Design "Strong Diffie-Hellman-Exponential-Schnnor Key Exchange" Over Elliptic Curves (SDH-XS-KE Over EC)

Demba Sow[1], Mamadou Ghouraissiou Camara[2]

[1] Université Cheikh Anta Diop de Dakar, Sénégal, Faculté des Sciences et Techniques, Département de Mathématiques et Informatique

[2] Institut Supérieur de Technologie de Mamou (ISTM), Département de Gńie Informatique, Republic of Guinea

Correspondence: Demba Sow, Universite Cheikh Anta Diop de Dakar, Senegal, Faculte des Sciences et Techniques, Departement de Mathematiques et Informatique

Received: June 16, 2019 Accepted: July 9, 2019 Online Published: July 15, 2019

doi:10.5539/jmr.v11n4p26 URL: https://doi.org/10.5539/jmr.v11n4p26

Abstract

In this paper, we design the so called "Strong Diffie-Hellman-Exponential-Schnnor Key Exchange (called SDH-XS-KE)" over Elliptic curves. SDH-XS-KE is a key echange protocol proposed in 2014. The protocol SDH-XS-KE improves the "Strong Diffie-Hellman-DSA Key Exchange (called SDH-DSA-KE)" proposed by Jeong and *al.* in 2007. First SDH-XS-KE is designed in finite groups such that $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number. So, in this paper, we present the elliptic curves version of the protocol SDH-XS-KE.

Keywords: DSA signature, Schnorr protocol, elliptic Curves, key exchange

1. Introduction

The Diffie-Hellman (DH) key exchange protocol is the best known protocol in this field (Diffie & Hellman, 1976). On the other hand, the basic protocol is vulnerable to many attacks. This is why many proposals have been made to improve the security of the DH protocol (Nyberg, 1994 & Krawczyk, 2005). But, most of the proposals have been attacked or suffered weaknesses.

1.1 Related Work

In 2003, Law, Menezes, Qu, Solinas and Vanstone designed the MQV protocol in (Krawczyk, 2005). The MQV protocol has been designed to achieve a remarkable list of security properties.

In 2005, Hugo Krawczyk show that MQV fails to a variety of attacks in Canetti-Krawczyk model (Canetti & Krawczyk, 2001) of key exchange that invalidate its basic security as well as many of its stated security goals. In (Krawczyk, 2005), Krawczyk present HMQV, a carefully designed variant of MQV, that provides the same superb performance and functionality of the original protocol but for which all the MQV's security goals can be formally proved to hold in the random oracle model under the computational Diffie-Hellman assumption.

In 2007, Jeong and *al*. proposed in (Jeong, Kwon & Lee, 2007) the "Strong Diffie-Hellman-DSA Key Exchange" (briefly: SDH-DSA-KE) where DSA signatures is used for mutual authentication but it is vulnerable to some attacks.

In 2014, Demba Sow and *al*. presented a cryptanalysis of SDH-DSA-KE (Sow, Camara & Sow, 2014) showing that it is not secure against KCI attacks and is vulnerable to disclosure to ephemeral and long-term CDH exponents. Next, they proposed "Strong Diffie-Hellman-Exponential-Schnorr Key Exchange" (briefly: SDH-XS-KE) which is an improvement of SDH-DSA-KE for efficiency and security. Their protocol use 4 exponents and is secure against Session State Reveal (SSR) attacks, Key independency attacks, Unknown-key share (UKS) attacks and Key-Compromise Impersonation (KCI) attacks.

In addition, SDH-XS-KE has the Perfect Forward Secrecy (PFS) property. For mutual authentication, instead of DSA signatures, they use a modified Schnorr Exponential protocol.

1.2 Our Contribution

First in (Sow, Camara & Sow, 2014), "Strong Diffie-Hellman-Exponential-Schnorr Key Exchange" (SDH-XS-KE) is designed in group G where $G = \mathbb{Z}/p\mathbb{Z}$ and p a prime number. In this paper, we propose the SDH-XS-KE protocol in elliptic curves.

1.3 Organization of the Paper

This paper is organize as follow:

- In **section 2**: we recall some definitions and results about elliptic curves (), Discrete Logarithm Problem over Elliptic curves (), Diffie-Hellman protocol over Elliptic curves (), Schnorr protocol over Elliptic curves () and security notions about key exchange protocols ().
- In **section 3**: first, we design SDH-XS-KE protocol over Elliptic curves. In additional, we show its performance and security.

2. Preliminaries

2.1 Elliptic Curves Over a Finite Field

Definition 1 Let $\mathbb{F}$ be a field.

- An elliptic curve $\mathcal{E}$ over $\mathbb{F}$ can be given by the so-called Weierstrass equation

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

  where the coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$ and $\mathcal{E}$ has to be nonsingular.

- The set of $\mathbb{F}$-rational points on $\mathcal{E}$ is defined by the set of points

$$\mathcal{E}(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{P_\infty\}$$

  where P_∞ is the point at infinity.

- The set of $\mathbb{F}$-rational points on $\mathcal{E}$ by means of the chord-and-tangent process turns $\mathcal{E}(\mathbb{F})$ into an abelian group with P_∞ as the neutral element.

Definition 2 (**Elliptic curves over a finite field $\mathbb{F}_q$**).
Let $\mathbb{F}_q$ be a field not of characteristic 2 or 3. Suppose $a, b \in \mathbb{F}_q$ such that $x^3 + ax + b$ has no multiple roots. The equation of the elliptic curve $\mathcal{E}$ can be transformed into the reduced Weierstrass form

$$y^2 = x^3 + ax + b,\ a, b \in \mathbb{F}_q$$

where $4a^3 + 27b^2 \neq 0$. When $\mathbb{F}_q$ for some prime $q > 3$, such a curve will be denoted $\mathcal{E}_q(a, b)$.

Theorem 1 (Hasse) *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$. Then*

$$q + 1 - 2\sqrt{p} \leq |E| \leq q + 1 + 2\sqrt{q}.$$

2.2 Discret Logarithm Problem

Let $E(\mathbb{K})$ an elliptic curve over a finite field $\mathbb{K}$ and a generator P of order q.

- The Elliptic Curve Discrete Logarithm Problem (ECDLP) is to determine the integer k, given rational points P and Q on $E(\mathbb{K})$, and given that $k * P = Q$.
- The Elliptic Curve Computational Diffie-Hellman Problem (ECCDH) is the following: given rational points $Q_1 = k_1P$ and $Q_2 = k_2P$, compute $Q = k_1k_2P$.

2.3 Diffie-Hellman Key Exchange

Diffie-Hellman is a key exchange protocol invented in 1976 and presented in the article: *New directions in cryptography* (Diffie & Hellman, 1976).

Diffie-Hellman protocol over elliptic curve

Let $E(\mathbb{K})$ an elliptic curve over a finite field $\mathbb{K}$ and a generator P of order q.

- A selects an integer a such that $1 < a < q - 1$, keeps it secret and sends $[a]P$ to B.
- B selects an integer b such that $1 < b < q - 1$, keeps it secret and sends $[b]P$ to A
- Both A and B compute $k = [a][b]P = [b][a]P = [ab]P$.

2.4 Schnorr Protocol

2.4.1 Schnorr Identification Protocol

Let $E(\mathbb{K})$ be an elliptic curve over a finite field $\mathbb{K}$ and $g \in E(\mathbb{K})$ be a point of order q.

In Schnorr identification protocol, sk is the secret key and $a \in [1, q]$ is an integer. Take $\gamma = [a]g$ and $pk = (E(\mathbb{F}_p), g, \gamma)$ the public key.

Let $\mathcal{P}$ the prover and $\mathcal{V}$ the verifier.

1. $\mathcal{P}$ takes an element $x \overset{Rand}{\leftarrow} [1, q]$ and dispatchs $X = [x]g$ to $\mathcal{V}$.
2. $\mathcal{V}$ takes an element "challenge" $e \overset{Rand}{\leftarrow} [1, q]$ and dispatchs e to $\mathcal{P}$.
3. $\mathcal{P}$ computes $s = x + ae \mod q$ and dispatchs s to $\mathcal{V}$.

$\mathcal{P}$ is identified by $\mathcal{V}$ if $[s]g = X + [e]\gamma$.

2.4.2 Exponential Schnorr Identification Protocol

Let $\mathcal{P}$ the prover and $\mathcal{V}$ the verifier.

In Exponential Schnorr identification protocol, sk is the secret key and $\alpha \in [1, q]$ is an integer. Take $\gamma = [\alpha]g$ and $pk = (E(\mathbb{F}_p), g, \gamma)$ the public key.

1. $\mathcal{V}$ takes an element $y \overset{Rand}{\leftarrow} [1, q]$ and dispatchs $Y = [y]g$ to $\mathcal{P}$.
2. $\mathcal{P}$ takes an element $x \overset{Rand}{\leftarrow} [1, q]$ and dispatchs $X = [x]g$ to $\mathcal{V}$.
3. $\mathcal{V}$ takes an element "challenge" $e \overset{Rand}{\leftarrow} [1, q]$ and dispatchs e to $\mathcal{P}$.
4. $\mathcal{P}$ computes $s = x + \alpha e \mod q$ and dispatchs $S = sY$ to $\mathcal{V}$.

$\mathcal{P}$ is identified by $\mathcal{V}$ if $S = y(X + [e]\gamma)$.

We can prove that Exponential Schnorr identification is a proof of the "ability" of the prover $\mathcal{P}$ to calculate $CDH(\gamma, Y)$ for all $X \in G$. The protocol is furthermore a zero knowledge for a verifier V that randomly takes e, (Krawczyk, 2005).

2.5 Security Notions About Key Exchange Protocols

In this section, we will define security terms that key sharing protocols should check.

1. **Key Independency**. Independence of keys: this term means that the keys of sessions are computationally independent between them.
2. **Session State Reveal Attack**. this term means that the security of the session keys is ensured even if the attacker has access to the random numbers which made it possible to generate them.
3. **Perfect Forward Secrecy (PFS)**: this term means that the attacker's knowledge of a long-term key must not compromise the progress of the protocol.
4. **Resistance to Key-Compromise Impersonation (KCI) attacks** This term means that even if the private key of one of the parties is known by the attacker, this should not allow him to control a session.

5. **The case of Diffie-Hellman Key exchange protocol:** (Krawczyk, 2005)
   Let a session $(id_A, id_B, V_A = v_A \cdot g, V_B = v_B \cdot g)$ for two parties A and B having the respective key pairs $(x_A, x_A \cdot g)$ and $(x_B, x_B \cdot g)$; the computation of the session key involves the four secret values x_A, x_B, v_A, v_B. Obviously the disclosure of $\{x_A, v_A\}$, or $\{x_B, v_B\}$, gives the attacker the advantage of reading the session key.

   Securing the communication between A and B requires that the attacker's knowledge of any other pair of values (except $\{x_A, v_A\}$, and $\{x_B, v_B\}$) in the set $\{x_A, x_B, v_A, v_B\}$ must not allow it to lead an attack. We can summarize this as follows:

   - $\{x_A, x_B\}$ and try to get the session key from the keys of previous sessions: this is PFS attack;
   - $\{v_A, v_B\}$: this stems from the security to State reveal attack;
   - $\{x_A, v_B\}$ or $\{x_B, v_A\}$: this stems from the security to KCI attacks;
   - $x_A x_B \cdot g$ without learning (x_A, x_B): this stems from the security of the disclosure of long-term DH exponents;
   - $v_A v_B \cdot g$, without learning $\{v_A, v_B\}$: this follows from the security of the disclosure of ephemeral DH exponents;

3. The Protocol SDH-XS-KE Over Elliptic Curves

In the SDH-XS-KE protocol, modified Schnorr Exponential protocol provides mutual authentication between parties.

3.1 Design SDH-XS-KE Over Elliptic Curves

Let $E(\mathbb{K})$ an elliptic curve over a finite field $\mathbb{K}$, $g \in E(\mathbb{K})$ a generator of order q and $\overline{O}$ the point at infinity. Let $H : E(\mathbb{K}) \times E(\mathbb{K}) \times \overline{\mathcal{P}} \to \{0,1\}^l$ be a hash function (where $l \geq 224$ and $\overline{\mathcal{P}}$ is the set of all parties authorized to take part in the protocol). Let $\mathcal{G} : E(\mathbb{K}) \to \{0,1\}^l$ be a randomness extractor on $E(\mathbb{K})$ and and $\overline{H} : \{0,1\}^l \times \overline{\mathcal{P}} \times \overline{\mathcal{P}} \times \{0,1\} \to \{0,1\}^l$ be a hash function and $\mathbf{MAC}_K : E(\mathbb{K}) \times E(\mathbb{K}) \times \overline{\mathcal{P}} \to \{0,1\}^l$ be a keyed hash function for Mac authentication.

Suppose that $(x_A, y_A = x_A \cdot g)$ the Alice key pair and $(x_B, y_B = x_B \cdot g)$ the Bob key pair where $x_A, x_B < q$ are random integers.

Protocol

1. Alice chooses a secret session's random $v_A < q$, calculates $V_A = v_A \cdot g$, $\delta_{AB} = (v_A + x_A) \cdot y_B$ and $h_{AB} = H(\delta_{AB}, V_A, id_A)$, destroy δ_{AB} and dispatchs (V_A, h_{AB}) to Bob;
2. - Bob verifies if $V_A \neq \overline{O}$, calculates $\lambda_{BA} = x_B \cdot (V_A + y_A)$ and $H(\lambda_{BA}, V_A, id_A)$ and destroy λ_{BA}; verifies if $H(\lambda_{BA}, V_A, id_A) \neq h_{AB}$;
   - If any of the above checks do not match then Bob interrupts the flow of the protocol.
   - Bob chooses a secret session's random $v_B < q$, calculates $V_B = v_B \cdot g$ and $K_{mac} = \overline{H}(K_{B2}, id_A, id_B, 1)$ where $K_{B2} = \mathcal{G}(g_{KBs}, l)$ and $g_{KBs} = (v_B + x_B) \cdot (V_A + y_A)$.
   - Bob calculates $\delta_{BA} = (v_B + x_B) \cdot y_A$, $h_{MAC_B} = \mathbf{MAC}_{K_{mac}}(\delta_{BA}, V_B, id_B)$, destroy δ_{BA} and dispatchs (V_B, h_{MAC_B}) to Alice;
3. - Alice verifies if $V_B \neq \overline{O}$, calculates $K_{mac} = \overline{H}(K_{A2}, id_A, id_B, 1)$ where $K_{A2} = \mathcal{G}(g_{KAs}, l)$ and $g_{KAs} = (v_A + x_A) \cdot (V_B + y_B)$.
   - calculates $\lambda_{AB} = x_A \cdot (V_B + y_B)$ and $h'_{MAC_B} = \mathbf{MAC}_{K_{mac}}(\lambda_{AB}, V_B, id_B)$, and destroy λ_{AB}; verifies if $h'_{MAC_B} \neq h_{MAC_B}$,
   - If any of the above checks do not match then Alice interrupts the flow of the protocol, otherwise,
   - Alice calculates $h_{MAC_A} = \mathbf{MAC}_{K_{mac}}(g_{KAs}, V_A, id_A)$, and dispatchs it to Bob.
   - Alice calculates and saves $K_{As} = \overline{H}(K_{A2}, id_A, id_B, 0)$ as her current session key.
4. - Bob calculates $h'_{MAC_A} = \mathbf{MAC}_{K_{mac}}(g_{KBs}, V_A, id_A)$, and verifies if $h'_{MAC_A} \neq h_{MAC_A}$.
   - If any of the above checks do not match then Bob interrupts the flow of the protocol, otherwise, Bob calculates and saves the key $K_{Bs} = \overline{H}(K_{B2}, id_A, id_B, 0)$ as his current session key.

3.2 SDH-XS-KE Over Elliptic Curves: Security and Performance

The modified Schnorr Exponential protocol has ensured mutual authentication between parties where their public keys are their challenges. The success of the protocol depends on the honesty of the participants who must select, use and save the values of the protocol parameters correctly. That said for the future that we assume the participants are honest.

Performance

In the SDH-XS-KE protocol, there is a key confirmation step and we used only 4 exponents and 4 passes. Thus, it is efficient (because faster) than SDH-DSA-KE where 5 exponents 4 passes are used.

Security

In (Sow, Camara & Sow, 2014), the vulnerability to KCI attacks of the SDH-DSA-KE protocol is shown. In what follows, we will prove the security of the SDH-XS-KE protocol if there is the impossibility of calculating CDH (V_A, V_B), CDH (y_A, y_B), CDH (V_A, y_B), CDH (V_B, y_A) and if the hash function used is solid.

Theorem 2 *The SDH-XS-KE protocol over elliptic curves has the Perfect Forward Secrecy property.*

Proof There is a key confirmation step, plus the attacker can not participate in the session where the parties will create the session key. The only possibility that the attacker is to compute the session key directly if we suppose that he holds the keys in the long term in other words x_A and x_B. The session key is thus equal to $K_{Bs} = \overline{H}(K_{B2}, id_A, id_B, 0)$ where $K_{B2} = \mathcal{G}(g_{KBs}, l)$ and $g_{KB} = (v_A + x_A)(v_B + x_B) \cdot g = v_A v_B \cdot g + x_A x_B \cdot g + x_B \cdot V_A + x_A \cdot V_B$ and the attacker knows x_A and x_B then he can compute $x_A x_B \cdot g + x_B \cdot V_A + x_A \cdot V_B$. So the attacker can calculate g_{KBs} if and only if he can calculate $(v_A v_B) \cdot g = CDH(V_A, V_B)$, this is impossible if we assume that both parties are honest.

Theorem 3 *The SDH-XS-KE protocol over elliptic curves is safe against KCI (Key-Compromise Impersonation) and UKS (Unknown Key Attack) attacks.*

Proof **1)** Security against KCI attack (Key-Compromise Impersonation): In SDH-XS-KE the modified Schnorr Exponential protocol is used to guarantee mutual authentication by hashing the output produced by this same protocol: Alice calculates $\delta_{AB} = (v_A + x_A) \cdot y_B$, dispatchs $h_{AB} = H(\delta_{AB}, V_A, id_A)$ to Bob and destroy δ_{AB}; Bob calculates $\delta_{BA} = (v_B + x_B) \cdot y_A$ and dispatchs $h_{MAC_B} = \mathbf{MAC}_{K_{mac}}(\delta_{BA}, V_B, id_B)$ to Alice and destroy δ_{BA}. Thus, the protocol fails if the attacker is active and does not know simultaneously v_A and x_A or v_B and x_B. So, the only possibility for the attacker is to directly calculate the session key, assuming he has access to Alice's long-term secret key (ie x_A) and the random value of Bob's session (ie v_B).

So the session key is $K_{Bs} = \overline{H}(K_{B2}, id_A, id_B, 0)$ where $K_{B2} = \mathcal{G}(g_{KB}, l)$ and $g_{KB} = (v_A + x_A)(v_B + x_B) \cdot g = v_B \cdot V_A + x_A \cdot y_B + x_A \cdot V_B + x_B \cdot V_A$ and the attacker knows x_A and v_B then he can calculate $v_B \cdot V_A + x_A \cdot y_B + x_A \cdot V_B$. Thus, the attacker can calculate g_{KBs} if and only if he can calculate $x_B \cdot V_A = CDH(V_A, y_B) = DLP_{V_A}(x_B \cdot V_A)$, this is impossible if we assume that both parties are honest.

2) Security against UKS (unknown-key share) attack: in the authentication process, Alice calculates $\delta_{AB} = (v_A + x_A) \cdot y_B$ and dispatchs $h_{AB} = H(\delta_{AB}, V_A, id_A)$ to Bob and destroy δ_{AB}; Bob calculates $\delta_{BA} = (v_B + x_B) \cdot y_A$ and dispatchs $h_{MAC_B} = \mathbf{MAC}_{K_{mac}}(\delta_{BA}, V_B, id_B)$ to Alice and destroy δ_{BA}. So the public keys and identities of the parts (id_A, id_B) are hashed. This causes UKS attacks to fail.

Theorem 4 *The SDH-XS-KE protocol over elliptic curves is safe against SSR (Session State Reveal) attacks.*

Proof As the session key is $K_{Bs} = \overline{H}(K_{B2}, id_A, id_B, 0)$ where $K_{B2} = \mathcal{G}(g_{KBs}, l)$ and $g_{KBs} = (v_A + x_A)(v_B + x_B) \cdot g = v_A v_B \cdot g + x_A x_B \cdot g + v_B \cdot y_A + v_A \cdot y_B$ and the attacker knows v_A and v_B then he can calculate $v_A v_B \cdot g + v_B \cdot y_A + v_A \cdot y_B$. Thus, the attacker can calculate g_{KBs} if and only if he can calculate $x_A x_B \cdot g = CDH(y_A, y_B)$, this is impossible if we assume that both parties are honest.

Theorem 5 *The SDH-XS-KE protocol over elliptic curves has the key independence property.*

Proof As the session key is $K_{Bs} = \overline{H}(K_{B2}, id_A, id_B, 0)$ where $K_{B2} = \mathcal{G}(g_{KBs}, l)$ and $g_{KBs} = (v_A + x_A)(v_B + x_B) \cdot g = v_A v_B \cdot g + x_A x_B \cdot g + x_B \cdot V_A + x_A \cdot V_B$. Thus the properties of the hash function, the use of identities (id_A and id_B) and the session's random (v_A and v_B) guarantee the key independence property.

Theorem 6 *The SDH-XS-KE protocol over elliptic curves is safe against attacks based on "disclosure to ephemeral and long-term CDH".*

Proof As the session key is $K_{Bs} = \overline{H}(K_{B2}, id_A, id_B, 0)$ where $K_{B2} = \mathcal{G}(g_{KBs}, l)$ and $g_{KBs} = (v_A + x_A)(v_B + x_B) \cdot g = v_A v_B \cdot g + x_A x_B \cdot g + v_B \cdot y_A + v_A \cdot y_B$ and the attacker knows $g^{v_A v_B}$ and $g^{x_A x_B}$, so he can calculate $v_A v_B \cdot g + x_A x_B \cdot g$. Thus the attacker can calculate g_{KBs} if and only if he can calculate $v_B \cdot y_A + v_A \cdot y_B = CDH(y_A, V_B) CDH(V_A, y_B)$, this is impossible if we assume that both parties are honest.

4. Conclusion

We have successfully introduced the elliptic curve version of the SDH-XS-KE key exchange protocol using Schnorr's modified identification protocol for mutual authentication.

References

Arazi, A. (1993, Nov). Inegrating a key cryptosystem into the digital signature standard, *Electron. Lett., 29,* 966-967. https://doi.org/10.1049/el:19930643

Canetti, R., & Krawczyk, H. (2001). *Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels*, Eurocrypt?2001, LNCS Vol. 2045. Full version in: Cryptology ePrint Archive (http://eprint.iacr.org/), Report 2001/040. https://doi.org/10.1007/3-540-44987-6_28

Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography, *IEEE Trans. on Info. Theory, IT-22*, 644-654. https://doi.org/10.1109/TIT.1976.1055638

Harn, L. M., & Hsin, W. J. (2004, Mar). Integratin Diffie-Hellman key exchange into a digital signature algorithm (DSA), *IEEE Commun. Lett., 8,* 198-200. https://doi.org/10.1109/LCOMM.2004.825705

Jeong, I. R., Kwon, J. O., & Lee, D. H. (2007, May). Strong Diffie-Hellman DSA Key Exchange, *IEEE Communications Letters, 11*(5), 432-433. https://doi.org/10.1109/LCOMM.2007.070004

Krawczyk, H. (2005). *HMQV: a high-performance secure Diffie-Hellman Protocol*, in Proc. CRYPTO'05, 546-566. https://doi.org/10.1007/11535218_33

Law, L., Menezes, A., Qu, M., Solinas, J., & Vanstone, S. (2003). An efficient Protocol for Authenticated Key Agreement, *Designs, Codes and Cryptography, 28*, 119-134.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*, CRC Press.

Menezes, A. J., Qu, M., & Vanstone, S. A. (1995). *Some new key agreement protocols providing mutual implicit authentication*, Second Workshop on Selected Areas in Cryptography (SAC 95).

Nyberg, K., & Rueppel, R. A. (1994, Jan). Weaknesses in some recent key agreement protocols, *Electron. Lett., 30*, 26-27. https://doi.org/10.1049/el:19940052

Phan, R. C. W. (2005, June). Fixing the integrated Diffie-Hellman-DSA key exchange protocol, IEEE Commun. *Lett., 9*, 570-572. https://doi.org/10.1109/LCOMM.2005.1437374

Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots $\mod p$, *Mathematics of Computation, 44*(170), 483 – 485. https://doi.org/10.2307/2007968

Sow, D., Camara, M. G., & Sow, D. (2014). Attack on Strong Diffie-Hellman-DSA KE, Improvement. *Journal of Mathematics Research*, *6,* 70-75. https://doi.org/10.5539/jmr.v6n1p70

Copyrights