàn và bảo mật.