



NỘI DUNG



1. Câu chuyện Mã nhảy Rolling-Code
2. Vấn đề nhức nhối
3. Giải pháp của chúng tôi



www.onyx.vn

Giới thiệu giải pháp công nghệ iKnock™ và CyLock

The Zero-Knowledge Protocol for Authentication
Một phát minh, giải pháp mới độc đáo để chế tạo Khóa **chống hack**.

+ CÂU CHUYỆN MÃ NHẢY ROLLING-CODE

1

- Đã từ lâu, việc sử dụng một chìa khóa điều khiển từ xa cửa cuốn cho các nhà mặt phố, các nhà kho và gara là việc phổ biến trong xã hội hiện đại.

Mã cố định - Fixed code



Mã nhảy - Rolling code

- 1960s
 - Biến thể: Learning code
 - Khóa, điều khiển từ xa, đồ chơi
 - Bảo mật yếu: bruteforce, replay attack
- 1990s, microchip,
 - Khóa, điều khiển từ xa,
 - Mã biến đổi, vô hiệu: bruteforce, replay attack
 - Thành trì bảo mật: 1 pháo đài bảo vệ suốt 30 năm
- Tuy nhiên, tính bảo mật của các loại khóa lại một lần nữa được nêu lên.

DefCon23, 2015, tại Nevada, US, Samy Kamkar đã chỉ ra lỗ hổng bảo mật nghiêm trọng của mã nhảy Rolling-Code. Mở khóa ô-tô với 1 thiết bị có giá thành khoảng \$30 (700k VNĐ)

Samy Kamkar

RollJam attack

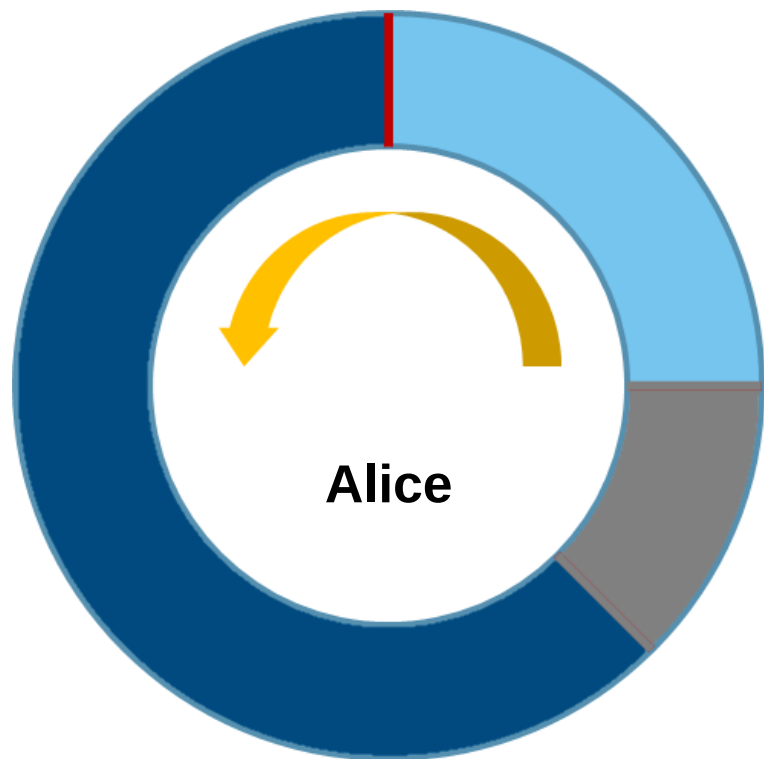


RollJam attack

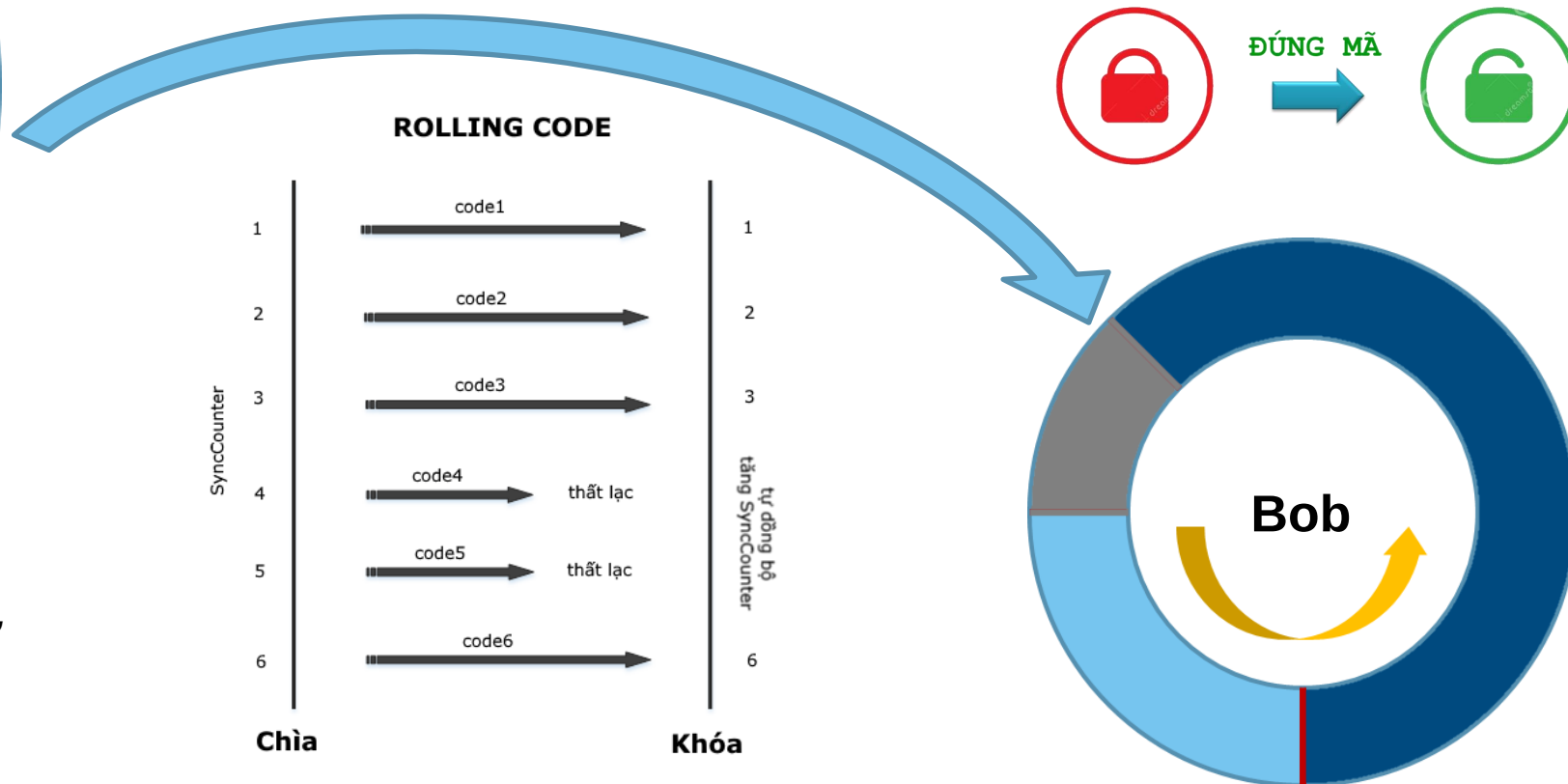
Microchip HCS301

1

- Nguyên lý: Đúng mã thì mở
- Code space: 64 bits
- SyncCounter: ≥ 256 (thường từ 8 - 16bits)

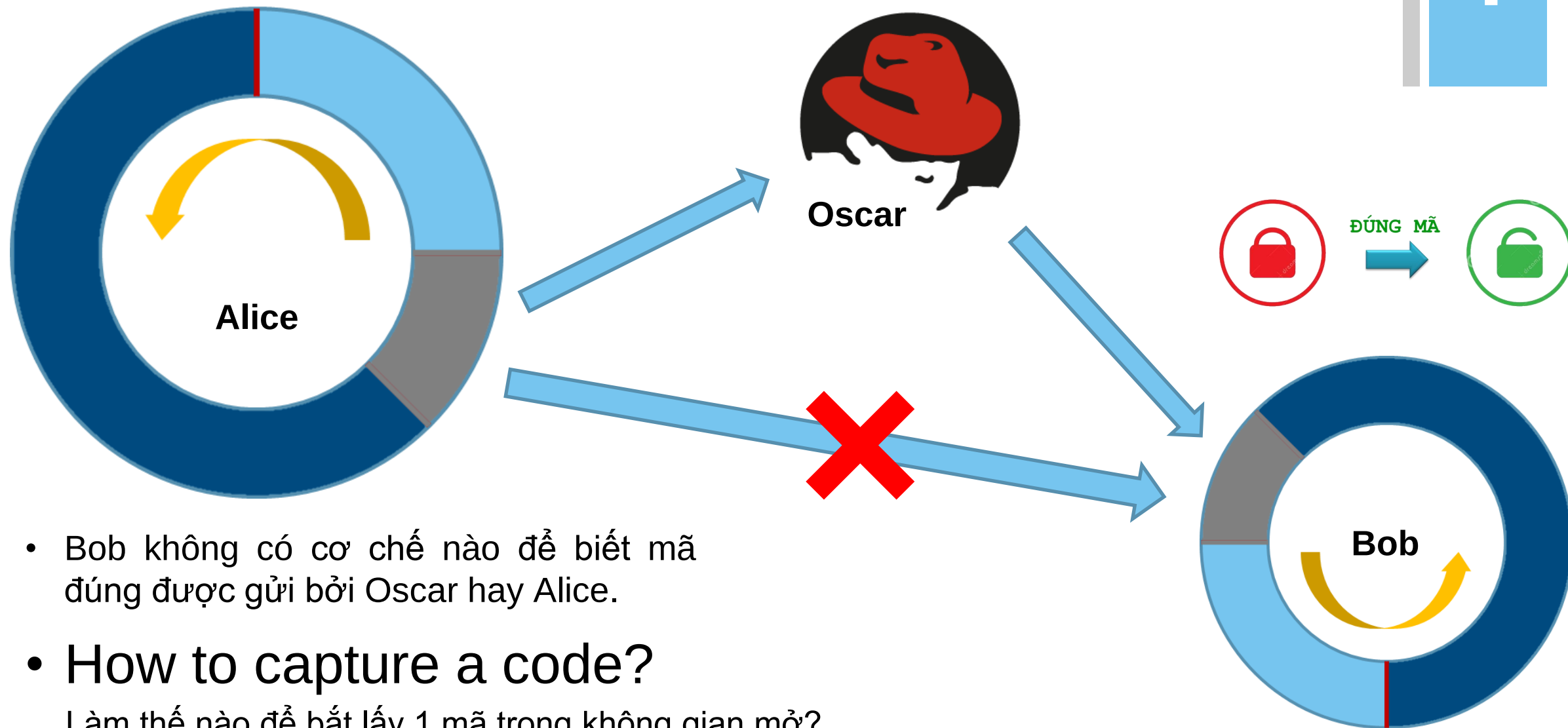


(*) SyncCounter: bộ đếm đồng bộ, sử dụng khi mã không đến đích



+

RollJam attack



- Bob không có cơ chế nào để biết mã đúng được gửi bởi Oscar hay Alice.
- **How to capture a code?**
Làm thế nào để bắt lấy 1 mã trong không gian mở?

+ GÓC NHÌN CỦA OSCAR

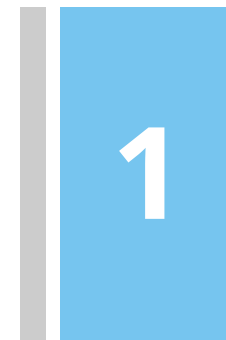
Điểm yếu của hệ thống bảo mật

- RSA, AES, SHA ? Có thể được coi là không thể phá (dù đã có thuật toán lượng tử SHOR phá mã RSA)
- Protocol: giả định rằng mọi tiến trình con trong 1 lượt giao thức chuẩn luôn có thể bị gián đoạn

Triển khai giao thức trong thực tiễn

- Giao thức tầng ứng dụng (phần mềm)
 - Alan Turing phá mã Enigma
 - Crypto coin bị hack
- Giao thức tầng giao vận (firmware)
 - Đích đến quan trọng hơn nơi gửi: DDoS
- Môi trường vật lý (hardware)
 - Can nhiễu, gián đoạn
 - Capture: can nhiễu khiến Bob không hiểu Alice

Điểm yếu



RollJam Attack:

Can nhiễu khiến Bob không hiểu Alice nhưng oscar vẫn lấy được thông tin từ Alice

- Lĩnh vực bảo mật phần cứng
- Lĩnh vực bảo mật phần mềm

+ NHỮC NHỒI

2



WOMEN OF THE YEAR

Meet the honorees ★

PLAY!

The Crossword

MILLENNIAL HOMEOWNERS

Where they buy

For You U.S. Sports Entertainment Life Money Tech Travel Opinion

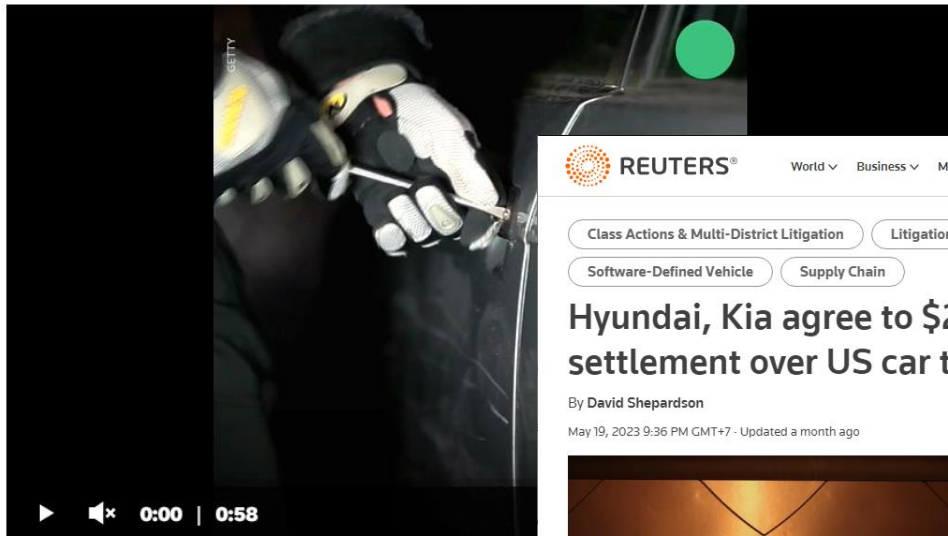
'Crisis of thefts': 23 attorneys general demand Kia, Hyundai take action



Grace Hauck

USA TODAY

Published 4:59 p.m. ET March 20, 2023



Auto theft has spiked during the pandemic, here's how it's striking



World Business Markets Sustainability Legal Breakingviews

Class Actions & Multi-District Litigation Litigation ADAS, AV & Safety

Software-Defined Vehicle Supply Chain

Hyundai, Kia agree to \$200 million settlement over US car thefts

By David Shepardson

May 19, 2023 9:36 PM GMT+7 - Updated a month ago



news.koreadaily.com/2023/03/20/society/generalsociety/20230320202440319.html

local home

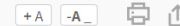
중앙일보
THE KOREA DAILY

full article society economy life Entertainment/Sports H

education business book

[Los Angeles]

input2023.03.21 10:24 correction2023.03.21 10:24



Attorney Generals of 23 States Pressure Hyundai Motor and Kia... Call for strengthening anti-theft measures

"Failed to prevent vehicle theft"

On the 20th, the attorney generals of 20 states urged Hyundai Motors and Kia to take more active anti-theft measures.

Attorneys generals from 23 states, including Wisconsin and Illinois, sent official letters to Hyundai and Kia on the same day, accusing the two companies of failing to take appropriate action to address the growing number of vehicle thefts, speeding up the implementation of related software upgrades. demanded mine It also recommends that vehicle owners without software support provide alternative protection measures.



美 20여개 주, 현대차·기아에 차량 도난 방지 조치 강화 촉구 / 연합뉴스TV (YonhapnewsTV)

2023, US,
Kia và Hyundai
phải đền bù cho người dùng
200 triệu USD

+ NHỨC NHỒI



Gia tăng hoạt động

CÔNG NGHỆ

Kia và Hyundai bị kiện vì trào lưu bẻ khóa xe trên TikTok

Anh Tuấn • Thứ ba, 27/9/2022 07:46 (GMT+7)

Một đơn kiện tập thể cáo buộc Kia và Hyundai cố tình không trang bị cảnh báo chống trộm, khiến trào lưu hướng dẫn bẻ khóa xe trên TikTok trở nên dễ dàng.



Chủ xe Kia và Hyundai kiện hãng vì bảo mật quá kém. Ảnh: AP.

Xem bài trên báo [ZingNews](#)

Một nhóm các 'nhà nghiên cứu' đã hack thành công hàng loạt xe mới trên thị trường, chiếm quyền điều khiển với nhiều cấp độ nghiêm trọng.



Kết nối Internet xuất hiện ngày một phổ biến trên ô tô cũng khiến chúng dễ bị chiếm quyền điều khiển từ xa hơn - Ảnh minh họa: CNET

Xem bài trên báo [Tuổi trẻ](#)



Kevin2600 thông báo về lỗ hổng bảo mật Rolling-Pwn trên Twitter cá nhân.

Kevin2600 công bố mã nguồn máy hack rolling-code xe ô tô Honda, xem bài trên báo [VietnamNet](#)

2

+ BÀI TOÁN: KHÓA ÔTÔ MỚI CHỐNG HACK

2

Đánh bại Oscar?

2018, US, **748.841** vụ việc

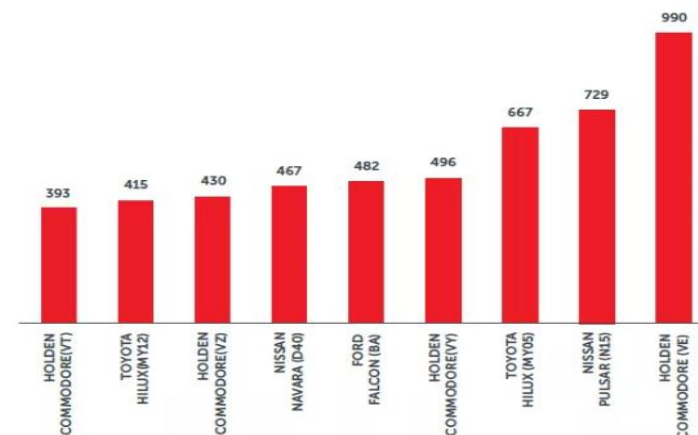
Top 10 Most Frequently Stolen Vehicles, 2018

All model years (1)			2018 model year vehicles only		
Rank	Model	Thefts	Rank	Model	Thefts
1	Honda Civic	38,426	1	GMC Pickup (Full size)	1,170
2	Honda Accord	36,815	2	Ford Pickup (Full size)	1,017
3	Ford Pickup (Full size)	36,355	3	Toyota Camry	976
4	Chevrolet Pickup (Full size)	31,566	4	Nissan Altima	912
5	Toyota Camry	16,906	5	Chevrolet Pickup (Full size)	790
6	Nissan Altima	13,284	6	Hyundai Elantra	775
7	Toyota Corolla	12,388	7	Ford Transit	723
8	GMC Pickup (Full size)	11,708	8	Dodge Charger	719
9	Dodge Pickup (Full size)	11,226	9	Toyota Corolla	699
10	Jeep Cherokee/Grand Cherokee	9,818	10	Chevrolet Malibu	698

2019, Australia,
58.285 vụ việc [2]

Tăng 9% so với 2018.
12% vụ việc do bằng cách nào đó sao chép được chìa khóa (hacker)

Most stolen cars in Australia in 2018



Oscar

2021, **Việt Nam**, tiêu thụ hàng trăm ô tô không rõ xuất xứ - [đây](#)

[1] <https://www.iii.org/fact-statistic/facts-statistics-auto-theft>

[2] <https://www.budgetdirect.com.au/car-insurance/research/car-theft-statistics.html>

Gia tăng hoạt động

Video này xác minh lỗi hỏng bảo mật khóa ô tô: <https://youtu.be/SW2nif3QCkA>

+ BÀI TOÁN: KHÓA CỬA CUỐN MỚI CHỐNG HACK

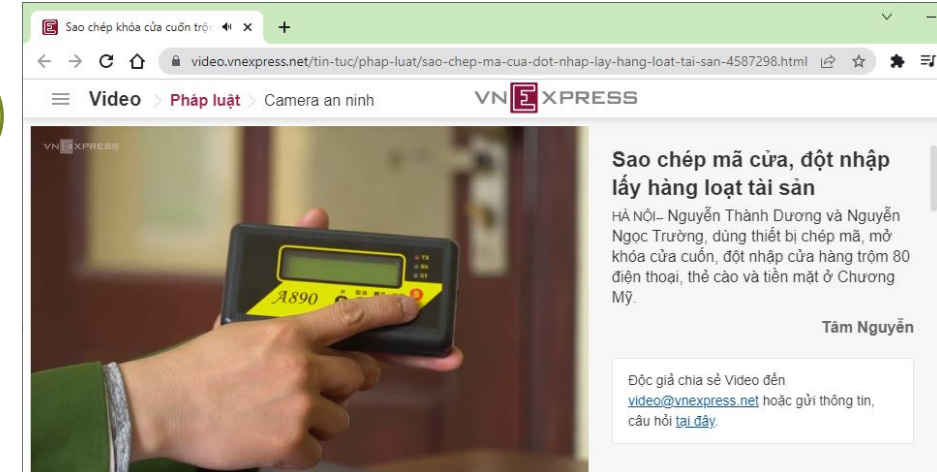


Các cụ nhà, cửa hàng nào lắp cửa cuốn điện thì nên lắp thêm chống trộm và camera an ninh thật tốt. Nhà em trộm vào lúc 4h21 phút sáng, nó bấm cửa cuốn như có chìa, rồi vào quăm tài sản đi một cách dễ dàng



- o Tại Việt Nam, 100% khóa cửa cuốn có lỗi hồng bảo mật Rolling-code hoặc Fix-code
- o 100% xuất xứ: Trung Quốc, Đài Loan; Không có nhà sản xuất khóa trong nước
- o 100% cơ sở sản xuất cửa cuốn nhập khẩu khóa và căng thương hiệu, họ không sở hữu công nghệ và bản thân họ cũng không hiểu được những rủi ro của công nghệ mình đang sử dụng.

Người dân chưa có công cụ nào để tự bảo vệ gia đình mình



[Xem tin gốc ngày 29/3 VTV1 đưa tin]



1 tiệm khóa nhỏ ven đường
Đánh chìa từ cửa cuốn để xe máy

Video sau đây xác minh lỗi hồng bảo mật khóa cửa từ xa cửa cuốn: https://youtu.be/st_xSEitji0

ZKP - Zero Knowledge Protocol

Protocol 18.2: Schnorr's Identification Protocol

Schnorr

COMMON INPUT:

p, q : two primes satisfying $q|p-1$;
(* typical size setting: $|p| = 1024$, $|q| = 160$ *)
 g : $\text{ord}_p(g) = q$;
 y : $y = g^{-a} \pmod{p}$;
(* tuple (p, q, g, y) is Alice's public-key material, certified by an CA *)

PRIVATE INPUT of Alice: $a < q$;

OUTPUT TO Bob: Alice knows some $a \in \mathbb{Z}_q$ such that $y \equiv g^{-a} \pmod{p}$.

Repeating the following steps $\log_2 \log_2 p$ times:

1. Alice picks $k \in_U \mathbb{Z}_q$ and computes $\text{Commit} \leftarrow g^k \pmod{p}$;
she sends **Commit** to Bob;
2. Bob picks **Challenge** $\in_U \{0, 1\}^{\log_2 \log_2 p}$;
he sends **Challenge** to Alice;
3. Alice computes $\text{Response} \leftarrow k + a \cdot \text{Challenge} \pmod{q}$;
She sends **Response** to Bob;
4. Bob checks $\text{Commit} \equiv g^{\text{Response}} y^{\text{Challenge}} \pmod{p}$;
he rejects and aborts if the checking shows error;

Bob accepts.

(* Bob's computation of $g^{\text{Response}} y^{\text{Challenge}} \pmod{p}$ should apply Alg 15.2 and so the cost is similar to computing single modulo exponentiation *)

⇒ Schnorr's Identification Protocol, trang 630,
sách "Modern cryptography - theory and practice, Wenbo Mao" (2003)
Và các sách kinh điển của ngành trong vòng 20 năm trở lại đây đều nhắc đến.

Diễn giải bằng lời thuật toán Schnorr:

Alice

Bob

0. Alice và Bob cùng chia sẻ 1 chìa khóa bí mật (p, q, g, y, a) từ trước

Lặp lại các bước sau đây **m** lần, $m = 4$ lần với p dài 1024 bit.

1. Alice nhặt 1 hòn đá ngẫu nhiên **Commit(k)** và ném cho Bob

2. Bob lựa chọn ngẫu nhiên cách ứng xử **Challenge** (gắt hoặc không)

3. Alice đáp trả **Response** là 1 hàm của Challenge (mà Bob cũng biết cách tính)

4. Bob kiểm tra **Response**

5. Sau m lần Alice đều trả lời đúng, Bob chấp nhận kết nối.

+ GIẢI PHÁP ĐANG CÓ

CHALLENGE AND RESPONSE

Kinh điển
tạo ra lỗ hổng
Tiêu chuẩn

A

386

Cryptography: Theory and Practice

Protocol 10.2: (SECURE) CHALLENGE-AND-RESPONSE

1. Bob chooses a random challenge, r , which he sends to Alice.
2. Alice computes
$$y = \text{MAC}_K(\text{ID}(\text{Alice}) \parallel r)$$
and sends y to Bob.
3. Bob computes
$$y' = \text{MAC}_K(\text{ID}(\text{Alice}) \parallel r).$$
If $y' = y$, then Bob "accepts"; otherwise, Bob "rejects."

Thuật toán: Challenge and Response

Kinh điển không kém Schnorr, Ví dụ:

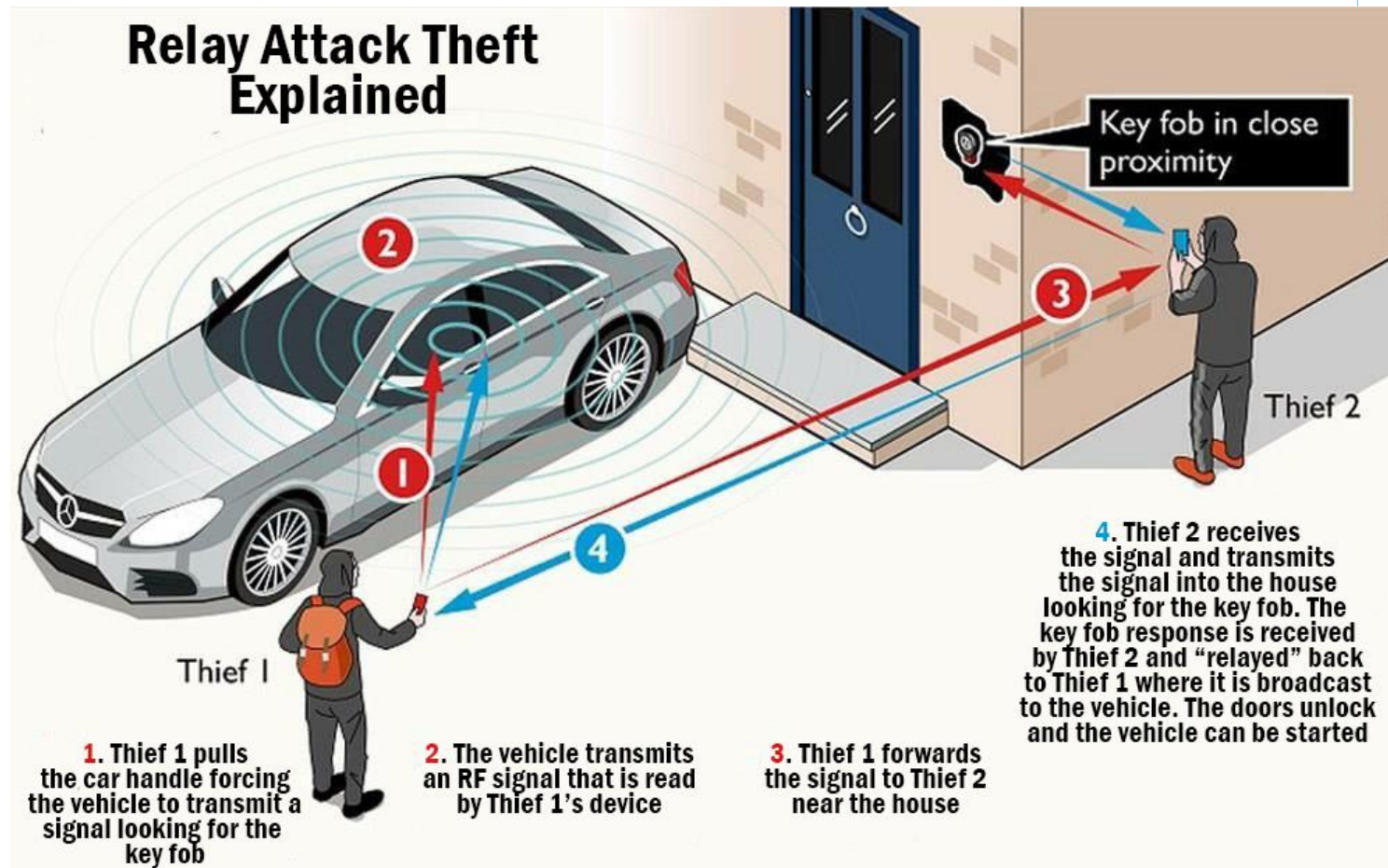
sách Cryptography: Theory and Practice, trang 386

Bob khởi xưởng Giao thức

(Khác với Schnorr, Alice khởi xưởng giao thức)

Relay Attack trầm trọng hơn

Relay Attack Theft Explained



1. Bob khởi xưởng giao thức

2-3-4. Oscar đứng giữa khuếch đại tín hiệu



GIẢI PHÁP



Sáng chế quốc tế 11 điểm bảo hộ,
WIPO: WO2021174264



3

Nguyên lý mới - Giao thức mới

Nguyên lý cũ: Mã hóa



Đúng mã thì mở,
Không quan tâm ai dùng mã

Nguyên lý mới: **Xác thực**



Đúng mã và
đúng chìa thì mở

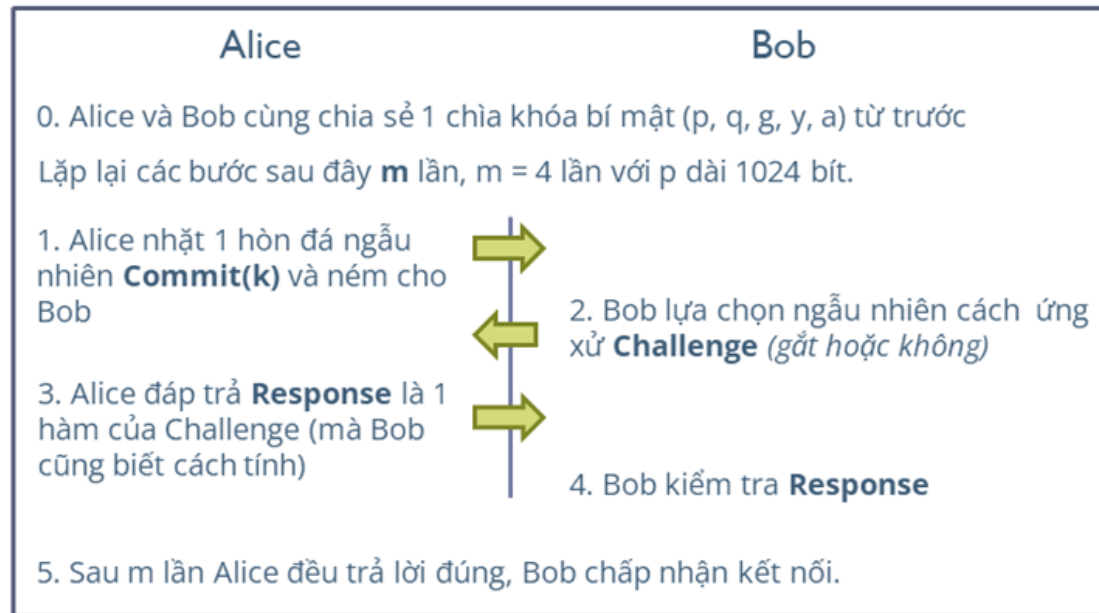
Với Token 64 bits, CypherKey 256 bits; không thể bị hách / crách với công nghệ điện toán hiện tại

+ iKnock: Giao thức Xác thực mới an toàn

ZKP – Schnorr vs iKnock

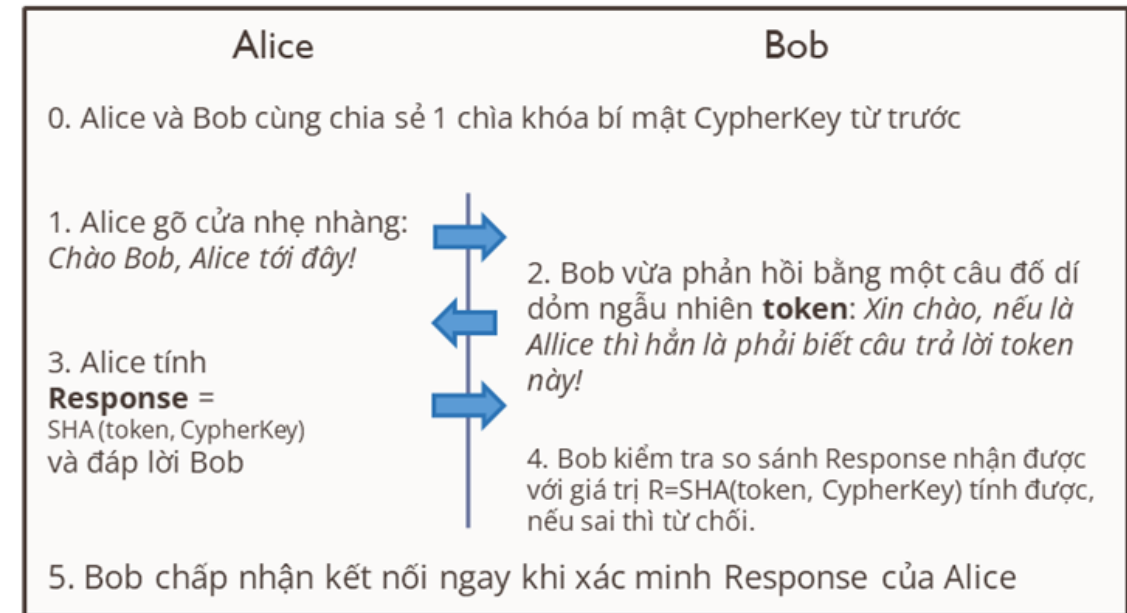
3

Diễn giải bằng lời thuật toán Schnorr: (U.S. Patent 4,995,082)



- Alice phải tính toán trên số nguyên tố lớn cho (Commit và Response) m lần.
- Alice truyền đi $2*m$ gói tin.
- Cả Alice và Bob đều cần bộ sinh ngẫu nhiên.

Diễn giải bằng lời thuật toán iKnock: (WIPO Patent WO2021174264)



- Alice chỉ tính Response 1 lần theo hàm SHA.
- Alice truyền đi 2 gói tin.
- Bob cần bộ sinh ngẫu nhiên, Alice thì không cần.

- Do cấu trúc của các hàm sử dụng, hàm Schnorr cần truyền nhiều lượt để tránh lộ khóa bí mật, hàm SHA thì không cần.
- Việc Alice truyền tin nhiều lượt ($2*m$ gói tin) yêu cầu đường truyền của Alice phải rất tốt và nhiều thời gian hơn để truyền tin.
- Việc Alice tính toán Response trên số nguyên tố lớn cần nhiều năng lực tính toán khiến cho thiết bị dùng Schnorr trở nên đắt đỏ.
- Việc Alice cần nhiều tài nguyên khiến triển khai Schnorr trên các phần cứng hạn chế tài nguyên như KeyFob của Khóa trở nên khó khăn.
- Và một lý do quan trọng là: iKnock đã có sản phẩm CyLock – khóa mật mã an toàn (với 100k lần bấm nút, xem video: <https://bit.ly/Pushed100k>).



2021



UNHACKABLE REMOTE LOCK



Sáng chế 02 điểm bảo hộ độc lập
Sáng chế thế giới WIPO: WO2021174264
Việt Nam: 1-2020-01076 | Taiwan: X211669TWI



CyLock: khóa mật mã an toàn

Chìa khóa:

- Chống thấm nước IP68
- Không phải thay pin
- Bền bỉ: 100k lần bấm nút

Video: Stress test CyLock, 100k lần bấm nút ~28 năm sử dụng: [Xem video youtube: Pushed100k](#)

Ổ khóa:

- Mật mã bất bại: AES, SHA
- Giao thức an toàn: chống bắt lầy mã, không thể sao chép chìa
- Tiết kiệm: khi mất chìa khóa không phải thay ổ khóa, chỉ cần hủy chìa đã mất và ghép chìa mới



tin cậy, bền bỉ, không thể bị hách

Ứng dụng

Bảo vệ tài sản



4

Ô tô



Xe máy



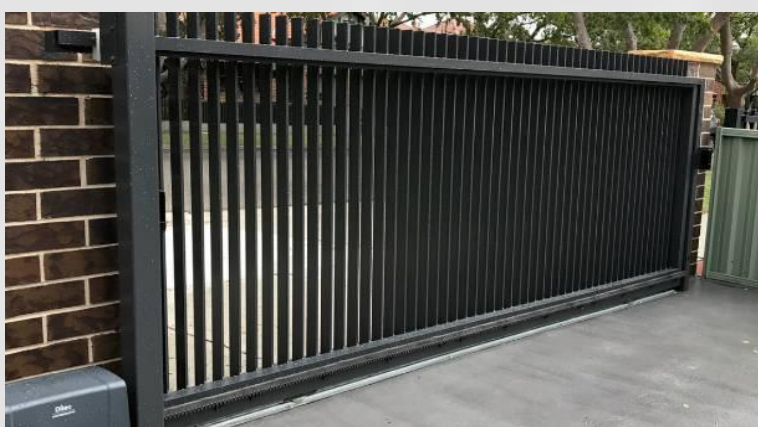
Xe điện



Cửa cuốn



Cửa trượt



Giếng trời



Thông tin: Việt Nam, hơn 4tr ô tô, 40tr xe máy thị trường tăng trưởng 10%

Toàn cầu: gần 100 triệu xe ô tô được sản xuất hàng năm

Việt Nam, khoảng 2.5 triệu cửa cuốn, toàn cầu & US rất lớn

1. WO2022043756 - SMART ELECTRONIC FENCE SYSTEM AND INTRUSION DETECTION METHOD USING THE SAME

PCT Biblio. Data Full Text Drawings

Publication Number
WO/2022/043756

Publication Date
03.03.2022

International Application No.
PCT/VN2021/00098

International Filing Date
20.09.2021

IPC
G08B 13/163 2006.1 G08B 29/04 2006.1

CPC
G08B 13/163 G08B 29/04 G08B 29/14

Applicants
VIETNAM ONYX JOINT STOCK COMPANY (VN)
No. 112, Vương Thừa Vũ Street, Phường
Trung Ward, Thanh Xuân District Hanoi, 100000, VN

Inventors
NGUYEN, Khuong Tuan
TRAN, Tien Trung

Agents
VIA A INTELLECTUAL PROPERTY CO., LTD.
No. 36, Alley 284 Kim Ma Street, Kim Ma
Ward, Ba Dinh District Hanoi, 100000, VN

Priority Data
1-2020-0400 26.08.2020 VN

Publication Language
English [en]

Filing Language
English [en]

Designated States
View all

Latest bibliographic data on file with the



Số: **WO2022043756**
Công bố ngày: **03/03/2022**



Số: **WO2022170370**
Công bố ngày: **11/08/2022**



Số: **WO2022094635**
Công bố ngày: **5/5/2022**



Số: **WO2021174264**
Công bố ngày: **2/9/2021**

1. WO2021174264 - METHOD FOR REMOTELY ACTIVATING A REMOTE LOCK SYSTEM USING CRYPTOGRAPHY AND THE REMOTE LOCK SYSTEM FOR IMPLEMENTING THE METHOD

PCT Biblio. Data Description Claims Drawings ISR/WISA/A17(2)[a] National Phase Notices Documents

Feedback Search Browse Tools Settings

Submit observation PermaLink Machine translation

Publication Number
WO/2021/174264

Publication Date
02.09.2021

International Application No.
PCT/VN2021/000004

International Filing Date
24.02.2021

IPC
G07C 9/00 2006.1 G06F 21/60 2013.1
H04L 9/32 2006.1 H04L 9/06 2006.1

Title
[EN] METHOD FOR REMOTELY ACTIVATING A REMOTE LOCK SYSTEM USING CRYPTOGRAPHY AND THE REMOTE LOCK SYSTEM FOR IMPLEMENTING THE METHOD
[FR] PROCÉDÉ D'ACTIVATION À DISTANCE D'UN SYSTÈME DE VERROUILLAGE À DISTANCE PAR CRYPTOGRAPHIE ET SYSTÈME DE VERROUILLAGE À DISTANCE POUR METTRE EN ŒUVRE LE PROCÉDÉ

Abstract
[EN] The invention provides a method for remotely activating a remote lock system using cryptography with two-way verification mechanism between the key and the lock, and a remote lock system implementing the method. Accordingly, the key and the lock simultaneously encrypt via a hash function formula to verify the cryptography before executing the control command. In addition, the method for remotely activating a remote lock system using cryptography according to the invention further comprises a timed cryptographic attack prevention mode by increasing the command receipt time from the key for each time input using cryptography.
[FR] L'invention concerne un procédé d'activation à distance d'un système de verrouillage à distance par cryptographie selon un mécanisme de vérification à deux voies entre la clé et le verrou, ainsi qu'un système de verrouillage à distance mettant en œuvre le procédé. En conséquence, la clé et le verrou chiffrent simultanément par une formule de fonction de hachage, pour vérifier la cryptographie avant d'exécuter l'instruction de commande. De plus, le procédé d'activation à distance d'un système de verrouillage à distance utilisant la cryptographie selon l'invention comprend en outre un mode temporel de prévention d'attaque cryptographique, par augmentation du temps de réception d'instruction à partir de la clé pour chaque fois que la cryptographie d'entrée temporelle.

Figures
Step 1: The key sends a packet to the lock to activate the lock, containing two parameters: the command code and the key identifier.
Step 2: When receiving the activation packet of the key, the lock outputs any random number encrypted with that of the key, generates activation and sends it to the receiver connected to the key.
Step 3: The lock generates and transmits to the key a random number encrypted with that of the key, the control command code, the key identifier, and an cryptographic parameter to which a cryptographic number, which is an encryption result.

Method: **iKnock**
System: **CyLock**

KHẢ NĂNG HỢP TÁC

5



KHAI THÁC CÔNG NGHỆ

- Đối tác thương mại sản phẩm tại Việt Nam
- Đối tác thương mại sản phẩm phạm vi Quốc tế
- Đối tác thương mại quyền Khai thác sáng chế



CHUYỂN GIAO CÔNG NGHỆ

- Chia sẻ quyền Khai thác sáng chế
- Chia sẻ hệ thống ứng dụng đã hoàn thiện
- Cùng hợp tác khai thác sáng chế và công nghệ lõi



PHÁT TRIỂN CÁC ỨNG DỤNG MỚI

- Hệ thống phân biệt quân ta
- Thiết lập kết nối an toàn trước khi truyền tin
- Chuẩn hóa Giao thức Quốc tế

ĐỘI NGŨ CỦA CHÚNG TÔI



Tuan Nguyen Khuong

Inventor, Founder, CTO

Tuấn có hơn 17 năm kinh nghiệm trong lĩnh vực phát triển sản phẩm, công nghệ và kinh doanh với tư cách là người sáng lập một số công ty khởi nghiệp công nghệ. Đam mê đổi mới công nghệ trong ngành bảo mật.



Ngoc Tran Dinh

Co-Founder, CEO

Ngọc làm việc tại các công ty đa quốc gia, với hơn 15 năm kinh nghiệm trong thị trường B2B. Đam mê thiết lập sự hợp tác để mang lại nhiều lợi ích.



Hung Nguyen Van

Co-Founder, CMO

Hùng có hơn 15 năm kinh nghiệm trong việc kết nối và cung cấp các giải pháp công nghệ cho khách hàng. Đam mê thiết lập sự hợp tác kết nối để mang lại nhiều lợi ích.



Trung Ha Thanh

Co-Founder, Researcher

PhD in Statistics, Univ. of Florida, USA

Tiến sĩ Trung thích giải quyết các vấn đề lớn của cộng đồng. Đam mê thiết lập các hệ thống để giúp đỡ mọi người.

Tiến sĩ Trung là tác giả của mô hình dự báo covid có độ chính xác rất cao: <https://onyx.vn/covid19>



Nguyet Nguyen Mai

Advisor

Mrs. Nguyet is the Director of Business Consulting, with 16 years of experience working at Ernst & Young Vietnam,

Bà Nguyệt phụ trách tư vấn các dự án chuyển đổi doanh nghiệp, quản lý và phục hồi rủi ro, cấu trúc doanh nghiệp.



Tan Le Thanh

Market advisor

Với 16 năm kinh nghiệm làm việc cho các Ngân hàng lớn, Ông Tân mang đến góc nhìn chân thực về thị trường.

MỘT SỐ SẢN PHẨM TIÊU BIỂU TỪ ĐỘI NGŨ ĐÃ THỰC HIỆN

SmartMEDIA



Máy bán
hàng tự
động



Kiosk



SmartQMA N Từ 2005



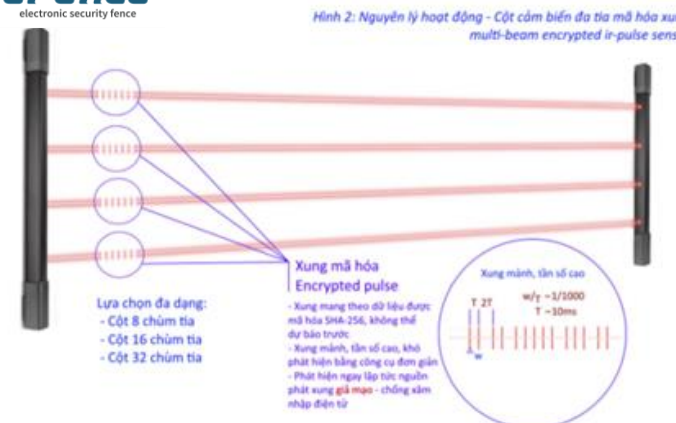
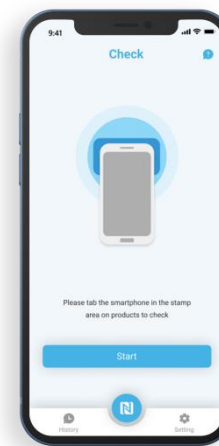
TrustFACEID



Unhackable Lock
Khóa từ xa an toàn
chống Hacker



- ① Coated paper
- ② iSeal™ Protect
- ③ Chip NFC
- ④ Antenna
- ⑤ Glue



Hàng rào lưới hồng ngoại mã hóa
Chống hacker

MỘT SỐ KHÁCH HÀNG SỬ DỤNG SẢN PHẨM ĐẾN TỪ ĐỘI NGŨ CỦA CHÚNG TÔI



Manulife - the top1 life insurance in Vietnam

Samsung - the top1 electronic maker in the world



Quality has been verified

Vietnamese solution
Vietnamese technology
Made in Vietnam

Vietcombank - the top1 bank in Vietnam



TrustFaceID



Onyx
Cypher

eFence
electronic security fence

iKnock™



Thank you!

think in simple way, do in detailed way,